

The Circle Method for Algebraic Number Fields

Kyrie Johnson

December 15, 2023

Abstract

In this short expository note, we motivate and describe an application of circle method over an algebraic number field K . In particular, we describe the Hasse principle – a fundamental local-global principle in number theory – and highlight through example how recent work of [SS14] employs the circle method to study the Hasse principle. Finally, we briefly introduce some ideas from algebraic geometry, and discuss the way in which [SS14] characterizes an obstruction to the Hasse principle for a large family of varieties. We make an effort to phrase everything as accessibly as possible; a reader with either background in the circle method or background in algebraic number fields – and possibly neither – will hopefully get something out of this note.

Developed in the early 20th century, the Hardy-Littlewood circle method has found numerous applications over the past 100 years. From triumphs in additive number theory – such as Waring’s Problem and progress toward the Goldbach Conjecture – to triumphs in Diophantine analysis, the circle method has proven a useful and flexible technique. In this expository note, we discuss the latter applications to Diophantine analysis over algebraic number fields. That the circle method readily adapts to work over algebraic number fields is a testament to its general applicability, a phenomenon we hope to highlight.

Section 1 sets up the relevant definitions and provides context for subsequent more technical theorems. Section 2 discusses the simplest example of the circle method over algebraic number fields, drawing from the exposition in Browning. Finally, Section 3 provides a glimpse at some of the most general results in the area. Throughout this exposition, we leave technical proofs to their original papers, and instead favour examples/discussion which will prepare the reader to get the most out of the technical papers referenced herein.

1 Classical Definitions and Motivation

A fundamental idea in mathematics is the existence of local-global principles: when does local information piece together to provide coherent global information? The classical Chinese Remainder theorem is among the simplest examples of an algebraic local-global idea: the residues of an integer modulo various coprime pieces determine the residue of that integer modulo the pieces’ product. In the analysis of Diophantine equations, the relevant local-global principle is the Hasse principle.

1.1 The Hasse principle

We begin with a motivating example.

Example 1.1. Consider the Diophantine equation $f(x, y, z) = x^2 + y^2 - 3z^2 = 0$ which has rational coefficients. We argue by reduction modulo 3 that $f = 0$ has no nonzero solutions in \mathbb{Q} . Indeed, suppose that $x', y', z' \in \mathbb{Q}$ satisfy $f(x', y', z') = 0$. Then multiplication by a least common denominator yields $x, y, z \in \mathbb{Z}$ coprime such that $f(x, y, z) = 0$. Modulo 3, we get $x^2 \equiv -y^2$. Because -1 is not a square modulo 3, we conclude that $x^2, y^2 \equiv 0 \pmod{3}$ which in turn implies $x, y \equiv 0 \pmod{3}$. That both x and y are divisible by 3 contradicts their coprimality and we conclude no rational solutions to $f = 0$ exist.

The above example illustrates the following general technique for studying Diophantine equations: to show that an equation $f(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ has no nonzero solutions over \mathbb{Q} , it suffices to show that the corresponding equation has no nonzero solutions modulo some rational prime. In more technical language, for a field \mathbf{k} let $V(\mathbf{k}) \subset \mathbf{k}^n$ denote the set of zeros of f . Then $V(\mathbb{Q}) \subset \mathbb{Q}^n$ is nontrivial implies that $V(\mathbb{Q}_p) \subset \mathbb{Q}_p^n$ is nontrivial for all primes p . The contrapositive reads

if $V(\mathbb{Q}_p)$ is trivial for any one p , then $V(\mathbb{Q})$ is itself trivial.

The converse of this statement is called the Hasse principle, a fundamental local-global principle. We state it here in its more general formulation for reference, and provide the relevant algebraic definitions in the next section.

Definition 1.2. (The Hasse principle) Fix an algebraic number field K , and consider a polynomial equation $f(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ defined over K . Let $V(K)$ denote the zero set of f inside K^n and $V(K_\nu)$ the zero set of f inside K_ν^n for a finite or infinite prime ν . Then what conditions on K and/or f ensure that whenever $V(K_\nu)$ is nontrivial for all ν , $V(K)$ is itself nontrivial?

Before proceeding to the relevant algebraic number field definitions, we provide some examples of the Hasse principle for particular K and f .

Example 1.3. (a failure of the Hasse principle) Let $K = \mathbb{Q}$ and consider $f(x, y, z) = 3x^3 + 4y^2 + 5z^3 \in \mathbb{Z}[x, y, z]$. Then $V(\mathbb{Q}_p) \subset \mathbb{Q}_p^3$ is nontrivial for every prime p , yet $V(\mathbb{Q}) \subset \mathbb{Q}^3$ is trivial! For a proof, see section 4 of [Cas66].

Example 1.4. (Hasse principle for quadratic forms) Hasse showed that the Hasse principle holds for $K = \mathbb{Q}$ and f be a quadratic form (homogeneous of degree 2). Minkowski later extended the result to any number field K . A nice exposition for $K = \mathbb{Q}$ is [Gam06] and the Heath-Brown article [HB96] provides a proof via the circle method for the number of variables $n \geq 3$.

We will see throughout this note that a restriction on the number of variables is standard for results proven via the circle method.

1.2 Algebraic number field definitions

This section sets notation for algebraic number fields, and surveys a couple essential facts. The reader may reasonably choose to skip this section for now, and refer to it as necessary.

Let K/\mathbb{Q} denote a number field; that is, K is a finite-dimensional \mathbb{Q} -vector space. Then we let $\mathfrak{o}_K \subset K$ denote the subset of K whose elements are all roots of monic polynomials with *integer* coefficients. Beautifully, \mathfrak{o}_K has the structure of a ring and the integrality condition gives \mathfrak{o}_K the name “the ring of integers of K ”. Moreover, geometrically \mathfrak{o}_K may be regarded as a lattice inside K in the following sense: as an abelian group – i.e. as a \mathbb{Z} -module – \mathfrak{o}_K is finitely-generated with dimension equal to the degree of K/\mathbb{Q} , and a basis $\omega_1, \dots, \omega_d$ for \mathfrak{o}_K as a \mathbb{Z} -module also functions as a basis for K as a \mathbb{Q} -vector space.

Each prime ideal \mathfrak{p} inside \mathfrak{o}_K “lies over” a unique rational prime $p \in \mathbb{Z}$ in the sense that $\mathfrak{p} \cap \mathbb{Z} = (p)$. Moreover, the ring localization $(\mathfrak{o}_K)_{\mathfrak{p}}$ has field of fractions denoted by $K_{\mathfrak{p}}$, and it turns out that $(\mathfrak{o}_K)_{\mathfrak{p}}$ is the ring of integers inside $K_{\mathfrak{p}}$.

Example 1.5. For $K = \mathbb{Q}$, we have $\mathfrak{o}_K = \mathbb{Z}$ and the prime ideals of \mathfrak{o}_K are precisely the principal ideals (p) generated by prime numbers $p \in \mathbb{Z}$. The localisation $\mathbb{Z}_{(p)}$ is denoted more simply by \mathbb{Z}_p , and is called the ring of p -adic integers. The fraction field \mathbb{Q}_p of \mathbb{Z}_p is the field of p -adic numbers; the suggestive notation reflects that \mathbb{Q}_p is topologically isomorphic to the completion of \mathbb{Q} with respect to the so-called p -adic topology. In this sense, the real numbers are a completion \mathbb{Q}_{∞} of \mathbb{Q} at a sort of “infinite place” while the \mathbb{Q}_p are completions at “finite places” p .

The idea of localization provides an algebraic formalism for the local-global principle discussed in the previous section. Indeed, one can often translate statements for the various “local fields” $K_{\mathfrak{p}}$ into a statement for the “global” field K – for $K = \mathbb{Q}$, this says that the arithmetic of \mathbb{Q}_p for varying p tells us something about the arithmetic of \mathbb{Q} .

Now, the preceding discussion applies to a single extension K/\mathbb{Q} . But to apply the circle method over algebraic number fields, we will need a natural way of passing between algebraic number fields in a tower $L/K/\mathbb{Q}$ of \mathbb{Q} -vector spaces. Enter the norm and trace maps!

Definition 1.6. (Field norm and trace) Let L/K be a finite extension of number fields of degree d , so that L has the structure of a K -vector space. Then for an element $\alpha \in L$, multiplication by α determines a linear transformation $M_{\alpha} : L \rightarrow L$ of K -vector spaces. Then the trace of M_{α} is called the trace of α , denoted $\text{Tr}_{L/K}(\alpha) \in K$. Likewise, the determinant of M_{α} is called the norm of α , denoted $N_{L/K}(\alpha)$. The field trace inherits the additivity of the trace for linear transformations, and the field norm inherits the multiplicativity of the determinant.

The norm and trace are fundamental ways of associating an element of a larger field L with an element of the base field K . Moreover, norms and traces play well with the rings of integers: $\text{Tr}_{L/K}(\mathfrak{o}_L) \subset \mathfrak{o}_K$ and $N_{L/K}(\mathfrak{o}_L) \subset \mathfrak{o}_K$

We finish this section by collecting two definitions we will reference later.

Definition 1.7. (Duals) The dual $\widehat{\mathfrak{o}_K}$ of the ring of integers \mathfrak{o}_K (with respect to the trace) is defined by

$$\widehat{\mathfrak{o}_K} = \{\alpha \in K : \text{Tr}(\alpha x) \in \mathbb{Z} \text{ for all } x \in \mathfrak{o}_K\}.$$

Then $\widehat{\mathfrak{o}_K}$ has basis ρ_1, \dots, ρ_d with the ρ_i determined by

$$\mathrm{Tr}(\rho_i \omega_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise.} \end{cases}$$

Definition 1.8. (Relative cubic norm forms) For a cubic extension L/K of number fields, let η_1, η_2, η_3 denote a basis for L as a K vector space. We define the relative cubic norm form of L/K by

$$N_{L/K}(x_1, x_2, x_3) = N_{L/K}(x_1\eta_1 + x_2\eta_2 + x_3\eta_3).$$

2 The Story for Cubic Forms

We saw in example 1.4 that the analysis of global roots – that is, roots in K – of quadratic forms is well understood over arbitrary number fields. It is natural to next increase the degree by 1 and consider cubic forms (homogeneous of degree 3). We generally follow the exposition in chapter 4 of [Bro21], using the same notation for ease of translation.

Let K/\mathbb{Q} be a number field of degree d with ring of integers \mathfrak{o}_K . Further, let $f \in \mathfrak{o}_K[x_1, \dots, x_n]$ be a cubic form. Then there are two broad strategies for considering the zero set of f :

1. Use an algebraic tool – such as the field trace or norm – to transfer zeros of f over K to zeros of a system of d cubic forms over \mathbb{Q} . Then apply the original Hardy-Littlewood circle method to the system.
2. Adapt the Hardy-Littlewood circle method to apply directly to the cubic form f .

Strategy 1 has an important limitation, which the next theorem demonstrates.

Theorem 2.1. *With notation as above, consider f non-singular and $n \geq 8d + 9$. Then there exists a constant $c_{f,K}$ such that*

$$\#\{x \in (\mathfrak{o}_K)^n : f(\mathbf{x}) = 0, |\mathbf{x}| \leq X\} = c_{f,K} X^{n-3} + \text{smaller-}O\text{-term}$$

where $|x| = \max_i |x_i|$.

Proof. We outline the proof argument for illustrative purposes, and refer to [Bro21] and [Bir57] for details. As in strategy 1, the proof has two steps.

Step 1: Let $\omega_1, \dots, \omega_d$ denote a basis for \mathfrak{o}_K over \mathbb{Z} . Then a zero $a \in (\mathfrak{o}_K)^n$ may be expressed in terms of the chosen basis,

$$a = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,d} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,d} \\ \vdots & & & \vdots \\ c_{n,1} & c_{n,2} & \cdots & c_{n,d} \end{bmatrix} \begin{bmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_d \end{bmatrix}$$

where $c_{i,j} \in \mathbb{Z}$. Then Birch shows that the equation $f(a) = 0$ is equivalent to the system of d equations $f_k(c_{1,k}, \dots, c_{n,k}) = 0$ over \mathbb{Q} . In particular, $f_k \in \mathbb{Z}[x_1, \dots, x_n]$ has coefficients in \mathbb{Z} which arise from taking the trace from K down to \mathbb{Q} .

Step 2: Apply [Bir57]: for a system of cubic forms with rational coefficients, an asymptotic for the count of zeros in a box can be obtained as long as

$$\text{total \# of variables} \leq d + 8d(d + 1).$$

Note that Birch proves the above statement via the Hardy-Littlewood circle method over \mathbb{Q} . Now, for a system of d forms in n variables each, we have (total # of variables) = dn , so we require

$$dn \geq d + 8d(d + 1) \iff n \geq 8d + 9.$$

□

In fact, in [Bir57] Birch handles general systems of odd degree forms in n variables: the lower bound $n \geq 8d + 9$ is replaced with a lower bound depending both on $d = \deg(K/\mathbb{Q})$ as well as the degrees of the forms. Either way, the crucial limitation in strategy 1 is that it produces results which require the number of variables to grow as the degree(s) of the forms grow. As we saw in Step 2 above, the limitation comes from translating statements over K to a system of statements over \mathbb{Q} , where we have increased the number of variables d -fold.

Strategy 2 overcomes the number field degree d limitation by applying the circle method directly; the below table collects benchmark results, which apply for any number field K/\mathbb{Q} of degree d .

Year	Mathematician(s)	Applicable Form(s)	$n \geq _$	Resource
1961	Birch	the diagonal cubic	9	[Bir61]
1975	Pleasants	(non-singular) cubic	16	[Ple75]
1994	Skinner	(non-singular) cubic	13	[Ski94]
2014	Browning, Vishe	(non-singular) cubic	10	[BV14]

So far in this section we've overlooked our motivation from the Hasse principle, and have instead looked at direct studies of global zero sets (without using local information). The techniques of direct application of the circle method – developed in large part by Birch, Pleasants, and Skinner — culminated in 2014 in two ways, not only in the above-tabulated work of Browning and Vishe but also in the work [SS14] of Schnidler and Skorobogatov. The algebraic importance of [SS14] lies in its characterisation of when the Hasse principle holds for a large family of forms. Roughly following chapter 4 of [Bro21], we next discuss the simplest example of the main theorem of [SS14] and return to a more general discussion in section 3.

2.1 Example: direct application of the circle method over K

For notational simplicity, we consider a totally real number field K/\mathbb{Q} of degree d with ring of integers \mathfrak{o}_K (rather than a general number field, though the discussion is analogous). As before, $\omega_1, \dots, \omega_d$ denotes a basis of \mathfrak{o}_K over \mathbb{Z} . Because K is totally real, we have $\omega_1, \dots, \omega_d \in \mathbb{R}$ and they determine a basis for the \mathbb{R} -vector space $V = K \otimes_{\mathbb{Q}} \mathbb{R}$. In this section, we will consider an explicit cubic form $f \in \mathfrak{o}_K[x_1, \dots, x_9]$ which we now define – in particular, note $n = 9$.

Let L_1, L_2 , and L_3 be cubic extensions of K and let $b_1, b_2, b_3 \in \mathfrak{o}_K$ be nonzero. Then we consider

$$f(x_1, \dots, x_9) = b_1 N_{L_1/K}(x_1, x_2, x_3) + b_2 N_{L_2/K}(x_4, x_5, x_6) + b_3 N_{L_3/K}(x_7, x_8, x_9),$$

where $N_{L_i/K}$ is the cubic norm form defined in definition 1.8. Then the main result of [SS14] answers the Hasse principle for this cubic norm form in 9 variables: it gives local conditions for zeros which guarantee a nontrivial $x \in (\mathfrak{o}_K)^9$ such that $f(\mathbf{x}) = 0$.

Theorem 2.2. [SS14] *Let K be totally real with f the cubic form in 2.1. If f has a (non-singular) real solution in each of the d real embeddings of $F \hookrightarrow \mathbb{R}$ and (non-singular) solutions in $(\mathfrak{o}_K/\mathfrak{p})^9$ for each finite prime \mathfrak{p} , then f has a nontrivial zero in $(\mathfrak{o}_K)^9$. That is, the Hasse principle holds for f over K .*

We will outline the proof of theorem 2.6 with an emphasis on both the elements that are similar to the circle method over \mathbb{Q} , as well as those that are different.

Let $\mathbf{x} = (\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3)$ for

$$\mathbf{x}_1 = (x_1, x_2, x_3), \mathbf{x}_2 = (x_4, x_5, x_6), \mathbf{x}_3 = (x_7, x_8, x_9)$$

so that $f(\mathbf{x}) = b_1 N_1(\mathbf{x}_1) + b_2 N_2(\mathbf{x}_2) + b_3 N_3(\mathbf{x}_3)$. Then for $\mathbf{u} = (u_1, \dots, u_9) \in V^9$ and fixed $\kappa > 0$, we define real variables x_{ij} and u_{ij} by

$$x_i = \sum_{k=1}^d x_{ik} \omega_k \text{ and } u_i = \sum_{k=1}^d u_{ik} \omega_k$$

and consider the box

$$\mathcal{B}(\mathbf{u}, \kappa) = \{ \mathbf{u} \in V^9 \text{ s.t. } |x_{ik} - u_{ik}| \leq \kappa, \forall i, k \}.$$

Via the circle method, one can determine asymptotics for the number of integral points up to κB for some real number B :

$$N(\mathcal{B}, B) = \# \{ \mathbf{x} \in (\mathfrak{o}_K)^9 \cap B\mathcal{B} \text{ with } f(\mathbf{x}) = 0 \}.$$

2.1.1 From points in a box to exponential sums

As in definition 1.7, we consider the dual $\widehat{\mathfrak{o}_K}$ of \mathfrak{o}_K with dual basis ρ_1, \dots, ρ_d . To a number field K , one often studies the associated Minkowski space $V = K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^d$. Because K is totally real, we may identify K with its image in V via its real embeddings. Under this embedding $K \hookrightarrow V$, the basis ρ_1, \dots, ρ_d for K determines a basis for V as an \mathbb{R} vector space and we may write

$$V = \{ x_1 \rho_1 + \dots + x_d \rho_d \text{ with } x_i \in \mathbb{R} \}.$$

Now, we define a measure on V by taking $d\mathbf{v} = dx_1 \cdots dx_d$, where dx_i is the standard \mathbb{R} -Lebesgue measure on the i^{th} component of \mathbb{R}^d . Then the map

$$e : V \rightarrow \mathbb{C} \\ v \mapsto \exp(2\pi i \text{Tr}(v))$$

serves as the appropriate additive character in this setting. Indeed, we have an analogous integral result over the circle $\mathbb{T} = \{ x_1 \rho_1 + \dots + x_d \rho_d \text{ s.t. } x_i \in [0, 1] \}$.

Lemma 2.3. For any $u \in \mathfrak{o}_K$,

$$\int_{\mathbb{T}} e(\alpha u) d\alpha = \begin{cases} 1 & \text{if } u = 0 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Unwrap the definitions, noting throughout that the trace transfers the setting from K down to \mathbb{Q} . Then apply the classical identity over \mathbb{Q} for integers n ,

$$\int_0^1 e(\alpha n) d\alpha = \begin{cases} 1 & \text{if } n = 0 \\ 0 & \text{otherwise.} \end{cases}$$

For details, see lemma 4.2 of [Bro21]. □

As in the classical setting over \mathbb{Q} , the circle integral of lemma 2.3 allows us to interpret the point count $N(\mathcal{B}, B)$ as an integral of exponential sums: for

$$S_j(\alpha) = \sum_{\mathbf{x}_j \in (\mathfrak{o}_K)^3 \cap B\mathcal{B}} e(\alpha b_j N_j(\mathbf{x}_j)),$$

we have

$$N(\mathcal{B}, B) = \int_{\mathbb{T}} S_1(\alpha) S_2(\alpha) S_3(\alpha) d\alpha.$$

2.1.2 Major and minor arcs

As in the classical circle method over \mathbb{Q} , one proceeds to split the integral over \mathbb{T} into major arcs \mathfrak{M} and minor arcs \mathfrak{m} :

$$\int_{\mathbb{T}} = \int_{\mathfrak{M}} + \int_{\mathfrak{m}}.$$

The formal definition of \mathfrak{m} and \mathfrak{M} is analogous to the classical setting, and we defer the reader to section 4.2 of [Bro21] for details. Suffice it to say that the major arcs $\mathfrak{M} = \mathfrak{M}_B(B, \Delta)$ are the subset of \mathbb{T} which can be well-approximated by rational numbers with “sufficiently-small” denominator relative to the parameters $B, \Delta > 0$. As above, we will think of B as growing toward infinity, while Δ will be some small parameter satisfying $\Delta < \min\{1, 3/2d\}$. As always, the minor arcs are $\mathfrak{m} = \mathbb{T} - \mathfrak{M}$.

Then lemma 4.7 of [Bro21] concludes

Lemma 2.4.

$$\int_{\mathfrak{m}} |S_1(\alpha) S_2(\alpha) S_3(\alpha)| d\alpha = O(B^{6d - \Delta/(9d)})$$

for the minor arcs, and lemma 4.8 of [Bro21] concludes

Lemma 2.5.

$$\int_{\mathfrak{M}} S_1(\alpha) S_2(\alpha) S_3(\alpha) d\alpha = \mathfrak{S}(B^\Delta) J(B^\Delta) B^{6d} + O(B^{6d - 1 + 2\Delta(d+1)})$$

for the major arcs, where $\mathfrak{S}(P)$ is the partial sum

$$\mathfrak{S}(P) = \sum_{q \leq P} \sum_{\mathbf{a} \in (\mathbb{Z}/q\mathbb{Z}^*)^d} q^{-9d} S_{\mathbf{a},q}$$

of the ‘‘singular series’’ and $J(P)$ is the partial integral

$$J(P) = \int_{|\gamma| \leq P} \int_{\mathcal{B}} e(\gamma_1 f_1(\mathbf{t}) + \cdots + \gamma_d f_d(\mathbf{t})) d\mathbf{t} d\gamma$$

of the ‘‘singular integral’’. Analogous to the classical case, $S_{\mathbf{a},q}$ denotes a sort of Gauss sum, taken over the residues modulo the denominator q .

In particular, we note that the major arcs constitute a main term (pending analysis of the singular series and singular integral) while the minor arcs contribute to the error term. Analysis of the singular integral is analogous to the classical case, and details can be found in Section 4.3 of [Bro21]. Putting everything together, one has

Theorem 2.6. *Let K/\mathbb{Q} be totally real of degree d , and suppose that the cubic norm form f defined above is non-singular in \mathcal{B} . Then there exists a constant σ_∞ and $\delta > 0$ such that*

$$N(\mathcal{B}, B) = \sigma_\infty \mathfrak{S} B^{6d} + O(B^{6d-\delta})$$

where

$$\mathfrak{S} = \sum_{q=1}^{\infty} \sum_{\mathbf{a} \in (\mathbb{Z}/q\mathbb{Z}^*)^d} q^{-9d} S_{\mathbf{a},q}$$

is the singular series. Moreover,

- $\sigma_\infty > 0$ if the equation $f(\mathbf{x}) = 0$ has a non-singular solution in \mathcal{B} ; and
- $\mathfrak{S} > 0$ if the equation $f(\mathbf{x}) = 0$ has a non-singular solution in $(\mathfrak{o}_K)_{\mathfrak{p}}^9$ for every prime \mathfrak{p} .

In particular, the last two bullets account for the appearance of the Hasse principle: (non-singular) zeros at all infinite and finite places guarantee that the main term has a positive coefficient which in turn guarantees (infinitely-many!) zeros over \mathfrak{o}_K .

For a full treatment of the singular series, we refer the reader to section 4.4 of [Bro21]. To highlight the role of the Hasse principle – our motivation – we discuss the proof of the second bullet point next.

2.1.3 The singular series and the Hasse principle

Factorisation is a fundamental feature of local-global principles in number theory. In its most classical form, this is the Chinese Remainder Theorem: for $n = p_1^{e_1} \cdots p_r^{e_r}$ with each p_i prime, one has

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_{i=1}^r \mathbb{Z}/p_i^{e_i}\mathbb{Z}.$$

Modern formulations are often phrased adelicly (for example, see weak and strong approximation in section 2.5 of [GH19]) but the spirit of products remains. We find the same phenomenon here, even within the context of an analytic tool like the circle method.

Lemma 2.7. *The singular series \mathfrak{S} factors as $\mathfrak{S} = \prod_{\mathfrak{p}} \sigma_{\mathfrak{p}}$ where, for a finite prime \mathfrak{p} lying over $p \in \mathbb{Z}$, we define*

$$\sigma_{\mathfrak{p}} = \lim_{l \rightarrow \infty} p^{-8l} D(\mathfrak{p}_i, l)$$

with local point counts

$$D(\mathfrak{p}_i, l) = \# \{ \mathbf{x} \in (\mathfrak{o}_K / \mathfrak{p}_i^l)^9 \text{ s.t. } f(\mathbf{x}) \equiv 0 \pmod{\mathfrak{p}_i^l} \}.$$

Thus, showing that $\mathfrak{S} > 0$ whenever local solutions exist amounts to showing that $\sigma_{\mathfrak{p}} > 0$ whenever $f(\mathbf{x}) = 0$ has a non-singular solution in $(\mathfrak{o}_K / \mathfrak{p})^9$. Indeed, once one has a single (non-singular) solution modulo \mathfrak{p} , arithmetic modulo \mathfrak{p} allows one to construct $p^{8(l-2\delta-1)}$ distinct “perturbed” solutions. Then the local point count satisfies the lower bound $D(\mathfrak{p}, l) \geq p^{8(l-2\delta-1)}$, thereby yielding $\sigma_{\mathfrak{p}} > 0$. So we have the second bullet of 2.6.

3 A Glimpse at the General

We conclude this expository note by briefly discussing the main theorem of [SS14], of which theorem 2.6 is the simplest example. For this, we begin with a general discussion of algebraic geometry.

3.1 A brief primer on varieties

So far we’ve considered zero sets $\{f(\mathbf{x}) = 0\}$ for some homogeneous polynomial f . In the language of algebraic geometry, such a zero set is called a projective variety. One then says that a (projective) variety X defined by a (homogeneous) polynomial f is defined over a field K if the coefficients of f lie in K .

The convenience of the formalism of a variety lies in its ability to readily shift between fields. Indeed, above we considered the zero sets of $f \in K[x_1, \dots, x_n]$ for various localizations K_{ν} of K . In the language of varieties, zero sets for shifting fields are concisely packaged into the notation $X(F_{\nu})$ and the Hasse principle is written concisely as

$$X(K_{\nu}) \neq 0 \text{ for all primes } \nu \implies X(K) \neq 0.$$

The main theorem of [SS14] proves the Hasse principle in this algebra-geometric language.

3.2 The Brauer-Manin obstruction

Precisely, Schindler and Skorobogatov show

Theorem 3.1. *([SS14]) Fix a number field extension L/K of degree d and let η_1, \dots, η_d denote a basis of L as a K vector space. Let X be the variety defined by the equation*

$$\prod_{i=1}^{2r} L_i^{e_i}(\mathbf{x}) - cN(\mathbf{z}) \in K[\mathbf{x}, \mathbf{z}]$$

in $r + d$ variables $\mathbf{x} = (x_1, \dots, x_r)$ and $\mathbf{z} = (z_1, \dots, z_d)$, where

$$N(\mathbf{z}) = N_{K/F}(z_1\eta_1 + \dots + z_d\eta_d)$$

is the norm form and $L_1(\mathbf{x}), \dots, L_{2r}(\mathbf{x})$ are “sufficiently general” linear polynomials. Then the only obstruction to the Hasse principle for X is the Brauer-Manin obstruction. Moreover, if $X(K) \neq \emptyset$ then $X(K)$ is large in a precise sense.

As such, the main theorem of section 2.1 above is but one case in a much more general theory. Note that the phenomenon noted parenthetically after 2.6 – namely, that the existence of just one solution over K implies the existence of many – holds quite generally!

It remains to say something about the mysterious “Brauer-Manin obstruction”. A precise statement is technical and beyond the scope of this short paper; see [Man] for details. For a variety X , the Brauer-Manin obstruction relates to the existence of non-trivial class in the so-called Brauer group of X which is a subgroup of the second (étale) cohomology group $H_{\text{ét}}^2(X, \mathcal{O}_X^*)$ of X (see [uh20]). In particular, there is a general phenomenon at play: non-trivial cohomology classes often represent obstructions to performing a desired construction, in this case the construction of a zero.

4 Concluding Remarks

The Hasse principle for Diophantine equations is a fundamental local-global principle in number theory. We have seen – in imprecise terms – that the 2014 work of Schindler and Skorobogatov provides a rather general characterisation of when the Hasse principle fails for a slew of algebraic varieties over a general number field K . We have also seen – in more precise terms – the manifestation of their work for a particular example. In either case, the circle method over K plays a crucial role. Indeed, the adaptability of the circle method is what makes it such a powerful tool.

References

- [Bir57] BJ Birch. Homogeneous forms of odd degree in a large number of variables. *Mathematika*, 4(2):102–105, 1957.
- [Bir61] BJ Birch. Waring’s problem in algebraic number fields. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 57, pages 449–459. Cambridge University Press, 1961.
- [Bro21] Tim Browning. *Cubic forms and the circle method*, volume 343. Springer, 2021.
- [BV14] TD Browning and Pankaj Vishe. Cubic hypersurfaces and a version of the circle method for number fields. 2014.
- [Cas66] John William Scott Cassels. Diophantine equations with special reference to elliptic curves. *Journal of the London Mathematical Society*, 1(1):193–291, 1966.

- [Gam06] Adam Gamzon. The hasse-minkowski theorem. 2006. Available at https://digitalcommons.lib.uconn.edu/srhonors_theses/17/.
- [GH19] Jayce R Getz and Heekyoung Hahn. An introduction to automorphic representations with a view towards trace formulae. *Graduate Studies in Mathematics*, 6, 2019.
- [HB96] DR Heath-Brown. A new form of the circle method, and its application to quadratic forms. 1996. Available at <https://core.ac.uk/download/pdf/96603.pdf>.
- [HBS02] Roger Heath-Brown and Alexei Skorobogatov. Rational solutions of certain equations involving norms. 2002.
- [Man] Shelly Manber. The brauer-manin obstruction. Available at <https://math.berkeley.edu/~shellym/BrauerManin.pdf>.
- [Ple75] PAB Pleasants. Cubic polynomials over algebraic number fields. *Journal of Number Theory*, 7(3):310–344, 1975.
- [Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.
- [Ski94] Christopher M Skinner. Rational points on nonsingular cubic hypersurfaces. 1994.
- [SS14] Damaris Schindler and Alexei Skorobogatov. Norms as products of linear polynomials. *Journal of the London Mathematical Society*, 89(2):559–580, 2014.
- [uh20] user267839 (<https://mathoverflow.net/users/108274/user267839>). Co-homological brauer group vs classical. MathOverflow, 2020. URL:<https://mathoverflow.net/q/365433> (version: 2020-07-11).