My mathematical research is in the general area of *number theory*. More specifically, I am interested in and have done work in analytic number theory, arithmetic statistics, and diophantine geometry.

Analytic number theory originated with the use of complex analysis to study counting functions of number theoretic interest, starting with the pioneering work of Riemann in the 19th century, leading to the proof of the prime number theorem by Hadamard and de la Vallee Poussin at the end of the 19th century. Analytic number theory flourished in the first half of the 20th century, due in no small part to the seminal contributions of G. H. Hardy, J. E. Littlewood, and S. Ramanujan. My work in analytic number theory largely concerns *density problems*; that is, obtaining asymptotic estimates for counting functions of objects of interest up to bounded height.

Arithmetic statistics is closely related, and in particular, is largely concerned with density problems. Arithmetic statistics in the modern age appear to have originated from the foundational work of Cohen and Lenstra, who gave overarching heuristics predicting the distribution of various group structures spanning the breadth of number theory. Most notably, they gave predictions for the distribution of class groups of number fields when ordered by discriminant. Theorems in arithmetic statistics are mostly concerned with giving instances for which the Cohen-Lenstra heuristics can be confirmed or denied. My work largely concerns the low degree cases, in particular degrees $n \leq 5$.

Diophantine geometry is at the interface of counting problems in number theory and algebraic geometry. The most intriguing problems in diophantine geometry concern the most basic objects, such as enumerating rational points on curves of positive genus. Central to diophantine geometry is the theory of heights. For instance, Faltings' magnificent proof of Mordell's conjecture largely centres on his insight of using a slightly different height, now named in his honour. In my work I have extended a general method of bounding rational points of bounded height on algebraic varieties in projective space due to Heath-Brown and Salberger to the setting of weighted projective spaces. More recently, I have started investigating extending theories of height to algebraic stacks.

A long term goal of my research is to understand how to *uniformize* various finiteness theorems. Specifically, I am motivated by the so-called *uniform boundedness conjecture* for algebraic curves of general type, known to hold under Lang's conjecture due to work of Caporaso, Harris, and Mazur [26]. Recently remarkable progress has been made towards this question from various angles: Minhyong Kim's generalization of the method of Chabauty has yielded significant progress towards enumerating all rational points on certain curves (especially curves with additional structure); Lawrence and Venkatesh [50] has come up with a new way to prove Faltings' theorem using p-adic period maps, and outstanding work due to Dimitrov, Gao, and Habegger have resolved an old conjecture due to Mazur concerning uniformity of rational points on curves of general type with respect to the rank of the Mordell-Weil group [30].

Another long term goal is to make further progress towards understanding instances of enumerating algebraic number fields and related objects. This includes understanding number fields, rings, and polynomials with "small Galois groups" (i.e., not the full symmetric group).

Analytic Number Theory

Analytic number theory has expanded to cover a large swath of modern mathematics. My work in analytic number theory largely concerns *density problems*; that is, obtaining asymptotic estimates for counting functions of objects of interest up to bounded height. My work in this area include obtaining density theorems for power-free values of binary forms [1], polynomials of any number of variables (joint work with K. Lapkova) [7] [8], and square-free values of decomposable forms [3]. Separately, in joint work with C. L. Stewart, we have obtained asymptotic formulae for the number of integers and the number of k-free integers $|h| \leq Z$ representable by a given binary form $F \in \mathbb{Z}[x, y]$ having degree $d \geq 3$ [12] [13].

My thesis was initially focused on finding improvements to the range of k, relative to the degree d of the binary form F, for which we can establish the expected density of k-free values. The best results prior were due to Greaves who established the best possible result for $d \leq 6$ [37], to Hooley who established the best known result for $d = 8$ [47], and to Browning for the range $k > 7d/16$ [24]. In [1], I expanded this range to $k > 7d/18$. Crucially, my work covers the case $(k, d) = (6, 15)$, which has implications in constructing interesting algebraic families of elliptic curves.

In joint work with C. L. Stewart, we established the following: given a binary form $F \in \mathbb{Z}[x, y]$ with non-zero discriminant and degree $d \geq 3$, the number of integers $R_F(Z)$ satisfying $|h| \leq Z$ for which the Thue equation $F(x, y) = h$ has a solution satisfies an asymptotic formula [12]. This problem has a long history and has been studied by a long list of mathematicians, including Gauss, Landau, Erdös [31], Mahler [51] [32], and Hooley [43] [44] [45]. More recent work on the subject include those of Skinner-Wooley [55], Bennett-Dummigan-Wooley [19], and of course the seminal work of Heath-Brown [39]. It is Heath-Brown's paper [39], where he introduced his p-adic determinant method, that paved the way for our work. Indeed, our key insight was that the remaining ingredient is to understand the behaviour of the *automorphism group* of the form F and its implications on the main term of the asymptotic formula.

Extending my work on k-free values of binary forms and the aforementioned work on estimating $R_F(Z)$, Stewart and I obtained the asymptotic formula for the number $R_F^{(k)}(Z)$ of k-free integers h satisfying $|h| \leq Z$ representable by the form F. Here our asymptotic formula is valid whenever the density of pairs $(x, y) \in \mathbb{Z}^2$ for which $F(x, y)$ is k-free can be established; that is, whenever $k > \min\{\lfloor d/2 \rfloor - 1, 7d/18\}$. We also obtain the asymptotic formula for $R_F^{(2)}(Z)$ for all degrees d provided that we assume the *abc*-conjecture, building on earlier work of Granville [36].

Using quite different methods, essentially building directly on the groundbreaking work of Greaves [37] and Hooley [47], I was able to establish that *incomplete norm forms* in n variables having degree $d > n$ take on the correct density of *square-free values*, provided that $d \leq 2n + 2$, in [2]. Note that when $n = 2$ we recover exactly the theorem of Greaves. This adds to a relative short list of polynomials where we can establish the correct density of square-free values (see for example [37], [36], [52] and [22]).

My more recent work on k-free values of polynomials is in joint work with K. Lapkova. Together we established, in [7] and [8], that polynomials $F \in \mathbb{Z}[x_1, \cdots, x_n]$ of degree $d \geq 2$ satisfying the basic necessary conditions take on the correct density of k-free values provided that $k \geq \{d-1, (3d-1)/4\}$. This work builds on earlier work of Hooley [47] and Browning [24], as well as the quantitative version of Ekedahl's sieve formulated by Bhargava and Shankar [21].

Because of its history and origin, analytic number theory is inseparable from the study of prime numbers. The subset of number theory concerning specifically the study of primes is appropriately called *prime number theory.* On this topic I have contributed the following: with S. Yamagishi we showed that systems of polynomial equations of sufficiently low degree and large number of variables, satisfying certain non-degeneracy conditions, are always solvable in primes [16]. This refines work of B. Cook and A. Magyar in some cases. With P. Lam and D. Schindler we showed that given a positive definite binary quadratic form $f(x,y)$ and a linear form $\ell(x,y)$, there exist infinitely many pairs of integers x, y such that $f(x,y), \ell(x,y)$ are both prime [9]. Currently, I am working to extend this result to cover also the case when f is indefinite and irreducible.

My paper with S. Yamagishi is part of a long story, starting with the foundational work of B. J. Birch [23]. In particular, we built on work of B. Cook and A. Magyar [28] and answered a question they posed in some special cases. Cook and Magyar essentially showed that Birch's conclusion in [23] holds when all variables are required to only take on prime values, at the cost that the number of variables required is greatly increased. The key algebraic input is an assumption on the so-called *Birch singular locus.* W. M. Schmidt showed in [54] that it suffices to consider a much simpler invariant, now known as Schmidt's h-invariant. Cook and Magyar asks whether one can obtain their result with an assumption on the h-invariant instead. With Yamagishi, we answer this question partially: the result holds provided that a new invariant, which we call the h^*-invariant, is sufficiently large. The interesting thing is that the h-invariant and our h^*-invariant coincide for forms of degree 2 and 3, allowing us to partially answer Cook and Magyar's question.

My joint work with Lam and Schindler sought to generalize work of Fouvry and Iwaniec [33], who showed that the quadratic form x^2+y^2 takes on infinitely many prime values with the added requirement that y is also prime. The analytic machinery they developed proved to be foundational, leading to subsequent breakthroughs by Friedlander and Iwaniec [35] and Heath-Brown and Li [40].

In [9], we proved that for any positive definite binary quadratic form f with co-prime coefficients and such that $f(x,1)$ is not always divisible by 2 has the property that $f(x,p)$ is prime infinitely often, with p a prime variable. An attractive consequence of our theorem is the following: let F be a reducible binary cubic form which has negative discriminant. Then modulo obvious necessary conditions, $F(x,y)$ is divisible by exactly two primes infinitely often. This gives a new case of a far reaching conjecture of Schinzel, which essentially asserts that polynomials $f(x_1, \cdots, x_n) \in \mathbb{Z}[x_1, \cdots, x_n]$ with exactly r factors over $\mathbb{Q}$ are divisible by exactly r distinct primes infinitely often.

Arithmetic Statistics

The rapid ascension of arithmetic statistics in recent years is largely due to the magnificent contributions of M. Bhargava and his collaborators, colleagues, and students, ultimately leading to him being awarded the Fields Medal in 2014. One particular result, due to Bhargava and Shankar [21], has been of particular interest to me. Indeed, they established unconditionally that the average rank of elliptic curves over $\mathbb{Q}$, ordered by the naive height given by their short Weierstrass models, is bounded. More precisely, they were able to establish an *exact* asymptotic formula for the number of 2-Selmer elements of bounded height.

Motivated by the work of Bhargava and Shankar, C. Tsang and I sought to refine their theorem to the case when one restricts to binary quartic forms having *small Galois group*. It turns out that the Galois group of binary quartic forms are controlled by certain quadratic covariants discovered by J. Cremona [29]. This was used by me to compute the automorphism groups of binary quartic forms explicitly in [3], thus making my theorem with C. L. Stewart [12] completely explicit in degrees 3 and 4. Motivated by the observation that for an irreducible binary quartic form F the Galois group $\mathrm{Gal}(F)$ is isomorphic to a subgroup of the dihedral group D_4 if and only if one of these quadratic covariants, which I named *Cremona covariants*, is rational, Tsang and I sought to count the number of $\mathrm{GL}_2(\mathbb{Z})$-orbits of binary quartic forms with a rational quadratic covariant. It turns out that this set of binary quartic forms is naturally partitioned into families indexed by $\mathrm{GL}_2(\mathbb{Z})$-classes of binary *quadratic* forms. In [14], we counted the number of $\mathrm{GL}_2(\mathbb{Z})$-classes of binary quartic forms for a fixed (rational) quadratic covariant.

Due to uniformity issues, we were not able to sum over all classes of indexing quadratic forms in [14], thus barring our methods from any applications in arithmetic statistics. However, if we consider $\mathrm{GL}_2(\mathbb{Z})$-classes of binary quartic forms as parametrizing objects for *quartic rings*, an idea fully explained by M. Matchett-Wood [59] in her thesis, then our methods allow us to count the following objects: irreducible, maximal quartic rings whose field of fractions is a quartic D_4, C_4, or V_4-field whose cubic resolvent ring is *monogenic*. This program is carried out in our subsequent paper [15]. The additional challenge is that we must count with respect to a height that makes sense for quartic rings, the obvious height being the absolute discriminant. This turns out to be a barely tractable problem, in the sense that we are able to produce lower and upper bounds of similar (but not identical) magnitude. However, as explained by Altug, Shankar, Varma, and Wilson [17] a more appropriate height to impose on quartic D_4-fields is their *Artin conductor*. It turns out that in our case the Artin conductor can be expressed as an explicit polynomial expression, which we dubbed the *conductor polynomial*, which makes the problem of counting quartic D_4-fields with monogenic cubic resolvent by conductor tractable to methods in Geometry of Numbers. In the same paper we also counted elliptic curves with a marked 2-torsion point by *discriminant*, which is of course an impossible task without the hypothesis of having a marked 2-torsion point.

More recently, I have began working on a more classical line of inquiry. Hilbert's irreducibility theorem can be considered an early theorem in arithmetic statistics. The question here is to understand the distribution of irreducible monic polynomials whose Galois group is not the full symmetric group. Van der Waerden was the first to obtain quantitative upper bounds for the number of such polynomials, and for a long time his results have stood firm. He asked whether the irreducible, non-S_n polynomials are dominated by the reducible polynomials. Chow and Dietmann showed that the reducible polynomials dominate the irreducible non-S_n polynomials for $n = 3, 4$ in [27]. Moreover, they obtained the exact order of magnitude for the number of monic, irreducible D_4-quartic polynomials. In [4], I improved their bound on the number of monic abelian cubic polynomials of bounded box height, obtaining the best possible exponent.

Subsequently I looked at the negative Pell equation and its generalizations. This is motivated by a result obtained with C. Tsang in [14], where we gave a new characterization for the solubility of the negative Pell equation, and by the recent breakthrough by A. Smith on the distribution of 2^∞-class groups of imaginary quadratic fields [56]. In joint work with E. Knight [5], we showed that there is a genus theory and distribution law for "one exponent above" in the case of the ζ_3-*Pell equation*. Here we consider the negative Pell equation to be whether a given quadratic extension $\mathbb{Q}(\sqrt{d})$ over the field $\mathbb{Q} = \mathbb{Q}(\zeta_2)$ contains an integer with norm equal to $\zeta_2 = -1$, and the corresponding generalization to be whether a *cubic* extension $K(\sqrt[3]{\alpha})$ of $K = \mathbb{Q}(\zeta_3)$. This work generalizes work by Fouvry and Kluners on the negative Pell equation [34]. In subsequent work with Knight, we are looking at the distribution of appropriate torsion parts of class groups of fields of the form $K_p(\sqrt[p]{\alpha})$, where $K_p = \mathbb{Q}(\zeta_p)$.

Recently, inspired by the work of A. B. Miller on enumerating simple knots of genus 1, I started a collaboration with her to obtain an asymptotic formula for the number of simple knots having discriminant of the form $1 - 4p$. These knots are expected to be "most" of the knots, despite the fact that numbers of the form $1 - 4p$ are relatively scarce among the integers. An exciting aspect of this work is that we acquired a quantitative version of an equidistribution result on roots to solutions of quadratic congruences. This aspect of the work is based on earlier work of Hooley [42].

Diophantine Geometry

My contributions to diophantine geometry have been relatively indirect. For example, in [1] I have shown that the number of integral points on surfaces of the shape

$$F(x, y) = uv^k$$

where F is a non-singular binary form of degree $d > k$, even in skew boxes, satisfy the expected bound from Serre's dimension growth conjecture. In particular, in [1] I extended the p-adic *determinant method* of Heath-Brown [39] and the global determinant method of Salberger [53] to the setting of certain weighted projective spaces. In particular, I proved that the main theorem of the (global) determinant method holds for weighted projective spaces with at least two weights equal to one.

In [3], as a corollary to the explicit calculations of the automorphism groups of binary cubic and quartic forms in terms of their Julia and Cremona covariants, I was able to gain a sharper understanding of the arithmetical nature of the lines on surfaces X_F given by

$$X_F : F(x_1, x_2) - F(x_3, x_4) = 0$$

where F is a binary cubic or quartic form defined over $\mathbb{Q}$. In particular, I was able to show that the field of definitions of the lines on X_F tend to be very small. In the cubic case for example I showed that the field of definition K of the lines in X_F satisfies $[K : \mathbb{Q}] \leq 12$, where as the generic cubic surface will have $[K : \mathbb{Q}] = 51840$, with Galois group isomorphic to $W(E_6)$, the Weyl group of the E_6-root system.

I am keenly interested in *uniformity* problems in diophantine geometry, in particular, the so-called *uniform boundedness conjecture*. This conjecture was famously proved by Caporaso, Harris, and Mazur [26] under the hypothesis that the Bombieri-Lang conjecture holds.

Since then, two spectacular unconditional results have been obtained: Katz, Rabinoff, and Zuerick-Brown [48] have proved that the uniform boundedness conjecture holds for curves satisfying $r \leq g - 3$, where r is the Mordell-Weil rank of the curve and g the genus, and the recent breakthrough by Dimtrov, Gao, and Habegger [30] which shows that the uniform boundedness conjecture holds for curves of bounded Mordell-Weil rank (that is, one no longer needs any assumption on the size of the rank compared to the genus). We note that the work of Katz, Rabinoff, and Zuerick-Brown builds on earlier work by Stoll [58], who proved the same result but for hyperelliptic curves. Lawrence and Venkatesh [50] recently gave a new proof of Faltings' theorem using p-adic period maps, which offers new hope that the dependence on the rank can be removed. Minhyong Kim's non-abelian Chabauty program (initiated in [49]) also holds much promise.

My key motivation behind this line of inquiry is the following conjecture, due to C. L. Stewart, given in [57]: There exists a positive integer c_0 such that whenever F is a non-singular binary form of degree $d \geq 3$ and discriminant $\Delta(F)$, there exists a positive number $r = r(F)$ such that for all integers h with $|h| \geq r$ the Thue equation $F(x, y) = h$ has at most c_0 primitive solutions. Stewart's conjecture is in some sense even stronger than the uniform boundedness conjecture, since it can be interpreted as asserting that for a given curve $\mathcal{C}/\mathbb{Q}$, the number of integral points on quadratic twists $\mathcal{C}_d$ of $\mathcal{C}$ is absolutely bounded except for finitely many exceptions (the "finitely many" depends on $\mathcal{C}$).

Even given the result of Dimitrov, Gao, and Habegger [30], which resolves Mazur's Conjecture B, Stewart's conjecture seems out of reach. Indeed, it is not known whether the Mordell-Weil rank is bounded within a twist family, and if this is true, this is likely as difficult to prove as the corresponding result for *all* curves of a given genus.

Recently, I took interest in the quest to generalize height theory to the setting of *algebraic stacks*. The theory of heights is very robust when it comes to *schemes*, since after appropriate massaging one can always "embed" a scheme into an appropriate projective space, where the height theory is clear, then pull-back the height to the original scheme. However, this is not applicable when it comes to stacks. Indeed, until recently it was thought that a proper height theory for algebraic stacks simply cannot exist.

Ellenberg, Satriano, and Zuerick-Brown has recently proposed a bold new height theory for algebraic stacks, yet to be published. Their key idea is that if certain functorial properties of heights are dropped, then it is possible to extend heights to the setting of algebraic stacks, still with the critical Northcott property. Indeed, their theory of height on stacks allows one to unify two outstanding conjectures in number theory: Manin's conjecture on the density of rational points on Zariski-open subsets of Fano varieties, and Malle's conjecture on the number of number fields of bounded discriminant with prescribed degree and Galois group.

Ellenberg proposed, as an illustration of their work, the following example: consider the *stacky curve* $\mathcal{P}(1/2, 1/2, 1/2)$ consisting of $\mathbb{P}^1$ with the three points $\{0, 1, \infty\}$ replaced with "half-points", or alternatively, the classifying stack $\mathrm{B}(\mathbb{Z}/2\mathbb{Z})$. This is an algebraic stack which is not a scheme. Since this is set-theoretically equal to $\mathbb{P}^1$, a typical (integral) point can be parametrized in the usual way, given by a pair of co-prime integers (a, b). The height given by the ESZ-B height machine in this setting is then

$$H(a, b) = \mathrm{sqf}(a)\mathrm{sqf}(b)\mathrm{sqf}(a + b) \max\{|a|, |b|\}.$$

Here $\mathrm{sqf}(n)$ refers to n/k^2, where k^2 is the largest square dividing n. Ellenberg conjectures that $N(T)$, the integral points in $\mathcal{P}(1/2, 1/2, 1/2)$ with $H(a,b) \leq T$, is bounded by $O_\varepsilon\left(T^{1/2+\varepsilon}\right)$. In forthcoming work with B. Nasserden [11] we prove Ellenberg's conjecture and then some, indeed showing that $N(T) \asymp T^{1/2}(\log T)^3$.

New directions

As mentioned before, I am currently working on extending my earlier work with Lam and Schindler [9] to the setting of indefinite binary quadratic forms. This case differs from the definite case due to the presence of an infinite unit group. As such it is more appropriate to adapt the methods introduced by Heath-Brown and Moroz in [38] and [41] respectively, rather than the approach given in [33] and [9].

It is natural to ask whether then whether the result in [33], [40], and [9] hold for *binary cubic forms*, given [38] and [41]. Indeed, the bottleneck appears to be a result on the separation of fractions of the shape $\{v/d\}$ where v is a root of the congruence $F(x,1) \equiv 0 \pmod{d}$, with F an irreducible binary cubic form. This makes the cubic, and indeed for any higher degree form, very different as equidistribution results of such fractions are far weaker, due to lack of structure (in the quadratic case there is a wonderful connection to automorphic forms that provide the needed structure). Nevertheless, I hope to overcome this issue and show that binary cubic forms take on infinitely many primes even when one variable is restricted to be prime.

Another project, which is based on recent work with B. Nasserden [11], is to count the number of integral points on the "stacky" curve $\mathcal{P}(1/2, 1/2, 1/2)(\mathbb{Q})$ exactly, with respect to the Ellenberg-Satriano-Zuerick-Brown height. This problem is essentially about counting integral solutions to the Thue inequality $|F(x,y)| \leq T$ for totally reducible binary cubic forms F and sextic *Klein forms*; see [18] and [2] for background. The special shapes of these forms may allow one to count the number of integral points to the Thue inequality above with sufficient uniformity to obtain an asymptotic formula for the number of integral points on $\mathcal{P}(1/2, 1/2, 1/2)$ having bounded ESZ-B height.

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*, Journal de Théorie des Nombres de Bordeaux, (2) **31** (2019), 323-341.

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

[4] *On monic abelian cubics*, arXiv:1906.08625 [math.NT], submitted to Compositio Mathematica (16 pages).

Co-authored articles

[5] E. Knight, S. Y. Xiao, *On the ζ_3-Pell equation*, arXiv:1910.14097 [math.NT] (13 pages), submitted.

[6] B. Nasserden, S. Y. Xiao, *The density of integral points on $\mathbb{P}^1$ with three stacky points*, preprint.

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

[8] K. Lapkova, S. Y. Xiao, *The density of k-free values of polynomials II*, submitted.

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

[10] A. B. Miller, S. Y. Xiao, *Binary quadratic forms with discriminant* $1 - 4p$, preprint.

[11] B. Nasserden, S. Y. Xiao, *The density of rational points on a stacky $\mathbb{P}^1$ with three half points*, preprint.

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

[13] 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.

[14] C. Tsang, S. Y. Xiao, *Binary quartic forms with bounded invariants and small Galois groups*, Pacific Journal of Mathematics (1) **302** (2019), 249-291.

[15] C. Tsang, S. Y. Xiao, *The number of quartic D_4-fields with monogenic cubic resolvent ordered by conductor*, arXiv:1712.08552 [math.NT], to appear in Transactions of the American Mathematical Society (41 pages).

[16] S. Y. Xiao, S. Yamagishi, *Zeroes of polynomials in many variables with prime inputs*, Canadian Journal of Mathematics **72** (2020), 805-833.

Other references

[17] A. Altug, A. Shankar, I. Varma, K. Wilson, *The number of quartic D_4-fields ordered by conductor*, arXiv:1704.01729 [math.NT].

[18] M. A. Bennett, S. R. Dahmen, *Klein forms and the generalized superelliptic equation*, Ann. of. Math. **177** (2013), 171-239.

[19] M. A. Bennett, N. P. Dummigan, T. D. Wooley, *The representation of integers by binary additive forms*, Comp. Math., **111** (1998), 15-33.

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

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

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

[23] B. J. Birch, *Forms in many variables*, Proc. Roy. Soc. London Ser. A (1961/62), 245-263.

[24] T. D. Browning, *Power-free values of polynomials*, Arch. Math. (2) **96** (2011), 139-150.

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

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

[27] S. Chow, R. Dietmann, *Enumerative Galois theory for cubics and quartics*, Adv. Math. **372** (2020), 1-37.

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

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

[30] V. Dimitrov, Z. Gao, P. Habegger, *Uniformity in Mordell-Lang for curves*, arXiv:2001.10276 [math.NT].

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

[32] 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.

[33] E. Fouvry, H. Iwaniec, *Gaussian primes*, Acta. Arith. **79** (1997), 249-287.

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

[35] J. Friedlander, H. Iwaniec, *The polynomial X^2+Y^4 captures its primes*, Ann. of. Math. **148** (1998), 945-1040.

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

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

[38] D. R. Heath-Brown, *Primes represented by $x^3 + 2y^3$*. Acta Math. **186** (2001), 1-84.

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

[40] D. R. Heath-Brown, X. Li, *Prime values of $a^2 + p^4$*, Invent. Math. (2) **208** (2017), 441-499.

[41] D. R. Heath-Brown, B. Z. Moroz, *Primes represented by binary cubic forms*, Proc. Lond. Math. Soc. (3) **84** (2002), 257-288.

[42] C. Hooley, *On the number of divisors of quadratic polynomials*, Acta. Math. **110** (1963), 97-114.

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

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

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

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

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

[48] 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.

[49] M. Kim, *The motivic fundamental group of* $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ *and the theorem of Siegel*, Invent. Math. **161** (2005), 629-656.

[50] B. Lawrence, A. Venkatesh, *Diophantine problems and p-adic period mappings*, Invent. Math. **221** (2020), 893-999.

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

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

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

[54] W. M. Schmidt, *The density of integer points on homogeneous varieties*, Acta. Math. **154** (1985), 243-296.

[55] C. M. Skinner, T. Wooley, *Sums of two k-th powers*, J. reine angew. Math., **462** (1995), 57-68.

[56] A. Smith, 2^∞*-Selmer groups,* 2^∞*-class groups, and Goldfeld's conjecture*, arXiv:1702.02325 [math.NT].

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

[58] 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.

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