DEGREES OF POINTS ON IRREDUCIBLE HYPERSURFACES

LEA BENEISH AND ANDREW GRANVILLE

Abstract. We study the set of D such that a given irreducible hypersurface C of degree d has infinitely many points of degree D over $\mathbb{Q}$. We give a new explicit proof that this set contains all (positive) multiples of the index of C with finitely many exceptions. When D is sufficiently large and divisible by the index of C, we show there are $\gg x^{1/2d^2-\epsilon}$ distinct fields with degree D and discriminant $\le x$ containing new non-singular points on C. Our proof relies on (what we define to be) the index of the Newton polytope $H(C)$ for C which we use as combinatorial proxy for the index of C. We conjecture that for almost all C with a given Newton polytope H, the index of H equals the index of C and we prove this conjecture for a positive proportion of curves with $H(C) = H$. As an application of our techniques, we prove half of Bhargava's conjecture on the least odd degree of points on a typical hyperelliptic and we recover Springer's theorem and a related statement for rational points on cubic hypersurfaces.

1. Introduction

Understanding and quantifying algebraic points on curves, surfaces and more generally higher dimensional varieties, is a fundamental subject of study in Diophantine geometry. Here we develop a relationship between the degrees of non-singular algebraic points on a given hypersurface and its "shape".

Let $C = C_f$ be an irreducible hypersurface given by the projective equation

$$f(x_1, \dots, x_m) = 0$$

(so that $m \ge 3$) defined over a number field K. Let $\mathcal{F}(C)$ denote the set of fields L for which C has *new points*, that is, non-singular L-rational points that do not belong to a subfield of L, and define

$$D_K(C) := \{n \ge 1 : \ \exists\ L \in \mathcal{F}(C) \text{ with } [L : K] = n\},$$

the set of degrees of the fields in $\mathcal{F}(C)$ over K. We also define $D_K(C)^{\inf}$ to be the set of integers n for which there are infinitely many fields L in $\mathcal{F}(C)$ of degree n over K.

When we have a fixed number field K we will omit the subscript K and write $D(C)$. Throughout we will take $K = \mathbb{Q}$ for simplicity though our results should hold for all number fields K via minor and expected modifications of the same proofs. Let

$$G(C) := \gcd_{n \in D(C)} n$$

be the *index* of C,[1] so that if $n \in D(C)$ then $G(C)$ divides n. The converse is almost true:

Theorem 1.1. *There exists a finite set of integers $\mathcal{E}(C)$ such that*

$$D(C)^{\inf} = G(C)\mathbb{Z}_{\ge 1} \setminus \mathcal{E}(C)$$

[1]The index is often defined to be the least positive degree of a K-rational divisor on C, though it is well-known that these definitions are equivalent.

In other words, the set of exceptions,

$$\mathcal{E}(C) := \{n \geq 1 : G(C) \text{ divides } n \text{ and } n \notin D(C)^{\inf}\},$$

is finite and so if n is sufficiently large then $n \in D(C)^{\inf}$ if and only if $G(C)$ divides n.

Clark, Milosevic and Pollack [4, Theorem 2.4] proved that the set of degrees for which there are new points is of the form $G(C)\mathbb{Z}_{\geq 1} \setminus \mathcal{E}(C)$ for any "nice" variety of positive dimension over a Hilbertian field K of characteristic zero. One can then deduce (the stronger) Theorem 1.1 for curves of genus > 1 by an application of Faltings' Theorem.

Our proof of Theorem 1.1 is for all irreducible hypersurfaces and gives an explicit lower bound on the number of fields $L \in \mathcal{F}(C)$ with $[L : K] = n$ of discriminant $\leq x$ for each sufficiently large $n \in D(C)^{\inf}$.

The basic idea of both proofs is linear algebra, in ours (see section 4) we explicitly construct solutions whereas [4, Theorem 2.4] used the Riemann-Roch theorem to show the existence of points of these degrees. Our proof of Theorem 1.1 allows us to give an explicit lower bound on the number of fields generated by points on hypersurfaces and in the case of curves, to be explicit about what $\mathcal{E}(C)$ is.

1.1. **General quantitative results.** For those degrees for which there are infinitely many points of degree D, we quantify them as suggested by Mazur, Rubin and Larsen in [10] by giving a lower bound on the number of fields generated by points of degree D.

Theorem 1.2. *Let C be an irreducible hypersurface given by a polynomial f in m variables with integer coefficients, of degree d. Fix $\epsilon > 0$. If D is divisible by $G(C)$ and is sufficiently large, and X is sufficiently large then*

$$\#\{\text{Fields } K \in \mathcal{F}(C) : [K : \mathbb{Q}] = D \text{ and } \operatorname{disc}(K/\mathbb{Q}) \leq X\} \gg X^{\frac{1}{2d^2}-\epsilon}.$$

In Theorem 2.1 we will prove a stronger result with "$\frac{1}{2d^2}$" replaced by some exponent $\operatorname{Exp}(C)$, and we prove that $\operatorname{Exp}(C) \geq \max_j \frac{1}{2(\deg_{x_j} f)^2} \geq \frac{1}{2d^2}$.

The best upper bound known [13] on the number of field extensions of degree D is

$$\#\{\text{Field extensions } K/L : [K : L] = D \text{ and } \operatorname{disc}(K/L) \leq X\} \ll_{L,D} X^{2(\log D)^2}$$

(where the constant "2" can be improved); it is believed that the correct quantity is $\sim c_{L,D}X$.

We can be more explicit about $D(C_f)^{\inf}$ when there is a non-singular rational point on C. The *Frobenius set* generated by given positive integers $a_1, \dots, a_k$ is

$$\operatorname{Frob}(a_1, \dots, a_k) := \{a_1n_1 + \cdots + a_kn_k : n_1, \dots, n_k \in \mathbb{Z}_{\geq 0}\}.$$

Then we have the following:

Theorem 1.3. *Let C be an irreducible hypersurface given by a polynomial in m variables with integer coefficients, of degree d and suppose that C has a non-singular rational point. Then $G(C_f) = 1$ and $D(C_f)^{\inf} \supset d^2 + \operatorname{Frob}(d-1, d)$ so that $\mathcal{E}(C_f) \subset \{1, \dots, 2d^2 - 3d + 1\}$.*

Remark 1.4. If C is a curve with no singular points then C has genus $g = \frac{(d-1)(d-2)}{2}$. Theorem 1.3 implies that if C has a rational point then there are infinitely many (non-singular) points of degree D on C, for every $D \geq 2g + d^2$.

1.2. **A combinatorial proxy for the index.** For a given irreducible hypersurface C_f it is difficult to determine the index explicitly. If C_f is given by the projective equation

$$f(x_1,\dots,x_m)=\sum_{(i_1,\dots,i_m)\in I_f} c_{i_1,\dots,i_m}x_1^{i_1}\cdots x_m^{i_m} \tag{1.1}$$

and if d is the degree of f then

$$I_f\subset \mathcal{M}_{m,d}:=\{\mathbf{i}=(i_1,\dots,i_m)\in\mathbb{Z}_{\geq 0}^m : i_1+\cdots+i_m=d\},$$

and for each $j, 1\leq j\leq n$ there exists $\mathbf{i}\in I_f$ with $i_j=0$. Let H_f be the *Newton polytope* of f, which is the set of corners of I_f, where we define $\mathbf{h}\in I_f$ to be a *corner* of I_f if there exists $\mathbf{v}\in\mathbb{Z}_{\geq 0}^m$ for which

$$\mathbf{h}\cdot\mathbf{v}>\mathbf{i}\cdot\mathbf{v} \text{ for all } \mathbf{i}\in I_f, \mathbf{i}\neq\mathbf{h}.$$

For each $\mathbf{h}=(h_1,\dots,h_m)\in\mathcal{M}_{m,d}$ define $g(\mathbf{h}):=\gcd(h_1,\dots,h_m)$.

Let $\mathcal{H}_{m,d}$ be the set of non-empty subsets H of $\mathcal{M}_{m,d}$ for which every element of H is a corner of H and, for each $j=1,\dots,m$, there exist $\mathbf{h},\mathbf{i}\in H$ with $h_j=0<i_j$. For each $H\subset\mathcal{H}_{m,d}$, define

$$G(H):=\gcd_{\mathbf{h}\in H} g(\mathbf{h});$$

in other words, $G(H)$ is the gcd of all of the co-ordinates of all the elements of H. In section 3.2 we will define a finite set $\mathcal{E}(H)$ of integer multiples of $G(H)$.

We begin by showing how $D(C_f)^{\inf}$ is related to $D(H_f)^{\inf}$:

Theorem 1.5. *For any given $f(x_1,\dots,x_m)\in\mathbb{Z}[x_1,\dots,x_m]$ we have*

$$G(C_f) \text{ divides } G(H_f);$$

and if $G(C_f)=G(H_f)$ then $\mathcal{E}(C_f)\subset\mathcal{E}(H_f)$.

1.3. **A conjecture: More than a proxy.** Our main claim is that $D(C)^{\inf}$ usually depends *only* on its Newton polytope, H_f:

Conjecture 1.6. *For almost all f with $H_f=H$ (where the f are ordered by the size of their coefficients, which* all *vary) we have*

$$G(C_f)=G(H) \text{ and } \mathcal{E}(C_f)=\mathcal{E}(H).$$

In other words, $D(C_f)^{\inf}$ is typically entirely determined *by H_f.*

We will prove this conjecture for (twisted) hyperelliptic curves $by^2=g(x)$ of even degree d. This curve can be written as $by^2=\sum_{i=0}^d g_ix^i$ with $g_d\neq 0$ in affine form and therefore homogenizes to

$$f_g(x,y,z):=\sum_{i=0}^d g_ix^iz^{d-i}-by^2z^{d-2}=0$$

so that $I_f\subset I_d:=\{(0,2,d-2)\}\cup\{(i,0,d-i):0\leq i\leq d)\}$. If $g(0)\neq 0$ then $H_f=H:=\{(0,2,d-2),(0,0,d),(d,0,0)\}$ so that $G(H_f)=2$. If $g(0)=0$ and $x^2\nmid g(x)$ (so that the point $(0,0)$ is non-singular) then evidently $G(C_f)=1$.

Theorem 1.7. *Fix even integer $d\geq 2$ and $H:=\{(0,2,d-2),(0,0,d),(d,0,0)\}$. Let C_{f_g} be the hyperelliptic curve $by^2=g(x)$ where $g(x)\in\mathbb{Z}[x]$ has degree d.*

(a) *For almost all $g(x)\in\mathbb{Z}[x]$ of even degree d with $g(0)\neq 0$ we have $G(C_{f_g})=G(H)=2$ and $D(C_f)^{\inf}=2\mathbb{Z}_{\geq 1}$.*

(b) *If there is a non-singular rational point on* C_f *then* $D(C_f)^{\inf} = \mathbb{Z}_{\geq 1} \backslash \mathcal{E}(C_f)$ *where* $\mathcal{E}(C_f) \subset \{1, 3, 5 \ldots, d-3\}$.

Since $g(0) \neq 0$ for almost all polynomials $g(x)$, we deduce from (a) that almost all hyperelliptic curves $by^2 = g(x)$ have infinitely many algebraic points of every even degree, but no algebraic points of odd degree. In particular they have no rational points.

If $g(x)$ has odd degree d then let $G(t) = t^{d+1}g(1/t)$, which has (even) degree $d+1$, and then there is a bi-rational transformation between the algebraic points of $y^2 = g(x)$ and those of $Y^2 = G(X)$. Now $Y^2 = G(X)$ has the non-singular rational point at $(0, 0)$, and so we apply Theorem 1.7(b).

We prove Theorem 1.7(a) in section 10.1, and Theorem 1.7(b) in section 8.1 as well as some generalizations.

Our conjecture holds for a positive proportion of curves f with $I_f = I$, for most I:

Theorem 1.8. *Fix integer* $m \geq 1$ *and assume that* $\{(i, j, 0) : i + j = m\} \cup \{(0, 0, m)\} \subset I \subset \mathcal{M}_{3,d}$*; in all cases* $H(I) = H := \{(0, 0, m), (0, m, 0), (m, 0, 0)\}$*. For at least a positive proportion of* $f(x, y) \in \mathbb{Z}[x, y]$ *of degree* m *with* $I_f = I$ *we have* $G(C_f) = m\mathbb{Z}_{\geq 1} = G(H)$.

1.4. **Applications to the sparsity of odd degree points.** Finally, we give applications of our methods to quadric and cubic hypersurfaces and to hyperelliptic curves.

1.4.1. *Applications to hypersurfaces.* Our methods can be used to show in certain cases that higher degree points on a hypersurface imply the existence of rational points. In particular we reprove Springer's theorem [15] and a result of Coray [6].

Theorem 1.9 (Springer)**.** *Any homogeneous quadratic* $f(x_1, \ldots, x_m) = 0$ *has a rational point if and only if it has a point of odd degree.*

We also have the following statement for cubic forms relating rational points and degree 2 points.

Proposition 1.10 (Coray)**.** *A homogeneous cubic* $f(x_1, \ldots, x_m) = 0$ *has a rational point if and only if it has a point of degree* 2.

1.4.2. *Applications to hyperelliptic curves.* Bhargava, Gross, and Wang [1, Corollary 8] showed that for any fixed odd integer m, the proportion of hyperelliptic curves of genus g that contain rational points of degree m, tends to 0 as $g \to \infty$. However, in the cases where a hyperelliptic curve does possess an odd degree point, Bhargava conjectures that 100% of the locally soluble hyperelliptic curves which have odd degree points will have an odd degree point of lowest degree *exactly* g or $g+1$ (whichever is odd). Below, we give a characterization of $D(C)^{\inf}$ in the case where a hyperelliptic curve has an odd degree point.

Proposition 1.11. *Let* C *be a hyperelliptic curve of genus* g *with a point* $P \neq (0, 1, 0)$ *of odd degree, and choose* P *to be of smallest odd degree* m*. If* P *is rational (that is,* $m = 1$*) then* $D(C)^{\inf} \supset \mathbb{Z}_{\geq g+1}$*. Otherwise* $m \leq g+1$ *and* $D(C)^{\inf} \supset \mathbb{Z}_{\geq 2g+2-m}$*. We deduce that* $\mathcal{E}(C)$ *is a subset of the odd integers* $\leq \max\{1, 2g-3\}$.

In particular, this confirms "half" of Bhargava's conjecture (hyperelliptic curves which have odd degree points will have an odd degree point of degree $\leq g+1$). It remains to show that 100% of such hyperelliptic curves have no points of odd degree $< g$.

Strategy and organization. The general strategy in our proofs is to insert irreducible polynomials for $x_1 = x_1(t), \dots, x_m = x_m(t)$ of given degrees $d_1, \dots, d_m$ to obtain $f(\mathbf{x}(t))$ of degree D (the maximal degree of any of the monomials in f), which is either irreducible, or is a given polynomial times an irreducible. This is guaranteed to happen for most inputs using Hilbert's irreducibility theorem. If $(d_1, \dots, d_m) = 1$ then the roots of $f(\mathbf{x}(t))$ give rise to new points of degree D on C.

If one does not get the same point nor the same field too often, then one obtains a good lower bound for the number of fields containing new points that one can construct by this method (which is Theorem 1.2). However for certain f there can be a large number of solutions to $f(\mathbf{x}(t)) = g(t)$, and so we can only work with f for which this does not happen (which we call *the reasonable image hypothesis*); in practice we guarantee this by fixing some of the $x_i(t)$.

In section 2 we explain the reasonable image hypothesis, and define $\mathrm{Exp}(C)$, and give the lower bound $\frac{1}{2d^2}$. Section 3 shows how to construct certain exponent vectors more-or-less in a given pre-determined direction, explains how to construct $D(H)^{\mathrm{inf}}$ and $D(C)^{\mathrm{inf}}$ leading to the proof of Theorem 1.5.

Section 4 puts Hilbert's Irreducibility Theorem in our context where we specialize an m-variable irreducible polynomial taking irreducible polynomials as entries, with an irreducible outcome, sometimes with extra conditions, and section 5 develops the theory of non-singular solutions to our equation.

In section 6 we carefully make substitutions and keep track of how many irreducible polynomials we have created with given degree and coefficient size. In section 7 we determine how many new fields come as a result of the constructions in section 6, and this is where the reasonable image hypothesis plays an important role. Section 7 contains the proofs of Theorem 1.1 and Theorem 2.1.

In section 8 we look at the special case that f has points of given degree, leading to the proof of Theorem 1.3. In section 9 we make a detailed look at improved lower bounds for $\mathrm{Exp}(C)$, in particular for equations of special interest (like hyperelliptics and diagonal equations).

In section 10 we look carefully at certain cases in which we can use local methods to show that $G(C)$ is must be divisible by a given prime, and therefore cases where we can fully determine $G(C)$ from $G(H)$. In particular, section 10 contains the proofs of Theorems 1.7 and 1.8.

In section 11 we give our alternative proof of Springer's theorem 1.9 and the proof of Proposition 1.10. Section 11 also includes a discussion of odd degree points on hyperelliptic curves including Bhargava's conjecture and contains a proof of Proposition 1.11.

Acknowledgements. Many thanks to Manjul Bhargava, Pete Clark, Henri Darmon, Robert Lemke Oliver, Morena Porzio, Samir Siksek and Frank Thorne for helpful remarks and/or useful email conversations. AG is grateful for support from NSERC (Canada). LB is grateful for the support of the U.S. National Science Foundation (DMS-2418835) and the Simons Foundation (MPS-TSM–00007992).

2. The reasonable image hypothesis and $\mathrm{Exp}(C)$

We begin by stating a slightly more general version of Theorem 1.2:

Theorem 2.1 (Theorem 1.2 revisited)**.** *Let C be an irreducible hypersurface given by a polynomial f in m variables with integer coefficients, of degree d. There exists a constant $\mathrm{Exp}(C) > 0$ for which the following holds.*

Fix $\epsilon > 0$. If D is divisible by $G(C)$ and is sufficiently large, and if X is sufficiently large then

$$\#\{\text{Fields } K \in \mathcal{F}(C) : [K:\mathbb{Q}] = D \text{ and } \mathrm{disc}(K/\mathbb{Q}) \le X\} \gg X^{\frac{1}{2}\mathrm{Exp}(C)-\epsilon}.$$

We will define $\mathrm{Exp}(C)$ in terms of the Newton polygon H_f, and the *reasonable image hypothesis* on repetitions in the image of f with polynomial inputs under certain (explicitly given) restrictions. These definitions are complicated and will occupy the rest of this section. One can sometimes obtain a better explicit result by taking into account further information about f.

2.1. **The reasonable image hypothesis.** A key technical issue is to determine how many different polynomial m-tuples substituted into f give rise to the same polynomial value? For any polynomial $g(t) = \sum_i g_i t^i$ we define $\|g(t)\| = \max_i |g_i|$. If $\mathbf{x}(t) = (x_1(t), \dots, x_m(t))$ then we define $\|\mathbf{x}(t)\| := \max_{1\le i\le m}\|x_i(t)\|$, and $\deg \mathbf{x}(t) := \max_{1\le i\le m} \deg x_i(t)$.

The reasonable image hypothesis (RIH). *Let $f(x_1, \dots, x_m) \in \mathbb{Z}[t][x_1, \dots, x_m]$, homogeneous in $x_1, \dots, x_m$, have degree $d \ge 1$. For any given irreducible polynomial $g(t) \in \mathbb{Z}[t]$, let $N_{f,D}(g, T)$ denote the number distinct m-tuples $\mathbf{x}(t) \in \mathbb{Z}[t]^m$ with $\deg \mathbf{x}(t) \le D$, given leading coefficients and $\|\mathbf{x}(t)\| \le T$ for which $f(\mathbf{x}(t)) = g(t)$. Then*

$$N_{f,D}(g, T) \ll_f T^{o_f(D)}.$$

The reasonable image hypothesis holds whenever $m = 1$ since then $f(x_1) - g(t)$ is a polynomial in x_1 of degree d and so there are no more than d solutions.

The RIH holds in many situations, but not always. For example, the polynomial $f(x, y) = x+y$ clearly fails the RIH since the number of solutions to $x(t)+y(t) = t^D+ct+1$ (assuming it is irreducible) with $\|x\| \le T$ and say $\deg x, \deg y = D$ and given leading coefficients is $\gg T^D$. One can create many such unreasonable images based on this idea, for example whenever $f(x_1, \dots, x_m) = g(x_1 + x_2, x_3, \dots, x_m)$ for some $g(y_1, \dots, y_{m-1}) \in \mathbb{Z}[y_1, \dots, y_{m-1}]$.

Another class of examples is given by polynomials f for which $m > d^2$; these all fail the reasonable image hypothesis: There are $\asymp T^D$ polynomials $x_i(t)$ of degree D, given leading coefficients with $\|x_i(t)\| \le T$, and so the number of m-tuples $(\mathbf{x}(t))$ is $\asymp T^{mD}$. Now $f(\mathbf{x}(t))$ has degree $\le dD$, with coefficients $\|f(\mathbf{x})\| \ll_f \|x(t)^d\| \ll (DT)^d \ll T^d$. The number of polynomials $g(t)$ with degree $\le dD$, bounded leading coefficient and $\|g\| \ll T^d$ is $\asymp_{d,D} T^{d^2D}$. Therefore if $m > d^2$ then some $g(t)$ must equal $f(\mathbf{x}(t))$ for $\gg T^{(m-d^2)D} \gg T^D$ different choices of $\mathbf{x}(t)$.

The following example further illustrates that the failure of the RIH can depend on the coefficients of f and not just H_f: Suppose that for some polynomials f_1, f_2 we have

$$f(x_1, \dots, x_m) = f_1(x_1, \dots, x_\ell) + f_2(x_{\ell+1}, \dots, x_m).$$

If $f_1(y_1(t), \dots, y_\ell(t)) = 0$ (which depends on the coefficients of f_1) then for any given $y_{\ell+1}(t), \cdots, y_m(t)$ we have

$$f(a(t)y_1(t), \dots, a(t)y_\ell(t)), y_{\ell+1}(t), \cdots, y_m(t)) = g(t) \text{ where } g(t) := f_2(y_{\ell+1}(t), \cdots, y_m(t))$$

and we can take any $a(t)$ with $\deg a \le D - \deg \mathbf{y}(y)$ and $\|a(t)\| \ll T/\max_i \|y_i(t)\|$, so that the RIH fails.

2.2. **Sub-images.** To get good lower bounds on the number of solutions our proofs need the reasonable image hypothesis to hold for the polynomial under consideration. We have just seen several examples where it fails; however for $f(x,y) = x+y$ the reasonable image hypothesis holds whenever we fix y and vary only over polynomials x. More generally we proceed as follows:

If $\mathbf{y}(t) \in \mathbb{Z}[t]^m$ for which $f(\mathbf{y}(t))$ is irreducible and J is a non-empty subset of $\{1,\dots,m\}$ then $f(\mathbf{x}_{J,\mathbf{y}}(t))$ is irreducible where we obtain $\mathbf{x}_{J,\mathbf{y}}(t)$ by fixing $x_j(t) = y_j(t)$ for all $j \in \{1,\dots,m\} \setminus J$, and allowing the x_j with $j \in J$ to be variables. Now let $\mathcal{J}_f$ denote those non-empty subsets J of $\{1,\dots,m\}$ for which there exists $\mathbf{y}(t) \in \mathbb{Z}[t]^m$ for which $f(\mathbf{y}(t))$ is irreducible and $f(\mathbf{x}_{J,\mathbf{y}}(t))$ satisfies the reasonable image hypothesis.

We saw that every one-variable polynomial satisfies the RIH and so $\{j\} \in \mathcal{J}_f$ for all $j \in \{1,\dots,m\}$.

There are many possibilities for subimages that we have not explored. Here we look at subvarieties of C given by fixing x_j for each $j \notin J$ (that is, intersecting the variety with a linear surface). But there are many other possible subvarieties, even other linear surfaces, for example considering whether RIH holds when x_1, x_2 vary with $x_1 + x_2$ fixed. A broad consideration of such possibilities might lead to significant improvements to our explicit results (and in particular the value of $\mathrm{Exp}(C)$ which we define below).

2.3. **Working with corners.** For any $\mathbf{r} \in \mathbb{R}^m_{\geq 0} \setminus \{\mathbf{0}\}$ we select $\mathbf{h}_r \in H$ to maximize $\mathbf{r}\cdot\mathbf{h}$.[2] For each $\mathbf{h} \in H$ we define the sets

$$R(\mathbf{h}) = R_H(\mathbf{h}) := \{\mathbf{e} \in \mathbb{R}^m_{>0} : \ |\mathbf{e}|= 1, \mathbf{e}\cdot\mathbf{h} > \mathbf{e}\cdot\mathbf{h}' \text{ for all } \mathbf{h}' \in H\}$$

so that $\overline{R(\mathbf{h})} = \{\mathbf{e} \in \mathbb{R}^m_{\geq 0} : \ |\mathbf{e}|= 1, \mathbf{e}\cdot\mathbf{h} \geq \mathbf{e}\cdot\mathbf{h}' \text{ for all } \mathbf{h}' \in H\}$. Now $\deg f = \mathbf{h}\cdot\mathbf{1}$ for all $\mathbf{h} \in H_f$ so we define $\deg H = d$ for all $H \in \mathcal{H}_{m,d}$ as $\mathbf{h}\cdot\mathbf{1} = d$ for all $\mathbf{h} \in H$.

For each non-empty subset J of $\{1,\dots,m\}$ we define

$$H_J = \{\mathbf{h}_J : h \in H\}$$

where $\mathbf{h}_J$ is given by the jth coordinate of the vector $\mathbf{h}$ for each $j \in J$ (that is, $\mathbf{h}_J$ is the vector $\mathbf{h}$ restricted to the co-ordinates in J). If $\mathbf{h}_J \in H_J$ then we define

$$R(\mathbf{h}_J) = R_H(\mathbf{h}_J) := \{\mathbf{e} \in \mathbb{R}^J_{>0} : \ |\mathbf{e}|= 1, \mathbf{e}\cdot\mathbf{h} > \mathbf{e}\cdot\mathbf{h}' \text{ for all } \mathbf{h}' \in H\}$$

where the vectors in $\mathbb{R}^J_{>0}$ are supported only on the jth co-ordinates with $j \in J$. Let $\deg H_J := \max_{\mathbf{h}\in H_J} \mathbf{h}\cdot\mathbf{1}$; and if $H = H_f$ then $\deg f_J := \deg H_J$. Finally we define

$$\mathrm{Exp}_J(H) := \max_{\substack{\mathbf{h}_r\in H\\ \mathbf{h}_e\in H_J}} \max_{\substack{\mathbf{r}\in\overline{R(\mathbf{h}_r)}\\ \mathbf{e}\in\overline{R(\mathbf{h}_e)}}} \frac{\mathbf{e}\cdot\mathbf{r}}{(\mathbf{e}\cdot\mathbf{h_e})(\mathbf{r}\cdot\mathbf{h_r})}.$$

Fix $j \in \{1,\dots,m\}$. Let $\mathbf{e} = \mathbf{r}$ be the vector with a 1 in the jth co-ordinate and 0 elsewhere and so $\mathbf{e}\cdot\mathbf{h} = \mathbf{h}_j$ which implies that $\mathbf{e}\cdot\mathbf{h_e} = \max_{\mathbf{h}\in H} h_j = \deg_{x_j} f$. Therefore

$$\mathrm{Exp}_{\{j\}}(H) \geq \frac{1}{(\deg_{x_j} f)^2}.$$

Let $\mathcal{J}$ be a set of non-empty subsets J of $\{1,\dots,m\}$ and define

$$\mathrm{Exp}(H,\mathcal{J}) := \max_{J\in\mathcal{J}} \mathrm{Exp}_J(H).$$

[2]There may be more than one possibility for $\mathbf{h}_r$; we can choose any of them.

The definitions imply that if $I \subset J$ then $\mathrm{Exp}_I(H) \le \mathrm{Exp}_J(H)$. Therefore if $\{1,\dots,m\} \in \mathcal{J}$ then [3]

$$\mathrm{Exp}(H,\mathcal{J}) = \mathrm{Exp}_{\{1,\dots,m\}}(H) = \max_{\mathbf{h}\in H} \max_{\mathbf{e}\in\overline{R(\mathbf{h})}} \frac{1}{(\mathbf{e}\cdot\mathbf{h})^2}.$$

This implies $\mathrm{Exp}(H,\mathcal{J}) \ge \frac{1}{(\mathbf{e}\cdot\mathbf{h})^2} \ge \frac{1}{\|\mathbf{h}\|^2}$ for any $\mathbf{h}\in H, \mathbf{e}\in \overline{R(\mathbf{h})}$. In particular, taking $\mathbf{e} = \mathbf{1}/\sqrt{m}$, this implies that $\mathrm{Exp}(H,\mathcal{J}) \ge \frac{m}{d^2}$. We discuss lower bounds on $\mathrm{Exp}(H,\mathcal{J})$ in more detail in section 9.

Finally if C be an irreducible hypersurface given by a polynomial f in m variables with integer coefficients, of degree d then for Theorem 2.1 we define

$$\boxed{\mathrm{Exp}(C) = \mathrm{Exp}(C_f) := \mathrm{Exp}(H_f, \mathcal{J}_f)}$$

where $\mathcal{J}_f$ was defined in section 2.2. We have seen that if $j \in \{1,\dots,m\}$ then $j \in \mathcal{J}_f$. Hence

$$\mathrm{Exp}(C_f) \ge \max_{j\in\{1,\dots,m\}} \mathrm{Exp}_{\{j\}}(H) \ge \frac{1}{(\deg_{x_j} f)^2} \ge \frac{1}{d^2}$$

which is how "Theorem 1.2, revisited" implies Theorem 1.2.

2.4. **A more geometric perspective.** If $\{1,\dots,m\} \in \mathcal{J}$ then $\mathrm{Exp}(H,\mathcal{J}) = \frac{1}{(\mathbf{u}\cdot\mathbf{h})^2}$ where we select $\mathbf{h}\in H, \mathbf{u}\in\overline{R(\mathbf{h})}$ for which $|\mathbf{u}\cdot\mathbf{h}|$ is minimized. The following lemma restricts our search space for $\mathbf{h}$ and $\mathbf{u}$ to a simple finite set of possibilities.

Lemma 2.2. *Suppose that $|\mathbf{u}\cdot\mathbf{h}|$ is minimized, over all $\mathbf{h}\in H, \mathbf{u}\in\overline{R(\mathbf{h})}$ at $\mathbf{h}=\mathbf{h}_1, \mathbf{u}=\mathbf{u}_1$. Let $\mathcal{L}_1$ be the set of linear forms given by*

$$\mathcal{L}_1 := \{(\mathbf{h}_1 - \mathbf{h})\cdot\mathbf{x} : \mathbf{h}\in H\} \cup \{\mathbf{e}_j\cdot\mathbf{x} : 1\le j\le m\}$$

where $\mathbf{e}_j$ is the unit vector in the jth coordinate direction. There exists a subset S of $\mathcal{L}_1$ which generates a subspace of $\mathbb{R}^m$ of dimension $m-1$ such that $\mathbf{u}_1$ generates the 1-dimensional null space of S and $\ell_{\mathbf{x}=\mathbf{u}_1} > 0$ for all $\ell\in\mathcal{L}_1\setminus S$.

To search for the optimal $\mathbf{h}$ and $\mathbf{u}$ we begin by applying Lemma 2.2 for each $\mathbf{h}_1 \in H$. There are only finitely many subsets of the finite set $\mathcal{L}_1$ and only finitely many of these that generate a subspace of $\mathbb{R}^m$ of dimension $m-1$. In these cases we determine the unit vector (up to sign) that generates the null space, and then verify whether there is a choice of sign which satisfies the criteria in the lemma. Finally we test which of these gives the largest value of $|\mathbf{u}\cdot\mathbf{h}|$.

Proof. Write $\mathbf{u}=\mathbf{u}_1$. Now $\mathbf{h}_1\cdot\mathbf{u}_1$ is a local minimum under the conditions that each $u_i \ge 0$, that $\|\mathbf{u}\|=1$ and that $\mathbf{h}_1\cdot\mathbf{u} \ge \mathbf{h}\cdot\mathbf{u}$ for all $\mathbf{h}\in H$ (that is, $\ell_{\mathbf{x}=\mathbf{u}_1}\ge 0$ for all $\ell\in\mathcal{L}_1$).

We will suppose that $\mathbf{u}$ satisfies various boundary conditions, $\mathbf{h}_i\cdot\mathbf{u} = \mathbf{h}_1\cdot\mathbf{u}$ for all $i\in I$ (and no others), and $u_j = \mathbf{e}_j\cdot\mathbf{u} = 0$ for all $j\in J$ and no others. Let V be the subspace of $\mathbb{R}^m$ generated by

$$\langle \{h_i - h_1 : i\in I\} \cup \{\mathbf{e}_j : j\in J\}\rangle$$

so that $\mathbf{u}\in N(V)$, the null space of V.

[3] In section 2.4 we restrict the possible $\mathbf{h}$ and $\mathbf{e}$ that give the maximum to an accessible finite set.

For any $\mathbf{v} \in N(V)$ there exists $\eta > 0$ such that $\mathbf{u} + \eta\mathbf{v}$ satisfies the same inequalities as $\mathbf{u}$ with respect to the boundaries, $\mathbf{h}_1 \cdot (\mathbf{u} + \eta\mathbf{v}) > \mathbf{h}_i \cdot (\mathbf{u} + \eta\mathbf{v})$ for all $i \notin I$, and $(\mathbf{u} + \eta\mathbf{v})_j > 0$ for any $j \notin J$. We must have $\mathbf{h}_1 \cdot \mathbf{u} \le \mathbf{h}_1 \cdot \frac{(\mathbf{u}+\eta\mathbf{v})}{\|\mathbf{u}+\eta\mathbf{v}\|}$ which is equivalent (after squaring) to

$$(\mathbf{h}_1 \cdot \mathbf{u})^2(2\eta\mathbf{u} \cdot \mathbf{v} + \eta^2\|\mathbf{v}\|^2) \le 2\eta(\mathbf{h}_1 \cdot \mathbf{u})(\mathbf{h}_1 \cdot \mathbf{v}) + \eta^2(\mathbf{h}_1 \cdot \mathbf{v})^2$$

Therefore taking arbitrarily small $\eta > 0$ implies that

$$(\mathbf{h}_1 \cdot \mathbf{u})(\mathbf{u} \cdot \mathbf{v}) \le (\mathbf{h}_1 \cdot \mathbf{v})$$

as $\mathbf{h}_1 \cdot \mathbf{u} > 0$, and this is also true when we change $\mathbf{v}$ to $-\mathbf{v}$ so that

$$(\mathbf{h}_1 \cdot \mathbf{u})(\mathbf{u} \cdot \mathbf{v}) = (\mathbf{h}_1 \cdot \mathbf{v}) \text{ for all } \mathbf{v} \in N(V).$$

Going back above we also have

$$(\mathbf{h}_1 \cdot \mathbf{u})^2\|\mathbf{v}\|^2 \le (\mathbf{h}_1 \cdot \mathbf{v})^2 = (\mathbf{h}_1 \cdot \mathbf{u})^2(\mathbf{u} \cdot \mathbf{v})^2$$

so that $\|\mathbf{v}\|^2 \le (\mathbf{u} \cdot \mathbf{v})^2 \le \|\mathbf{u}\|^2\|\mathbf{v}\|^2 = \|\mathbf{v}\|^2$. Therefore $|\mathbf{u} \cdot \mathbf{v}| = \|\mathbf{u}\| \, \|\mathbf{v}\|$ so that $\mathbf{v}$ is a scalar multiple of $\mathbf{u}$. This implies that $N(v)$ is a 1-dimensional space, which is generated by S in the statement of the result. □

3. Elementary number theory

In this section we collect together the elementary number theory we will use to exploit our constructions. Let H be a given *Newton polytope*, which is defined to be a finite subset of $\mathcal{M}_{m,d}$ such that for each $\mathbf{h} \in H$ there exists $\mathbf{v} \in \mathbb{Z}^m_{\ge 0}$ for which

$$\mathbf{h} \cdot \mathbf{v} > \mathbf{i} \cdot \mathbf{v} \text{ for all } \mathbf{i} \in H, \mathbf{i} \ne \mathbf{h}.$$

We will define a set $D(H)^{\inf}$ that contains all the elements of $D(C)^{\inf}$ which can be obtained without any specific knowledge of the hypersurface $C = C_f$ other than that its Newton polygon H_f is H. The next result provides a typical construction.

3.1. Elements of $D(H)^{\inf}$ constructed from a given element of H_f.

Proposition 3.1. *Fix $\mathbf{h} \in H$ and $\mathbf{r} \in R(\mathbf{h})$. If D is divisible by $g(\mathbf{h})$ and is sufficiently large then there exists $\mathbf{d} \in \mathbb{Z}^m_{\ge 1}$ with $(d_1, \dots, d_m) = 1$ and each $d_j = \frac{Dr_j}{\mathbf{r}\cdot\mathbf{h}} + O((\log D)^2)$ for which $D = \mathbf{d} \cdot \mathbf{h}$ and $D > \mathbf{d} \cdot \mathbf{h}'$ for all $\mathbf{h}' \in H$.*

We will prove this using a tool from sieve theory: Let $J(D)$ be Jacobsthal's function, the minimal integer such that every interval of this length contains an integer coprime to D. Iwaniec [8] proved that we can take $J(D) \ll (\omega \log \omega)^2 \ll (\log D)^2$ where ω denotes the number of prime factors of D. Our path involves proving the following:

Lemma 3.2. *Fix $r_1, \dots, r_m > 0$ and integers $i_1, \dots, i_m \ge 1$ with $m \ge 2$. If D is divisible by $\gcd_j i_j$ and is sufficiently large then there exist integers $d_1, \dots, d_m \ge 1$ with $(d_1, \dots, d_m) = 1$ and $D = d_1 i_i + \cdots + d_m i_m$ where each*

$$\left| d_\ell - \frac{r_\ell D}{i_1 r_1 + \cdots + i_m r_m} \right| \le (i_1 + i_2) J(D) 1_{\ell=1,2} + \sum_{j=2}^{m} i_j$$

Proof of Proposition 3.1. Since $\mathbf{r} \in R(\mathbf{h})$ we have $\mathbf{r}\cdot\mathbf{h} > \mathbf{r}\cdot\mathbf{h}'$ for all $\mathbf{h}' \in H$. The strict inequality implies that this is also true for all $\mathbf{r}'$ in a small ball B around $\mathbf{r}$; in particular we may assume that $\mathbf{r} \in \mathbb{R}^m_{>0}$.

We now apply Lemma 3.2 with $\mathbf{i} = \mathbf{h}$ so that $\|\mathbf{r} - c_D\mathbf{d}\| \ll \frac{(\log D)^2}{D}$ where $c_D = \frac{\mathbf{r}\cdot\mathbf{h}}{D}$. If D is sufficiently large then $c_D\mathbf{d} \in B$, so that $D = \mathbf{h}\cdot\mathbf{d} > \mathbf{j}\cdot\mathbf{d}$ for all $\mathbf{j} \in H, \mathbf{j} \neq \mathbf{h}$. □

We prove Lemma 3.2 by induction on m beginning with the $m = 2$ case:

Lemma 3.3. *If $(i_1, i_2) = 1$ with $i_1, i_2 > 0$ then for all sufficiently D there exists integers $d_1, d_2 > 0$ with $(d_1, d_2) = 1$ for which $D = i_1d_1 + i_2d_2$ with*

$$\left|d_1 - \frac{r_1D}{i_1r_1 + i_2r_2}\right| \le i_2J(D) \text{ and } \left|d_2 - \frac{r_2D}{i_1r_1 + i_2r_2}\right| \le i_1J(D).$$

Proof. Let N be the nearest integer to $\frac{r_2D}{i_1r_1+i_2r_2}$ with $N \equiv D/i_2 \pmod{i_1}$, so $|N - \frac{r_2D}{i_1r_1+i_2r_2}| \le \frac{i_1}{2}$. Now let $M = \frac{D-i_2N}{i_1}$ so that $D = i_1M + i_2N$ and $|M - \frac{r_1D}{i_1r_1+i_2r_2}| = \frac{i_2}{i_1}|N - \frac{r_2D}{i_1r_1+i_2r_2}| \le \frac{i_2}{2}$.

We now select k as small as possible for which $m = M - ki_2, n = N + ki_1$ with $(m, n) = 1$. Now (m, n) divides D, so we need to ensure that for all primes p dividing D, p does not divide m or n. Now p does not divide at least one of i_1 and i_2, say i_2, so p does not divide m provided $k \not\equiv M/i_2 \pmod{p}$ (and if p divides i_2 then $k \not\equiv -N/i_1 \pmod{p}$). So we need to sieve out from integers k one residue class for each prime p dividing D, and so $|k| \le \frac{J(D)}{2}$. The result follows with $d_1 = m$ and $d_2 = n$. □

Proof of Lemma 3.2. Suppose it is true when $gcd_j i_j = 1$. Now if $gcd_j i_j = g$ then $g|D$ so write $D' = D/g$ and each $i'_j = i_j/g$. Then $D = gD' = g(d_1i'_i + \cdots + d_mi'_m) = d_1i_i + \cdots + d_mi_m$ and the approximations stays good.

So henceforth assume that $gcd_j i_j = 1$. We proceed by induction on $m \ge 2$. The result is given by lemma 3.3 for $m = 2$. Let $b_1 = i_2J(D), b_2 = i_1J(D)$ and $b_\ell = i_{\ell-1}$ for all $\ell \ge 3$.

Now write $s_m := i_1r_1 + \cdots + i_mr_m$ and for $m \ge 3$ let $g = (D, i_1, \dots, i_{m-1})$ so that $g|d_m$.

We select d_m divisible by g with d_m as close as possible to $\frac{r_mD}{s_m}$ so that

$$\left|d_m - \frac{r_mD}{s_m}\right| \le g \le i_{m-1} = b_m.$$

Let $D' = D - d_mi_m$ so that $|D' - \frac{s_{m-1}}{s_m}D| \le i_mg$. We can now proceed with the induction hypothesis so that $D' = d_1i_i + \cdots + d_{m-1}i_{m-1}$ with $(d_1, \dots, d_{m-1}) = 1$ where, for $1 \le \ell \le m-1$,

$$\left|d_\ell - \frac{r_\ell D}{s_m}\right| \le \left|d_\ell - \frac{r_\ell D'}{s_{m-1}}\right| + \frac{r_\ell}{s_{m-1}}\left|D' - \frac{s_{m-1}D}{s_m}\right|$$

$$\le b_\ell + \sum_{j=\max\{3,\ell\}}^{m-1} i_j + \frac{r_\ell i_m g}{s_{m-1}} \le b_\ell + \sum_{j=\max\{3,\ell\}}^{m} i_j$$

since $gr_\ell \le i_\ell r_\ell \le s_{m-1}$. The result follows. □

3.2. **Defining $D(H)^{\mathbf{inf}}$.** For each $\mathbf{h} \in H$ and any integer $n \ge 0$ let

$$S_{\mathbf{h},j}(n) := \{\mathbf{h}\cdot\mathbf{d} - n : \mathbf{d} \in \mathbb{Z}^m_{\ge n}, (d_1, \dots, d_m) = 1, d_j \ge n + \deg_{x_j} f \text{ and } \mathbf{h}\cdot\mathbf{d} \ge \mathbf{i}\cdot\mathbf{d} \text{ for all } \mathbf{i} \in H_f\},$$

$S_{\mathbf{h}}(n) = \bigcup_j S_{\mathbf{h},j}(n)$ and $S_{\mathbf{h}} = S_{\mathbf{h}}(0)$.

We construct $D(H)^{\inf}$ in stages: We begin with

$$D(H)_0 = \bigcup_{\mathbf{h}\in H} S_{\mathbf{h}}.$$

Now given $D(H)_k$ for some $k \geq 0$ we define

$$D(H)_{k+1} = \bigcup_{\substack{\mathbf{h}\in H \\ n\in \mathrm{Frob}(D(H)_k)}} S_{\mathbf{h}}(n),$$

so that $D(H)_0 \subseteq D(H)_1 \subseteq \cdots$.

By Proposition 3.1, there exists $n_{\mathbf{h}} > 0$ for which $g(\mathbf{h})\mathbb{Z}_{\geq n_{\mathbf{h}}} \subset S_{\mathbf{h}}$ for each $\mathbf{h}\in H$. Elementary number theory then yields that there exists $N_H > 0$ for which $G(H)\mathbb{Z}_{\geq N_{\mathbf{h}}} \subset \mathrm{Frob}(D(H)_0)$. Then there exists $m_{\mathbf{h}} > 0$ such that $G(H)\mathbb{Z}_{\geq m_{\mathbf{h}}} \subset \bigcup_{n\in \mathrm{Frob}(D(H)_0)} S_{\mathbf{h}}(n)$ for each $\mathbf{h}\in H$. Hence $D(H)_1 = G(H)\mathbb{Z}_{\geq 1} \setminus \mathcal{E}_1(H)$ for some finite set $\mathcal{E}_1(H) \subset G(H)\mathbb{Z}_{\geq 1}$. Now we keep on iterating and so $\mathcal{E}_1(H) \supseteq \mathcal{E}_2(H) \supseteq \cdots$ Since $\mathcal{E}_1(H)$ is finite there exists some k with $\mathcal{E}_k(H) = \mathcal{E}_{k+1}(H)$ and then $\mathcal{E}_j(H) = \mathcal{E}_k(H)$ for all $j \geq k$, so we define $\mathcal{E}(H) := \mathcal{E}_k(H)$.

Finally we define $D(H)^{\inf} = G(H)\mathbb{Z}_{\geq 1} \setminus \mathcal{E}(H)$.

3.3. **Construction of $D(C)^{\inf}$.** Given only $H = H_f$ one can determine $D(H)^{\inf}$ as in section 3.2 and we know that $D(H)^{\inf} \subset D(C)^{\inf}$. If $G(C_f) \neq G(H_f)$ then there exist new points $P_1, \ldots, P_r$ degrees $n_1, \ldots, n_r \in D(C_f)^{\inf}$, not divisible by $G(H_f)$ for which $G(C_f) = \gcd(G(H_f), n_1, \ldots, n_r)$. To construct $D(C)^{\inf}$ we let

$$D(C)_0 = D(H)_0 \cup \{P_1, \ldots, P_r\} \text{ and then } D(C)_{k+1} = \bigcup_{\substack{\mathbf{h}\in H \\ n\in \mathrm{Frob}(D(C)_k)}} S_{\mathbf{h}}(n),$$

for all $k \geq 0$. Then $D(C)^{\inf} = \lim_{k\to\infty} D(C)_k$ (as we did for $D(H)^{\inf}$) and $D(C)^{\inf} = G(C)\mathbb{Z}_{\geq 1} \setminus \mathcal{E}(C)$. Theorem 1.5 follows immediately from this construction.

4. Hilbert's Irreducibility Theorem

Hilbert's Irreducibility Theorem implies that if $f(x, y, z) \in K[x, y, z]$ is irreducible then the polynomial $f(x(t), y(t), z(t)) \in K[t]$ is irreducible for almost all choices of $x(t), y(t), z(t) \in K[t]$. We now make this precise in the form needed.

4.1. **Thin sets.** Throughout let K be a field of characteristic 0. In section 9.1 of [14], Serre defined a set $\Omega \subset K^n$ or $\mathbb{P}_n(K)$ to be *thin* if there is an algebraic variety Z over K and a morphism $\pi\colon Z \to K^n$ or $\mathbb{P}_n(K)$, respectively, such that $\Omega \subset \pi(Z(K))$ and the fiber of π over the generic point is finite and π has no rational section over K (that is, π is quasi-finite and has no section in a neighborhood of the generic point).

He went on to classify thin sets and showed in section 9.2 of [14] (see Proposition 1 and the following comment) that if $F(X; T_1, \ldots, T_n)$ is an irreducible polynomial over $K(T)$ then

$$\{t = (t_1, \ldots, t_n) : \ F(X, t) \text{ is reducible over } K[X]\}$$

is a subset of a thin set Ω in $\mathbb{P}_n(K) \simeq \mathbb{P}_n(\mathcal{O}_K)$, where $\mathcal{O}_K$ be the ring of integers of K. (Moreover, Serre's Proposition 2 implies that $F(X, t)$ has the same Galois group as $F(X, T)$ outside of a thin set.)

Now let K be a number field of degree d and $||x|| = \max_\sigma |\sigma x|$ for $x \in \mathcal{O}_K$, where σ runs over the different embeddings of K in $\mathbb{C}$.

Lemma 4.1 (Hilbert's Irreducibility Theorem)**.** *Let $f(X, T_1, ...T_n) \in \mathcal{O}_K[X, T_1, \dots T_n]$ be an irreducible polynomial in $K[X, T_1, ..., T_n]$, and $e_1, \dots, e_n \in \mathbb{R}^+$. Then*

$$\#\{(a_1, ...a_n) \in \mathcal{O}_K^n : \textit{Each } ||a_i|| \leq T^{e_i} \textit{ and } f(X, a_1, ...a_n) \textit{ reducible in } K[X]\} \ll T^{(e_1+\cdots+e_n-\min(e_i)/2)d} \log T.$$

Proof. As remarked above, Serre showed in section 9.2 of [14] that

$$M := \{(a_1, \dots a_n) \in \mathcal{O}_K^n : f(X, a_1, ...a_n) \text{ is reducible in } K[X]\}$$

is a thin set.

In Theorem 1 of section 13.1 of [14], Serre observes that a theorem of Cohen [5] is easily modified to establish a uniform bound on the number of points of a thin subset M of $\mathcal{O}_K$ inside a box of diameter N: For any given $(c^{(1)} \dots c^{(n)})$ we have

$$\#\{(x^{(1)} \dots x^{(n)}) \in M : \ \max_{1\leq i\leq n} ||x^{(i)} - c^{(i)}|| \leq N\} = O(N^{(n-1/2)d} \log N).$$

For given $e_i \in \mathbb{R}^+$ let $e_0 = \min_{1\leq i\leq n} e_i$. We can bound

$$M(\mathbf{e}) := \#\{(x^{(1)} \dots x^{(n)}) \in M : \ \max_{1\leq i\leq n} ||x^{(i)}|| \leq T^{e_i}\}$$

by covering the region in dn-dimensional cubes of side length $N = 2T^{e_0}$. If T is sufficiently large then we will need no more than

$$T^{d(e_1-e_0)} \cdots T^{d(e_n-e_0)} \text{ such boxes,}$$

and so

$$M(\mathbf{e}) \ll T^{d(e_1-e_0)} \cdots T^{d(e_n-e_0)} \cdot T^{(n-1/2)de_0} \log T = T^{(e_1+\cdots+e_n-e_0/2)d} \log T. \qquad \square$$

5. Non-singular solutions to an equation

Throughout the rest of this paper we will suppose that

$$f(x_1, \dots, x_m) = \sum_{(i_1,\dots,i_m)\in I_f} a_{i_1,\dots,i_m} x_1^{i_1} \cdots x_m^{i_m} \in \mathbb{Z}[x_1, \dots, x_m]$$

is irreducible and homogenous of degree d, where $a_{\mathbf{i}} \neq 0$ for all $\mathbf{i} \in I_f$.

An algebraic solution $\gamma = (\gamma_1, \cdots, \gamma_m)$ to $f(\gamma) = 0$ is *singular* if $\frac{\partial f(\mathbf{x})}{\partial x_j}|_{\mathbf{x}=\gamma} = 0$ for each j. Now $d \cdot f = \sum_j x_j \frac{\partial f}{\partial x_j}$ and so if γ is non-singular then there are at least two values of j for which $\frac{\partial f(\mathbf{x})}{\partial x_j}|_{\mathbf{x}=\gamma} \neq 0$. In particular, we can analogously determine that f is non-singular whenever we de-projectivize f.

A polynomial solution $\mathbf{y}(t) = (y_1(t), \dots, y_m(t)) \in \mathbb{Z}[t]^m$ to $f(\mathbf{y}(t)) \equiv 0 \pmod{P(t)}$ is *singular* if $\frac{\partial f(\mathbf{x})}{\partial x_j}|_{\mathbf{x}=\gamma} \equiv 0 \pmod{P(t)}$ for each j. Here $P(t)$ is an irreducible polynomial. We remark that if $P(t) := f(\mathbf{x}(t))$ is irreducible then it is non-singular else

$$\frac{df(\mathbf{x}(t))}{dt} = \sum_{j=1}^{m} \frac{dx_j(t)}{dt} \cdot \frac{\partial f(\mathbf{x})}{\partial x_j}\bigg|_{\mathbf{x}=\mathbf{x}(t)} \equiv 0 \pmod{P(t)},$$

so that $P(t)$ divides $P'(t)$ which is impossible.

We now show that singular algebraic solutions and singular polynomial solutions are essentially the same thing:

If $f(\mathbf{y}(t)) \equiv 0 \pmod{P(t)}$ is singular then let α be a root of $P(t)$, that is $P(\alpha) = 0$ and let $\gamma_j = y_j(\alpha)$ for each j. Therefore $f(\gamma) = f(\mathbf{y}(t))|_{t=\alpha}$ which must equal 0 as $f(\mathbf{y}(t))$ is a

multiple of $P(t)$. Analogously $\partial_j f(\gamma) = 0$ for each j and so γ is a singular algebraic point on $f(x_1, \cdots, x_m) = 0$.

On the other hand if γ is a singular solution to $f(\gamma) = 0$ then suppose $\gamma \in \mathbb{Q}(\alpha)$, the smallest such field, where α has minimal (irreducible) polynomial $P(t)$. We can write each $\gamma_j = y_j(\alpha)$ for some polynomials $y_j(t)$. Then $f(\mathbf{y}(t))|_{t=\alpha} = f(\gamma) = 0$ and so $P(t)$ divides $f(\mathbf{y}(t))$. Analogously $\partial_j f(\mathbf{y}(t)) \equiv 0 \pmod{P(t)}$ for each j and so $f(\mathbf{y}(t))$ is a singular polynomial solution to $f(x_1, \cdots, x_m) = 0$.

It is important to note that this is not a 1-to-1 correspondence since we can obtain different $P(t)$ for a given γ by selecting $\alpha' \neq \alpha$ for which $\mathbb{Q}(\alpha') = \mathbb{Q}(\alpha)$; for example, $\alpha' = \frac{a\alpha+b}{c\alpha+d}$, an invertible transformation (in which case $P_\alpha(t) = P_{\alpha'}(\frac{at+b}{ct+d})(ct+d)^{\deg f}$. We call P_α and $P_{\alpha'}$ *equivalent*, and note that the roots of equivalent polynomials generate the same number fields.

Throughout we let $\mathcal{P}_f$ denote the set of irreducible polynomials $P(t) \in \mathbb{Z}[t]$ for which there exists a non-singular solution $y_1(t), \ldots, y_m(t) \in \mathbb{Z}[t]$ to $f(\mathbf{y}(t)) \equiv 0 \pmod{P(t)}$.

We make a straightforward but useful observation:

Lemma 5.1. *If $f(x_1, \ldots, x_m) \in K[x_1, \ldots, x_m]$ is homogenous of degree d and $f(x_1, \ldots, x_m) - c$ has a singularity at $\mathbf{x} = \mathbf{x}_0$ then $c = 0$.*

Proof. If $f(x_1, \ldots, x_m) - c$ has a singularity at $\mathbf{x} = \mathbf{x}_0$ then all the partial derivatives vanish and so

$$\frac{\partial}{\partial x_i} f(x_1, \ldots, x_m)|_{\mathbf{x}=\mathbf{x}_0} = \frac{\partial}{\partial x_i}(f(x_1, \ldots, x_m) - c)|_{\mathbf{x}=\mathbf{x}_0} = 0$$

for each i. But then

$$c = f(x_1, \ldots, x_m)|_{\mathbf{x}=\mathbf{x}_0} = \frac{1}{d}\sum_{i=1}^{m} x_i \frac{\partial}{\partial x_i} f(x_1, \ldots, x_m)|_{\mathbf{x}=\mathbf{x}_0} = 0. \qquad \square$$

5.1. **The algebra of already constructed non-singular points.** We begin with some basic algebra of the $P(t) \in \mathcal{P}_f$.

Proposition 5.2 (Hensel lifting for polynomial solutions)**.** *If $P(t) \in \mathcal{P}_f$ then $P(t)^e \in \mathcal{P}_f$ for every integer $e \geq 1$.*

Proof. We proceed by induction on $e \geq 2$, as the hypothesis gives the $e = 1$ case. Let $c_j(t)$ be a polynomial which is the inverse of $\frac{\partial f(\mathbf{x})}{\partial x_j}|_{\mathbf{x}=\mathbf{y}(t)} \pmod{P}$. Take the solution $\mathbf{y}_e(t)$ for e, so for some polynomial $Q_e(t)$ we have

$$f(\mathbf{y}_e) = P(t)^e Q_e(t)$$

(where $\mathbf{y}_e \equiv \mathbf{y} \pmod{P}$), let $w_i(t) = y_i(t)$ for $i \neq j$, and $w_j(t) = y_j(t) - c_j(t)Q_e(t)P^e$. Now by the multivariable Taylor expansion we have

$$f(\mathbf{w}) \equiv f(\mathbf{y}_e) - c_j(t)Q_e(t)P^e \cdot \left.\frac{\partial f(\mathbf{x})}{\partial x_j}\right|_{\mathbf{x}=\mathbf{y}_e(t)} \equiv 0 \pmod{P^{e+1}},$$

as required. $\square$

Lemma 5.3 (Chinese Remainder Theorem for polynomial solutions)**.** *If $G(t) \in \mathbb{Z}[t]$ factors over $\mathbb{Q}[t]$ into coprime powers of irreducibles in $\mathcal{P}_f$ then there exist $y_1(t), \ldots, y_m(t) \in \mathbb{Z}[t]$ such that $G(t)$ divides $f(\mathbf{y}(t))$.*

Proof. The result for $G(t) = P_1(t)^{e_1} \cdots P_k(t)^{e_k}$ with each $P_i(t)^{e_i} \in \mathcal{P}_f$. Given a solution $\mathbf{y}_j$ to $f(\mathbf{y}_j) \equiv 0 \pmod{P_j(t)^{e_j}}$ for each j, let $\mathbf{y} \equiv \mathbf{y}_j \pmod{P_j(t)^{e_j}}$ for each j, by the Chinese Remainder Theorem, and then $f(\mathbf{y}) \equiv 0 \pmod{G(t)}$. □

Lemma 5.4 (Minimal elements in a residue class for polynomial congruences)**.** *If $G(t) \in \mathbb{Z}[t]$ for which there exist $y_1(t), \dots, y_m(t) \in \mathbb{Z}[t]$ such that $G(t)$ divides $f(\mathbf{y}(t))$ then there exist $u_1(t), \dots, u_m(t) \in \mathbb{Z}[t]$ with each $\deg u_i \le \deg G - 1$ such that*

$$G(t) \text{ divides } f(u_1(t), \dots, u_m(t)).$$

Proof. Suppose $G(t)$ divides $f(y_1(t), \dots, y_m(t))$ for some $y_1(t), \dots, y_m(t) \in \mathbb{Z}[t]$, and now select the solution of smallest possible degree. Let $G = g_0 t^D + \dots$ so that G divides $f(g_0 y_1(t), \dots, g_0 y_m(t))$. If $\deg y_j \ge D$ for some j then writing $y_j = c_0 t^d + \dots$ with $d \ge D$ let $v_j(t) := g_0 y_j(t) - c_0 t^{d-D} G(t)$ which has lower degree than y_j and $v_i(t) = g_0 y_i(t)$ if $i \ne j$ so that $G(t)$ divides $f(v_1(t), \dots, v_m(t))$, contradicting the minimality of the degrees of the y_j. Hence we deduce that there are solutions with each $\deg u_i \le D - 1$. □

Lemma 5.5. *Let $f(x_1, \dots, x_m) \in \mathbb{Z}[x_1, \dots, x_m]$ be irreducible. Suppose that $G(t)$ is a product of elements of $\mathcal{P}_f$ so there exist a nonsingular solution $(u_1(t), \dots, u_m(t)) \in \mathbb{Z}[t]^m$, with each $\deg u_i \le \deg G - 1$ for which $G(t)$ divides $f(u_1(t), \dots, u_m(t))$. Then*

$$g(x_1, \dots, x_m)[t] = f(x_1 G(t) + u_1(t), \dots, x_m G(t) + u_m(t))/G(t) \in \mathbb{Z}[x_1, \dots, x_m, t]$$

is irreducible, I_g is contained inside the convex hull of I_f and $H_g = H_f$.

Proof. Let $y_i(t) = x_i(t)G(t) + u_i(t)$ for each so that $f(\mathbf{y}) \equiv f(\mathbf{u}) \equiv 0 \pmod{G(t)}$. Therefore $g(x_1, \dots, x_m)[t] \in \mathbb{Z}[x_1, \dots, x_m, t]$. Now

$$g(x_1, \dots, x_m)[t] = \sum_{\mathbf{i} \in I_g} c_{\mathbf{i}}(t) x_1^{i_1} \cdots x_m^{i_m} \in \mathbb{Z}[x_1, \dots, x_m, t] \tag{5.1}$$

When we expand the polynomial f to obtain g, we see that the jth co-ordinate is $\mathbb{Z}[t]$-linear in x_j, which means that when we expand the $x_1^{i_1} \cdots x_m^{i_m}$ term with $(i_1, \dots, i_m) \in I_f$, we get monomials $x_1^{j_1} \cdots x_m^{j_m}$ with each $j_\ell \le i_\ell$ including monomial with each $j_\ell \le i_\ell$. Therefore I_g is contained inside the convex hull of I_f and $H_g = H_f$. In particular if $\mathbf{i} \in H_f = H_g$ then $b_{\mathbf{i}}(t) = G(t)^{d-1} c_{\mathbf{i}}$ by comparing (1.1) with (5.1).

Finally we prove that $g(x_1, \dots, x_m)[t]$ is irreducible:

If $g(x_1, \dots, x_m)[t]$ is reducible then then one of the factors must be a polynomial $h(t)$ in t else we could factor $f(x_1, \dots, x_m)$ by substituting an integer n in for t such that $G(n) \ne 0$, and then making a linear change of variables. Therefore there exists an irreducible polynomial $Q(t)$ which divides $g(x_1, \dots, x_m)[t]$.

Now $Q(t)$ divides $g(x_1, \dots, x_m)[t]$ as presented in (5.1) so $Q(t)$ divides every $c_{\mathbf{i}}(t)$. In particular if $\sum_j i_j = d$ then $c_{\mathbf{i}}(t) = G(t)^d$ and so $Q(t)$ divides $G(t)$ (and therefore $Q(t) \in \mathcal{P}_f$). We now compute $g(x_1, \dots, x_m)[t] \pmod{G}$: By construction if $s \ge 1$ then $G(t)^{s-1}$ divides $c_{\mathbf{i}}(t)$ when $\sum_j i_j = s$, so we can restrict our attention to $s = 0$ and 1. Therefore

$$g(x_1, \dots, x_m)[t] \equiv \frac{f(\mathbf{u}(t))}{G(t)} + \sum_{j=1}^{m} f_j(\mathbf{u}(t)) \cdot x_j \pmod{G(t)} \text{ where } f_j(\mathbf{u}(t)) := \left.\frac{\partial f(\mathbf{x})}{\partial x_j}\right|_{\mathbf{x}=\mathbf{u}(t)}.$$

Now $Q(t)$ divides $g(x_1, \dots, x_m)[t]$ and so $Q(t)$ divides $f(\mathbf{u}(t))$ and each $f_j(\mathbf{u}(t))$ which contradicts that $f(\mathbf{u}(t))$ is non-singular. □

6. Creating one variable irreducible polynomials

Lemma 6.1. *Let $g(x_1,\dots,x_m)\in\mathbb{Z}[x_1,\dots,x_m]$. There exist positive integers $n_1,\dots,n_m$ with $n_1+\cdots+n_m\le m+\deg g$ such that $g(n_1,\dots,n_m)\neq 0$.*

Proof. We prove this by induction on m. If $m=1$ then g is a monomial so we can take $n_1=1$. For any $m>1$ we write g as a polynomial in $\mathbb{Z}[y_1,\dots,y_{m-1}][y_m]$ which has degree d, say, in y_m. The coefficient of y_m^d is a polynomial of degree $\le \deg g-d$ in $y_1,\dots,y_{m-1}$. By the induction hypothesis there exist positive integers $n_1,\dots,n_{m-1}$ with $n_1+\cdots+n_{m-1}\le m-1+\deg g-d$ such that the leading coefficient of g is non-zero, and therefore there exists $n_m\le d+1$ such that $g(n_1,\dots,n_m)\neq 0$. □

Corollary 6.2. *Let $f(x_1,\dots,x_m)\in\mathbb{Z}[x_1,\dots,x_m]$. For any given $\mathbf{d}=(d_1,\dots,d_m)\in\mathbb{Z}^m_{\ge 0}$ there exist positive integers $n_1,\dots,n_m$ with $n_1+\cdots+n_m\le m+\deg f$ such that the leading term of $f(x_1(t),\dots,x_m(t))$, when each $x_j(t)=n_jt^{d_j}+\cdots$ is a polynomial of degree d_j, is of the form Ct^D where $D:=\max_{\mathbf{h}\in H_f}\mathbf{h}\cdot\mathbf{d}$ and C is a bounded positive integer. Here an upper bound on C can be determined explicitly in terms of the polynomial f and is independent of the choice of d_i's.*

Proof. Given $\mathbf{d}=(d_1,\dots,d_m)\in\mathbb{Z}^m_{\ge 0}$ suppose that $x_j(t)=n_jt^{d_j}+\cdots$ is a polynomial of degree d_j. Let $D:=\max_{\mathbf{h}\in H_f}\mathbf{h}\cdot\mathbf{d}$ so that $f(x_1(t),\dots,x_m(t))$ is a polynomial of degree D with leading coefficient given by $g_{\mathbf{d}}(n_1,\dots,n_m)$ where

$$g_{\mathbf{d}}(y_1,\dots,y_m)=\sum_{\substack{(i_1,\dots,i_m)\in I_f:\\ d_1i_1+\cdots+d_mi_m=D}} a_{i_1,\dots,i_m}y_1^{i_1}\cdots y_m^{i_m}\in\mathbb{Z}[y_1,\dots,y_m].$$

We can then select the n_i as in Lemma 6.1 to guarantee that the leading coefficient $g_{\mathbf{d}}(n_1,\dots,n_m)$ is non-zero. There are only finitely many distinct polynomials $g_{\mathbf{d}}(\mathbf{y})$ since there are just finitely many subsets of I_f. The result follows. □

Proposition 6.3. *Given $\mathbf{d}=(d_1,\dots,d_m)\in\mathbb{Z}^m_{\ge 0}$, $\mathbf{e}\in\mathbb{R}_{>0}$ let*

$$R:=\mathbf{e}\cdot\mathbf{d},\ N:=\mathbf{1}\cdot\mathbf{d}\ \text{and}\ e_0=\min_{1\le i\le m}e_i.$$

Select integers $n_1,\dots,n_m$ and $C:=g_{\mathbf{d}}(n_1,\dots,n_m)$ as in Corollary 6.2. There are $2^NT^R(1+O(1/T^{e_0/2}))$ m-tuples of irreducible polynomials $\mathbf{x}(t)=(x_1(t),\dots,x_m(t))\in\mathbb{Z}[t]^m$ where $x_i(t)$ has leading term $n_it^{d_i}$ and $\|x_i(t)\|\le T^{e_i}$, for which $f(\mathbf{x}(t))$ is non-singular and has leading term Ct^D with $\|f(\mathbf{x}(t))\|\ll_f T^E$ where

$$D:=\max_{\mathbf{h}\in H_f}\mathbf{h}\cdot\mathbf{d}\quad\text{and}\quad E:=\max_{\mathbf{h}\in H_f}\mathbf{h}\cdot\mathbf{e}.$$

Proof. Let $x_i(t)=\sum_{j=0}^{d_i}x_{i,j}t^j$ for each i where the $x_{i,j}$ are all variables except that $x_{i,d_i}=n_i$; we will now prove

$$F(t,x_{1,0},\dots,x_{m,d_m}):=f(x_1(t),\dots,x_m(t))$$

is irreducible: If $t=0$ and $x_{i,j}=0$ for all $j\ge 1$ then

$$F(0,x_{1,0},0,\dots,0,x_{2,0},0\dots,0,x_{m,0},0\dots,0)=f(x_{1,0},\dots,x_{m,0})$$

which is irreducible (as the $x_{j,0}$ are variables), and therefore $F(\cdot)$ must be irreducible.

The number of $f(x_1(t),\dots,x_m(t))$ constructed (irreducible or not) is given by

$$\#\{x_{i,j}\in\mathbb{Z}:|x_{i,j}|\le T^{e_i},1\le i\le m,0\le j\le d_i-1\}=\prod_i(2T^{e_i}+O(1))^{d_i}=2^NT^R(1+O(T^{-e_0})).$$

We need to show that the number of these for which $f(x_1(t),\dots,x_m(t))$ has degree $< D$, or for which $f(x_1(t),\dots,x_m(t))$ is reducible, or for which some $x_j(t)$ is reducible, has much smaller order. As discussed in section 5, if $f(x_1(t),\dots,x_m(t))$ is irreducible then it is non-singular.

We note that $f(\mathbf{x}(t))$ has leading term Ct^D by Corollary 6.2.

Since $F(t, x_{1,0},\dots,x_{m,d_m})$ is irreducible we apply Lemma 4.1 with $n = N$, where the T_ℓ are given by the $x_{i,j}$, and so the number of choices of the $x_i(t)$ for which $f(x_1(t),\dots,x_m(t))$ is reducible is

$$\ll \prod_i T^{e_i d_i} \cdot (\log T)/T^{e_0/2} = T^{R-e_0/2}.$$

Finally we need to ensure that each $x_i(t)$ is irreducible. Bhargava [2] proved van de Waerden's conjecture that $\ll (T^{e_i})^{d_i-1}$ of the $x_i(t)$ are reducible for each i, and thus

$$\ll \sum_i T^{R-e_i} \ll \ T^{R-e_0}$$

of our choices of the set $x_1(t),\cdots,x_m(t)$. Our count for the number of m-tuples of irreducible polynomials for which $f(x_1(t),\dots,x_m(t))$ is non-singular and irreducible of degree D now follows.

For the second result we note that the sum of the absolute values of the coefficients of $x_i(t)$ is $\le d_i T^{e_i}$, so the sum of the absolute values of the coefficients of $f(x_1(t),\dots,x_m(t))$ is

$$\le \sum_{(i_1,\dots,i_m)\in I_f} |a_{i_1,\dots,i_m}|\cdot(d_1T^{e_1})^{i_1}\cdots(d_mT^{e_m})^{i_m} \ll_f T^E. \qquad \square$$

Corollary 6.4. *Let $f(x_1,\dots,x_m) \in \mathbb{Z}[x_1,\dots,x_m]$ be irreducible, let $G(t)$ be a product of elements of $\mathcal{P}_f$ and define $g(x_1,\dots,x_m)[t] \in \mathbb{Z}[x_1,\dots,x_m,t]$ as in Lemma 5.5. Given integers $d_1,\dots,d_m \ge \deg G$ and reals $e_1,\dots,e_m > 0$ define R, N, E, e_0 as in Proposition 6.3, and*

$$R' := R - \left(\sum_i e_i\right)\deg G, D' := D - \deg G \text{ and } N' := N - m\deg G.$$

Then there are $2^{N'}T^{R'}(1+O(1/T^{e_0/2}))$ m-tuples of irreducible polynomials $\{x_i(t) : \deg x_i = d_i\} \in \mathbb{Z}[t]^m$ with coefficients $\ll_G T^{e_i}$ for which $g(x_1(t),\dots,x_m(t))[t]$ is non-singular and irreducible of degree D'. Moreover, the coefficients of $g(x_1(t),\dots,x_m(t))[t]$ are all $\ll_f T^E$. Here $D' \ge (d-1)\deg G$.

Proof. We let each $x_i(t) = y_i(t)G(t) + u_i(t)$ with the u_i chosen as in Lemma 5.5, and each $y_i(t)$ has degree $d_i - \deg G$ with all coefficients integers of size $\le T^{e_i}$. Since $H_g = H_f$ the argument is then completely analogous to that of Proposition 6.3. We note that $D = \sum_j d_j i_j \ge \sum_j i_j \deg G = d\deg G$. $\square$

7. Counting the number of distinct fields created

Lemma 7.1. *Suppose that $x_1(t),\dots,x_m(t) \in \mathbb{Z}[t]$ are irreducible of degrees $d_1,\dots,d_m$ with $(d_1,\dots,d_m) = 1$. If α is an algebraic number then*

$$\mathbb{Q}(x_1(\alpha),\dots,x_m(\alpha)) = \mathbb{Q}(\alpha).$$

Proof. Now $[\mathbb{Q}(\alpha) : \mathbb{Q}(x_j(\alpha))] = d_j$ since $x_j(t)$ is irreducible of degree d_j and

$$\mathbb{Q}(\alpha) \supset \mathbb{Q}(x_1(\alpha),\dots,x_m(\alpha)) \supset \mathbb{Q}(x_j(\alpha))$$

so that $d := [\mathbb{Q}(\alpha) : \mathbb{Q}(x_1(\alpha), \dots, x_m(\alpha))]$ divides each d_j. But then d divides $(d_1, \dots, d_m) = 1$ and so $d = 1$; the result follows. □

Lemma 7.2. *For any given number field K, the number of irreducible polynomials $F(x) \in \mathbb{Z}[x]$ of degree D with $\|F\| \ll T^E$, bounded leading coefficient and $\mathbb{Q}[x]/(F(x)) \cong K$ is $\ll_D T^{E+o(1)}$.*

Proof. More generally, let K be a given number field of degree D. Proposition 2.2 of [11] states that the number of monic polynomials $f(x) \in \mathbb{Z}[x]$ for which $\mathbb{Q}[x]/(f(x)) \cong K$ with $\|f\| \le H$ is $\ll_D H(\log H)^{D-1}$. Now if $F(x) = \sum_{i=0}^{D} c_i x^i$ with $c_D = c$ then let $f(x) = x^D + \sum_{i=0}^{D-1} c^{D-1-i} c_i x^i$ so that $f(cx) = F(x)$ and therefore $\mathbb{Q}[x]/(F(x)) \cong \mathbb{Q}[x]/(f(x))$ with f monic. Thus we can apply Proposition 2.2 of [11] to the $f(x)$ for each $c \le C$. The result follows taking $H \asymp c^D T^E \ll C^D T^E \ll_D T^E$. □

Lemma 7.3. *Let $g(t)$ be an irreducible polynomial in $K[t]$ of degree D. If $g(\alpha) = 0$ then $\operatorname{disc}(K(\alpha)/K) \ll_D \|g\|^{2D-2}$.*

Proof. It is known that $\operatorname{disc}(g)/\operatorname{disc}(L(\alpha)) \in \mathbb{Z}^2$, so $\operatorname{disc}(L(\alpha)) \le \operatorname{disc}(g)$. Now $\operatorname{disc}(g)$ is a homogenous polynomial in its coefficients of degree $2D-2$ and so $\operatorname{disc}(g) \ll_D \|f\|^{2D-2}$. □

Proof of Theorem 1.1. Fix $\mathbf{h} \in H$ and $\mathbf{r} \in R(\mathbf{h})$. If D is divisible by $g(\mathbf{h})$ and is sufficiently large then we determine $d_1, \dots, d_m$ by Proposition 3.1 which can be used in Proposition 6.3 to show that $D \in D(C)$. If we fix all but one of the $x_i(t)$ in Proposition 3.1 then we obtain the same polynomial no more than d times. Lemma 7.2 then implies that $D \in D(C)^{\inf}$. This in turn implies that $G(C)$ divides $g(\mathbf{h})$.

There exist integers $D_1, \dots, D_n \in D(C)^{\inf}$ such that $G(C) = \gcd(D_1, \dots, D_n)$. For any $b \pmod{g(\mathbf{h})}$ such that $G(C) \mid b$, there exist positive integers $m_1, \dots, m_k$ such that $B := m_1 D_1 + \cdots + m_k D_k \equiv -b \pmod{D}$. Therefore there is a polynomial $G(t)$ which is a product of elements of $\mathcal{P}_f$ for which $\deg G = B$. Now suppose that $D \equiv b \pmod{g(\mathbf{h})}$ and is sufficiently large. We use Proposition 3.1 to determine $d_1, \dots, d_m$ so that $D = \mathbf{d} \cdot \mathbf{h} + B$ and then use Corollary 6.4 to show that $D \in D(C)$, obtaining that $D \in D(C)^{\inf}$ using Lemma 7.2 as in the previous paragraph. □

Proposition 7.4. *Let C be an irreducible hypersurface given by a polynomial f in m variables with integer coefficients, of degree d. Suppose that $H = H_f$ and $J \in \mathcal{J}_f$, so that the reasonable image hypothesis holds for H_J. Let $\mathbf{d} \in \mathbb{Z}_{\ge 0}^m$ and $\mathbf{e} \in [0,1]^m$.*

There are $\gg T^{R_J - o(D))}$ distinct non-singular, irreducible polynomials $f(\mathbf{x}(t))$ of degree D with $\|f(\mathbf{x}(t))\| \ll_f T^E$, where each $x_i(t)$ is an irreducible polynomial of degree d_i with $\|x_i(t)\| \le T^{e_i}$. where $D := \max_{\mathbf{h} \in H_f} \mathbf{h} \cdot \mathbf{d}$, $E := \max_{\mathbf{h} \in H} \mathbf{h} \cdot \mathbf{e}$ and $R_J := \mathbf{e}_J \cdot \mathbf{d}_J$.

Proof. We fix any one solution $\mathbf{y}(t)$ given by Proposition 6.3, so that

$$F_J((x_j)_{j \in J}, t) := f(x_1, \cdots, x_m)|_{x_i = y_i(t) \text{ for all } i \in \overline{J}}$$

is irreducible (as we know that there is a specialization that is irreducible). Proposition 6.3 applied to $F_J((x_j)_{j \in J}, t)$ then yields $\sim 2^{N_J} T^{R_J}$ m-tuples of irreducible polynomials $\mathbf{x}(t) \in \mathbb{Z}[t]^m$ where $x_i(t)$ has degree d_i and $\|x_i(t)\| \le T^{e_i}$ for which $f(\mathbf{x}(t))$ is non-singular and irreducible of degree D with $\|f(\mathbf{x}(t))\| \ll_f T^E$ where $N_J := \mathbf{1}_J \cdot \mathbf{d}_J$.

The same polynomial $g(t)$ is given by $F_J((x_j)_{j \in J}, t)$ no more than $T^{o(D)}$ times by the reasonable image hypothesis (since $\|\mathbf{x}(t)\| \le T$ and each $d_j \le D$ by hypothesis), and so we have $\gg T^{R_J - o(D)}$ *distinct* non-singular, irreducible polynomials $f(\mathbf{x}(t))$. □

By proceeding analogously but now using Corollary 6.4 instead of Proposition 6.3, we obtain the following:

Corollary 7.5. *Assume the hypothesis of Proposition 7.4, let $G(t)$ be a product of elements of $\mathcal{P}_f$ with $\mathbf{d} \in \mathbb{Z}^m_{\geq \deg G}$ and define $g(\mathbf{x})[t]$ as in Lemma 5.5.*

There are $\gg T^{R'_J - o(D)}$ distinct non-singular, irreducible polynomials $g(\mathbf{x}(t))$ of degree D' with $\|g(\mathbf{x}(t))\| \ll_f T^E$, where each $x_i(t)$ is an irreducible polynomial of degree d_i with $\|x_i(t)\| \leq T^{e_i}$, where $D' := D - \deg G$ and $R'_J := R_J - (\mathbf{e}_J \cdot \mathbf{1}_J)\deg G$.

Proposition 7.6. *Let C be an irreducible hypersurface given by a polynomial f in m variables with integer coefficients, of degree d, and let $G(t)$ be a product of elements of $\mathcal{P}_f$ of degree n (including the possibility $G = 0$). We assume hypotheses and notation of Proposition 7.4 and Corollary 7.5 so that $J \in \mathcal{J}_f$. If D is an integer that can be written as*

$$D := \max_{\mathbf{h} \in H_f} \mathbf{h} \cdot \mathbf{d}$$

where $\mathbf{d} \in \mathbb{Z}^m_{\geq n}$ with $(d_1, \dots, d_m) = 1$ then

$$\#\{\text{Fields } K \in \mathcal{F}(C) : [K : \mathbb{Q}] = D - n \text{ and } \mathrm{disc}(K/\mathbb{Q}) \leq X\} \gg X^{\frac{\mathbf{e}_J \cdot \mathbf{d}_J}{2DE} - O(\frac{1}{D}) - o(1)}.$$

Proof. We prove this first with $G = 0$ so that $\deg G = 0$. In Proposition 7.4 we constructed $\gg T^{R_J - o(D)}$ distinct, non-singular degree D irreducible polynomials $f(\mathbf{x}(t))$ with coefficients all $\ll T^E$, where each $x_j(t)$ is irreducible. Then Lemma 7.2 implies that these generate $\gg T^{R_J - o(D)}$ distinct fields $\mathbb{Q}[t]/(f(\mathbf{x}(t)))$ since $E \ll 1$. Any root α of $f(\mathbf{x}(t)) = 0$ therefore generates a field of degree D, and $\mathbb{Q}(\mathbf{x}(\alpha)) = \mathbb{Q}(\alpha)$ by Lemma 7.1; moreover $\mathrm{disc}(\mathbb{Q}(\alpha)/\mathbb{Q}) \ll_D T^{2(D-1)E}$ by Lemma 7.3. Therefore we have constructed $\gg X^{\frac{R_J - o(D)}{2(D-1)E}}$ fields of degree D with discriminant $\leq X$ which contain a point on $f(\mathbf{x}) = 0$.

Now $E \ll 1$ so that $R_J = \mathbf{e}_J \cdot \mathbf{d}_J + O(1) \ll D$, so that $\frac{R_J - o(D)}{2(D-1)E} = \frac{\mathbf{e}_J \cdot \mathbf{d}_J}{2DE} - O(\frac{1}{D}) - o(1)$. The result for $G = 0$ follows.

We follow the same route when $G \neq 0$ but using Corollary 7.5 in place of Proposition 7.4, noting that for a given G we have $(\mathbf{e}_J \cdot \mathbf{1}_J)\deg G \ll 1$ and so $R'_J = R_J + O(1)$. □

Proposition 7.7. *Let C be an irreducible hypersurface given by a polynomial f in m variables with integer coefficients, of degree d, with $H = H_f$ and suppose that $n \in \mathit{Frob}(D(C))$. Assume that $J \in \mathcal{J}_f$. If D is divisible by $g(\mathbf{h})$ where $\mathbf{h} \in H$ and is sufficiently large then*

$$\#\{\text{Fields } K \in \mathcal{F}(C) : [K : \mathbb{Q}] = D - n \text{ and } \mathrm{disc}(K/\mathbb{Q}) \leq X\} \gg X^{\frac{1}{2}\mathrm{Exp}_J(H) - o_{D\to\infty}(1)}.$$

Proof. If $n \neq 0$ then we can construct elements of $\mathcal{P}_f$ from points that lead to elements of $D(C)$, and therefore construct $G(t)$ as in lemma 5.4 of degree n, for any $n \in \mathrm{Frob}(D(C))$.

Select $\mathbf{r} \in R(\mathbf{h})$. There exists $\mathbf{d} \in \mathbb{Z}^m_{\geq 1}$ with $(d_1, \dots, d_m) = 1$ and each $d_j = \frac{Dr_j}{\mathbf{r}\cdot\mathbf{h}} + O((\log D)^2)$ for which $D = \mathbf{d} \cdot \mathbf{h}$ and $D > \mathbf{d} \cdot \mathbf{h}'$ for all $\mathbf{h}' \in H$ by Proposition 3.1. This also implies that each $d_j \geq \deg G$ (as D is sufficiently large). Therefore the exponent in Proposition 7.6 is $\frac{1}{2}$ of

$$\frac{\mathbf{e}_J \cdot \mathbf{d}_J}{DE} = \frac{\mathbf{e}_J \cdot \mathbf{r}_J}{(\mathbf{h}_r \cdot \mathbf{r})(\mathbf{h}_e \cdot \mathbf{e})} + O\left(\frac{(\log D)^2}{D}\right)$$

where $\mathbf{h}_r \in H$ is selected so that $\mathbf{h}_r \cdot \mathbf{r}$ is maximal and $\mathbf{h}_e \in H$ is selected so that $\mathbf{h}_e \cdot \mathbf{e}$ is maximal. Now to maximize this expression we evidently can take $\mathbf{e} = \mathbf{e}_J$ since any non-zero co-ordinate outside J makes the denominator larger without effecting the numerator. We

may also divide numerator and denominator through by $\|\mathbf{e}\|$ so that $\mathbf{e} \in R(\mathbf{h}_e)$ and again $\mathbf{h}_e \in H_J$. We want to maximize the above over all the possible choices for $\mathbf{e}, \mathbf{r}, \mathbf{h}_e, \mathbf{h}_r$ but the sets $R(*)$ are open so the above is $\geq \mathrm{Exp}_J(H) - \epsilon$ if D is sufficiently large. The result follows. □

Corollary 7.8. *Let C be an irreducible hypersurface given by a polynomial f in m variables with integer coefficients, of degree d, with $H = H_f$. If D is divisible by $G(H)$ and is sufficiently large, and X is sufficiently large then*

$$\#\{\textit{Fields } K \in \mathcal{F}(C) : [K:\mathbb{Q}] = D \textit{ and } \mathrm{disc}(K/\mathbb{Q}) \leq X\} \gg X^{\frac{1}{2}\mathrm{Exp}(C) - o_{D\to\infty}(1)}.$$

Proof. Fix $\mathbf{h}_0 \in H$. Since $G(H) = \gcd(g(\mathbf{h}) : \mathbf{h} \in H)$, there exists integers $a_{\mathbf{h}}$ such that $G(H) = \sum_{\mathbf{h}\in H} a_{\mathbf{h}} g(\mathbf{h})$. Select $A_{\mathbf{h}}$ to be the least non-negative residue of $a_{\mathbf{h}} \pmod{g(\mathbf{h_0})}$ so that $\sum_{\mathbf{h}\in H} A_{\mathbf{h}} g(\mathbf{h}) \equiv G(H) \pmod{g(\mathbf{h_0})}$.

Next we apply Proposition 7.7 with $n = 0$ and $J \in \mathcal{J}$, so if $\mathbf{h} \in H$ and $D_{\mathbf{h}}$ is sufficiently large with $D_{\mathbf{h}} \equiv g(\mathbf{h}) \pmod{g(\mathbf{h_0})}$ then $D_{\mathbf{h}} \in D(H) \subset D(C)$. This implies that $n_1 = \sum_{\mathbf{h}\in H} A_{\mathbf{h}} D_{\mathbf{h}} \in \mathrm{Frob}(D(H)) \subset \mathrm{Frob}(D(C))$, and $n_1 \equiv G(H) \pmod{g(\mathbf{h_0})}$. Therefore $n_k := kn_1 \in \mathrm{Frob}(D(C))$ and $n_k \equiv kG(H) \pmod{g(\mathbf{h_0})}$ for $0 \leq k < g(\mathbf{h_0})/G(H)$.

Now if D is divisible by $G(H)$ and is sufficiently large then it can be written as $D' - n_k$ where D' is divisible by $g(\mathbf{h})$ with $\mathbf{h} \in H$, for some k. The result then follows from applying Proposition 7.7 for every $J \in \mathcal{J}_f$ to get the exponent $\frac{1}{2}\mathrm{Exp}(H_f, \mathcal{J}_f) - o(1) = \frac{1}{2}\mathrm{Exp}(C_f) - o(1)$. □

We do not use any information about C in the proof of Corollary 7.8 other than H_f and $\mathcal{J}_f$. This means that any new points on C that might arise from the arithmetic of the particular choice of coefficients of f, with given values of H and $\mathcal{J}$, have not been included in the calculation. Thus, for any f with given H_f and $\mathcal{J}_f$ we prove the following:

Proof of Theorem 2.1. The result holds for any sufficiently large D that is divisible by $G(H)$, by Corollary 7.8. Now $G(C)$ divides $G(H)$ and if $G(C) < G(H)$ then there exists $n_1, \dots, n_\ell \in D(C)$ for which $G(C) = \gcd(G(H), n_1, \dots, n_\ell)$, by definition.

We now proceed analogously to the proof of Corollary 7.8: First find integers a_i for which $\sum_{i=0}^{\ell} a_i n_i = G(C)$ (where $n_0 = G(H)$), select A_i to be the least non-negative residue of $a_i \pmod{G(H)}$. This implies there are integers $N_j \in D(C)$ with $N_j \equiv jG(C) \pmod{G(H)}$, and therefore we can apply Proposition 7.7 for every $J \in \mathcal{J}_f$ to obtain our claim. □

8. Frobenius sets

Corollary 8.1. *If there are non-singular $P_i(t)$ of degree m_j in $\mathcal{P}_f$ for $1 \leq i \leq r$ then*

$$d \deg_{x_j} f + \mathrm{Frob}(d, (d-1)m_1, \dots, (d-1)m_r) \subset D(C_f)^{\mathrm{inf}}.$$

Proof. For any integers $e_1, \dots, e_r \geq 0$, let $G(t) = \prod_i P_i(t)^{e_j}$ so that $n = \deg G = \sum_i e_i m_i$. For any given $k \geq 0$ let $d_i = n + k$ for all $i \neq j$ and $d_j = n + \max\{k, \deg_{x_j} f\}$. Since the largest co-ordinate of d_j is the jth co-ordinate, we must have $h_j = \deg_{x_j} f$. By Corollary 6.4 we have

$$(d-1)n + dk + \max\{0, \deg_{x_j} f - k\} \deg_{x_j} f = \max_{\mathbf{h}\in H_f} \mathbf{h}\cdot\mathbf{d} - n \in D(C_f)^{\mathrm{inf}}.$$

Now the possible values of n are the integers in the set $\mathrm{Frob}(m_1, \dots, m_r)$. The result follows from taking $k \geq \deg_{x_j} f$. □

Proof of Theorem 1.3. The hypothesis implies that we can take $m_1 = r = 1$ in Corollary 8.1 so that $d \min_j \deg_{x_j} f + \mathrm{Frob}(d,(d-1)) \subset D(C_f)^{\inf}$.

We observe that if $a \equiv -j \pmod d$ for $1 \le j \le d-1$ then $a \in \mathrm{Frob}(d-1,d)$ if and only if $a \ge (d-1)j$. Therefore the largest integer not in $\mathrm{Frob}(d-1,d)$ must be $(d-1)(d-1)-d = d^2-3d+1$. The result follows as $\deg_{x_j} f \le d$. □

8.1. **Superelliptic hypersurfaces.** Let f be the projective version of

$$Y : ay^q = g(x_2, \dots, x_{m-1})$$

where q divides $d := \deg g$ so that $\deg f = d$. (Twisted) hyperelliptic curves are the example $q = 2, m = 3$. We projectivize to obtain

$$f(x_1, \dots, x_m) = ax_0^q x_m^{d-q} - g(x_2/x_m, \dots, x_{m-1}/x_m)x_m^d.$$

Evidently $(q, 0, \cdots, 0, d-q) \in H_f$.

If α is a non-singular point on Y of degree r then we obtain a a non-singular point β on C_f of degree r with $\beta_m = 1$, and corresponding polynomial $P_\beta(t) \in \mathcal{P}_f$ of degree r. Using the Chinese Remainder Theorem with several such points we obtain $G(t) = \prod_\beta P_\beta(t)$ together with a non-singular solution $f(u(t)) \equiv 0 \pmod G(t)$ where $u_m(t) = 1$.

We now apply Corollary 6.4 but with $d_m = 0, d_j = \deg G$ for $2 \le j \le m-1$, and then d_1 is any integer with $d_1 \ge \frac{d}{q} \deg G$, so that the first monomial has highest degree when we substitute in polynomials $x_j = x_j(t)$ of degree d_j. Taking each $e_i = 1$ we deduce that $D = qd_1$ and so $D' = qd_1 - \deg G \in D(C_f)^{\inf}$. Writing $d_1 = \frac{d}{q} \deg G + e$ for $e \ge 0$ we see that $(d-1)\deg G + q\mathbb{Z}_{\ge 0} \subset D(C_f)^{\inf}$.

Now if there is a non-singular rational point on our superelliptic hypersurface then $t \in \mathcal{P}_f$ and taking $G(t) = t^e$ for any $e \ge 0$ we deduce that $\mathrm{Frob}(d-1,q) \subset D(C_f)^{\inf}$. The largest integer not in $\mathrm{Frob}(d-1,q)$ is $(d-1)(q-1) - q = dq - 2q - d + 1$ and so every integer $\ge (d-2)(q-1)$ belongs to $D(C_f)^{\inf}$. If $q = 2$ then $\mathcal{E}(C_f) \subset \{1, 3, \dots, d-3\}$, which proves Theorem 1.7(b).

9. Lower bounds on $\mathrm{Exp}(C)$

Suppose that f satisfies the reasonable image hypothesis (RIH) so that $\{1, \dots, m\} \in \mathcal{J}_f$. In section 2.3 we saw that this implies that $\mathrm{Exp}(C_f) \ge \frac{m}{d^2}$.

Now if f doesn't satisfy RIH, but f_J does, then we obtain a lower bound $\mathrm{Exp}_J(H)$ by letting $\mathbf{e} = \mathbf{1}_J/\sqrt{\#J}$ so that $\mathbf{e} \cdot \mathbf{h_e} = \deg H_J/\sqrt{\#J}$, and then

$$\mathrm{Exp}(C_f) \ge \mathrm{Exp}_J(H) \ge \max_{\mathbf{h}_r \in H} \max_{\mathbf{r} \in \overline{R(\mathbf{h}_r)}} \frac{\mathbf{1}_J \cdot \mathbf{r}}{(\deg H_J)(\mathbf{r} \cdot \mathbf{h_r})} \ge \frac{\#J}{(\deg H_J)^2} \ge \frac{\#J}{d^2}$$

letting $\mathbf{r} = \mathbf{1}_J$. In particular if $J = \{j\}$ then $\mathrm{Exp}(C_f) \ge \frac{1}{(\deg_{x_j} f)^2} \ge \frac{1}{d^2}$ as we showed in section 2.3. We now study various interesting special cases:

9.1. **Diagonal surfaces:** If $f = a_1 x_1^d + \cdots + a_m x_m^d$ then

$$H_f = \{\mathbf{h}_i := (0, \dots, 0, d, 0, \dots, 0), 1 \le i \le m\}.$$

This gives that $\overline{R(\mathbf{h}_i)} = \{\mathbf{x} \in \mathbb{R}^m_{\geq 0} : \|x\| = 1 \text{ and } x_i \geq x_j \text{ for all } j\}$. Therefore if $\mathbf{x} \in \overline{R(\mathbf{h}_1)}, \mathbf{y} \in \overline{R(\mathbf{h}_2)}$ then each $x_i y_j \leq x_1 y_2$ so that

$$\frac{\mathbf{x} \cdot \mathbf{y}}{(\mathbf{x} \cdot \mathbf{h}_1)(\mathbf{y} \cdot \mathbf{h}_2)} = \frac{\sum_{i=1}^m x_i y_i}{dx_1 \cdot dy_2} \leq \frac{m x_1 y_2}{d^2 x_1 y_2} = \frac{m}{d^2}$$

and so $\mathbf{Exp}(H) = \frac{m}{d^2}$ if f satisfies the RIH. In fact the proof yields that we attain the bound only if each $x_i = x_1$ and each $y_j = y_2$ so that $\mathbf{x} = \mathbf{y} = \frac{1}{\sqrt{m}}\mathbf{1}$. Recall that we showed in section 2.1 that f cannot satisfy the RIH if $m > d^2$.

9.2. **Superelliptics:** Let $f(x_1, x_2, x_3)$ be the homogenization of $y^q = g(x)$ where $\deg g = d > q > 1$ and $g(0) \neq 0$. Then $H_f = \{(d, 0, 0), (0, 0, d), (0, q, d-q)\}$. Now $\mathbf{Exp}_{\{2\}}(H) = \frac{1}{q^2}$ taking $\mathbf{e} = (0, 1, 0)$. If $\mathbf{r} = \mathbf{e} = (\frac{q}{(q^2+d^2)^{1/2}}, \frac{d}{(q^2+d^2)^{1/2}}, 0) \in \overline{R((d, 0, 0))}$, then

$$\mathbf{Exp}_{\{1,2\}}(H) \geq \frac{1}{q^2} + \frac{1}{d^2},$$

and we have $\mathbf{Exp}_{\{1,2,3\}}(H) \geq \frac{3}{d^2}$. One can compare this to the exponents found in [12], [9], [3] who count fields generated by points on elliptic, hyperelliptic, and superelliptic curves, respectively.

9.3. **A symmetric polynomial:** If $f = x^a y^b + y^a z^b + z^a x^b$ where $a > b \geq 1$ then $H = \{(a, b, 0), (0, a, b), (b, 0, a)\}$. Taking $\mathbf{r} = \mathbf{e} = \frac{1}{\sqrt{2}(a^2+ab+b^2)^{1/2}}(a, a+b, b) \in \overline{R(a, b, 0)}$,

$$\mathbf{Exp}_{\{1,2,3\}}(H) \geq \frac{2}{a^2 + ab + b^2} > \frac{3}{(a+b)^2}.$$

9.4. **More symmetric polynomials:** Let G be a group of permutations on m letters and let $f = \sum_{\sigma \in G} a_{\sigma(1)}^{i_1} \cdots a_{\sigma(m)}^{i_m}$ with $i_1 \geq \cdots \geq i_m = 0$. We saw earlier that $\mathbf{Exp}(H) \geq 1/(\sum_{j=1}^n i_j^2)$. We can instead try $\frac{1}{\sqrt{2i_1^2 - 2i_1 i_2 + i_2^2}}(i_1 - i_2, i_1, 0, \ldots, 0) \in \overline{R(i_1, \ldots, i_n)}$ and so

$$\mathbf{Exp}(H) \geq \frac{2i_1^2 - 2i_1 i_2 + i_2^2}{i_1^4} \geq \frac{1}{i_1^2}.$$

10. Cases where $G(H)$ and $G(C)$ are equal for curves

10.1. **Hyperelliptic curves with index 2.**

Lemma 10.1. *Suppose that the binary form $f(x, y) \in \mathbb{Z}[x, y]$ of degree $2m$ is irreducible mod p, and that prime $p \| d$. Then $C : dz^2 = f(x, y)$ has no points in fields of odd degree.*

Proof. Suppose u and v are algebraic integers, and w is an algebraic number such that $f(u, v) = dw^2$ where $K = \mathbb{Q}(u/v, w/v^m)$ is a field of odd degree.[4] We are able to assume that u and v are algebraic integers by multiplying through by any common denominator. Now let R be an ideal in the same ideal class as $Q = (u, v)$ and which is coprime with p. Select algebraic integers q and r so that $Q\overline{Q} = (q)$ and $R\overline{Q} = (r)$. We now replace u and v

[4]As the triple $u : v : w$ comes from the weighted projective space $\mathcal{A}(1, m)$. Thus we begin with a point $f(U, 1) = dW^2$ and then select v from the ring of algebraic integers of $K = \mathbb{Q}(U, W)$ for which $u := Uv$ is also an algebraic integer. Then $w = Wv^m$.

by ur/q and vr/q which are algebraic integers since $(r/q) = R/Q$ and $Q|u$ and v, so we may assume that $(u, v, p) = 1$.

Let P be any prime ideal dividing p. We now show that $f(u, v) \not\equiv 0 \pmod P$. Suppose otherwise that $f(u, v) \equiv 0 \pmod P$. Since $(u, v, p) = 1$, P does not divide at least one of u and v, say v. Then there is a linear factor of $f(x, y)$ in the reduction K/P and so has relative degree $2m$ dividing $[K : \mathbb{Q}]$, a contradiction.

Therefore P does not divide dw^2, and so if P^r divides the denominator of w exactly then P^{2r} divides (p) exactly; in other words e_P is even, But then $[K : \mathbb{Q}] = \sum_{P|(p)} e_P$ is even, again a contradiction. □

Corollary 10.2. *Suppose that the binary form $f(x, y) \in \mathbb{Z}[x, y]$ of degree $2m$ is irreducible. Then $C : dz^2 = f(x, y)$ has no points in any fields of odd degree for almost all squarefree d.*

Proof. Let $\mathcal{P}(f)$ be the set of primes p for which $f(x, y)$ is irreducible mod p. Then $\mathcal{P}(f)$ contains a positive proportion (say δ) of all primes by the Cebotarev density theorem. Let $\mathcal{D}(f)$ be the set of integers that are not divisible by any prime from $\mathcal{P}(f)$; by sieve theory we know that $\#\{d \le x : d \in \mathcal{D}(f)\} \ll x/(\log x)^\delta$.

Now if d is squarefree and $C : dz^2 = f(x, y)$ has a point of odd degree then $p \nmid d$ for all $p \in \mathcal{P}(f)$ by Lemma 10.1. Thus the number of such $d \le x$ is $\ll x/(\log x)^\delta$ and the result follows as there are $\gg x$ squarefree $d \le x$. □

In our next result we fix d and vary f, rather than the other way around.

Let $\mathrm{Poly}(B, 2m)$ be the set of binary forms $f(x, y) \in \mathbb{Z}[x, y]$ of degree $2m$ with $\|f\| \le B$.

Corollary 10.3. *Let d be an integer $\le B$ and let $S_d := \{\text{Primes } p : p\|d\}$. The probability that $C : dz^2 = f(x, y)$ has at least one point in any field of odd degree, for a binary form $f(x, y)$ randomly chosen from Poly$(B, 2m)$, is $\ll_m (1 - \frac{1}{2m})^{|S_d|}$.*

Proof. Let $q := \prod_{p \in S_d} p \le d \le B$. If $C : dz^2 = f(x, y)$ has a point in a field of odd degree then $f(x, y)$ must be reducible mod p for every prime p dividing q, by Lemma 10.1. We dissect the domain for the coefficients up into boxes with side length q: There are $(2B/q + O(1))^{2m+1} \ll_m (B/q)^{2m+1}$, such boxes.

There are $\frac{1}{\ell} \sum_{d|\ell} \mu(d) p^{\ell/d} = \frac{p^{2m}}{2m}(1 + O(p^{-m}))$ irreducible polynomials in $\mathbb{F}_p[t]$ of degree $\ell (= 2m)$ which split completely in $\mathbb{F}_{p^\ell}$, but remain irreducible in $\mathbb{F}_{p^k}[t]$ for $1 \le k \le \ell - 1$. Therefore the number of polynomials mod q that are reducible mod p for every prime p dividing q is

$$q^{2m+1} \prod_{p|q} \left(1 - \frac{1}{2m}(1 + O(p^{-m})\right) \asymp q^{2m+1} \left(1 - \frac{1}{2m}\right)^{|S_d|}.$$

Multiplying together the above yields the claimed result. □

Proof of Theorem 1.7(a). Let the degree $d = 2m$. Let $f(\cdot)$ be the multiplicative function with each $f(p^k) = 1 - \frac{1}{2m}$. By Corollary 10.3 the probability that a curve $dy^2 = a_{2m}x^{2m} + \cdots + a_0$ has a point of odd order, where $0 < |d|, |a_0|, \ldots, |a_{2m}| < B$ is

$$\ll_m \frac{1}{B} \sum_{d \le B} f(d) \ll \exp\left(\sum_{p \le B} \frac{1 - f(p)}{p}\right) \ll \frac{1}{(\log B)^{1/2m}}$$

using Halasz's theorem to bound the mean value of a positive valued real multiplicative function. This $\to 0$ as $B \to \infty$. □

Remark 10.4. To prove the analogy of Theorem 1.7 for sets I^+ with $I^+ = \{(0,2,d-2)\} \cup \{(i,0,d-i) : i \in J\}$ where $0, d \in J \subset \{0,1,\dots,d\}$. we need to count irreducible degree d polynomials mod p, where the coefficients of $t^j, j \notin J$ equal zero. This can be done sufficiently well provided $\#J \geq \frac{3d}{4}$ using [7, Theorem 1.1].

10.2. **Curves which have no points of order divisible by n.** Given $\alpha \in K$, a given number field, and P a prime ideal of K, define $v_P(\alpha)$ to be the exact power of P that divides (α), positive or negative, so that the fractional ideal $(\alpha)/P^{v_P(\alpha)}$ is not divisible by P in either the numerator or denominator

Lemma 10.5. *Suppose $\alpha, \beta \in K$ a given number field, and that P is a prime ideal of K. Then there exist $\alpha_P, \beta_P, \gamma_P \in K$ with $\alpha : \beta : 1 = \alpha_P : \beta_P : \gamma_P$, such that $\min\{v_P(\alpha_P), v_P(\beta_P)\} = 0$ and $v_P(\gamma_P) < 0$ if and only if $\min\{v_P(\alpha), v_P(\beta)\} > 0$.*

Proof. Let $v_P(\alpha) = u$ and $v_P(\beta) = v$ so we can write the ideals

$$(\alpha) = P^u A \text{ and } (\beta) = P^v B$$

with $u, v \in \mathbb{Z}$ where $v_P(A) = v_P(B) = 0$.

Let R be an integral ideal in the same ideal class as P but with $(R, P) = 1$. Let $w := \min\{u, v\}$, $R\overline{R} = (r)$ and $P\overline{R} = (q)$ and then let

$$\alpha_P = \alpha(r/q)^w, \ \beta_P = \beta(r/q)^w, \text{ and } \gamma_P = (r/q)^w$$

Then $v_P(\alpha_P) = u - w, v_P(\beta_P) = v - w, v_P(\gamma_P) = -w$ and all the claims follow. □

Proposition 10.6. *Fix integer $m \geq 2$ and prime p. Suppose that $f(t) \in \mathbb{Z}[t]$ has degree m, is irreducible and remains so when reduced mod p. Let $g(x,y) \in \mathbb{Z}[x,y]$ be a polynomial of degree $\leq m-1$ with $p \nmid g(0,0)$. Finally let*

$$F(x,y) := y^m f(x/y) - pg(x,y) \in \mathbb{Z}[x,y].$$

If $F(x,y) = 0$ has a K-rational point then m divides $[K : \mathbb{Q}]$. Moreover

$$D(C_F)^{\inf} = m\mathbb{Z}_{\geq 1}.$$

Proof. Let P be a prime ideal of K dividing (p) and suppose $P^{e_P} \| (p)$ (that is $v_P(p) = e_P$). Write $f(x,y) = y^m f(x/y) = \sum_{i=0}^m f_i x^i y^{m-i}$ where $f_0, f_m \not\equiv 0 \pmod p$ since f is irreducible of degree m when reduced mod p. Write $g(x,y) = \sum_{i=0}^{m-1} g_i(x,y)$ where g_i is homogenous of degree i and then let $G(x,y,z) := \sum_{i=0}^{m-1} g_i(x,y) z^{m-i}$ which is homogenous of degree m.

Suppose that $F(\alpha, \beta) = 0$ where $\alpha, \beta \in K$, so that

$$f(\alpha, \beta) = p\, g(\alpha, \beta).$$

Applying Lemma 10.5 there exist $\alpha_P, \beta_P, \gamma_P \in K$ with $\min\{v_P(\alpha_P), v_P(\beta_P)\} = 0$ such that

$$f(\alpha_P, \beta_P) = p\, G(\alpha_P, \beta_P, \gamma_P).$$

Since α_P and β_P are P-integral, so $f(\alpha_P, \beta_P)$ is also P-integral, that is $v_P(f(\alpha_P, \beta_P)) \geq 0$.

Now suppose that $v_P(f(\alpha_P, \beta_P)) \geq 1$, so that $f(\alpha_P, \beta_P) \equiv 0 \pmod P$. We claim that $v_P(\beta_P) = 0$ for if not then $v_P(\alpha_P) = 0$ and $f(\alpha_P, \beta_P) \equiv f_m(\alpha_P)^m \not\equiv 0 \pmod P$, a contradiction. Now $\alpha/\beta = \alpha_P/\beta_P$ and so $f(\alpha/\beta) = f(\alpha_P/\beta_P) = \beta_P^{-m} f(\alpha_P, \beta_P) \equiv 0 \pmod P$. Embedding this into $\overline{\mathbb{F}_p}$ we deduce that there exists a root ρ of $f(t)$ in $\mathbb{F}_{p^m}$ such that $\rho = \alpha/\beta \in \mathbb{F}_p(\alpha/\beta)$, and so $\mathbb{F}_p(\alpha/\beta) = \mathbb{F}_{p^n}$ where m divides n. However then n must divide $[\mathbb{Q}(\alpha/\beta) : \mathbb{Q}]$ which divides $[K : \mathbb{Q}]$, and so m divides $[K : \mathbb{Q}]$.

Now suppose that $v_P(f(\alpha_P,\beta_P))=0$. Then $v_P(\gamma_P)<0$ else $v_P(G(\alpha_P,\beta_P,\gamma_P))\ge 0$ and so $v_P(f(\alpha_P,\beta_P))\ge e_P>0$, a contradiction. Lemma 10.5 implies that

$$u:=\min\{v_P(\alpha),v_P(\beta)\}>0$$

so that P^{iu} divides $g_i(\alpha,\beta)$ and so $g(\alpha,\beta)\equiv g_0(\alpha,\beta)=g(0,0)\not\equiv 0 \pmod P$, and therefore $v_P(f(\alpha,\beta))=e_P+v_P(g(\alpha,\beta))=e_P$. Now $v_P(\alpha_P)=v_P(\alpha)-u$ and $v_P(\beta_P)=v_P(\beta)-u$ and so $v_P(f(\alpha_P,\beta_P))=e_P-mu=0$, and so m divides e_P, the ramification index of P in K. Therefore m divides $\sum_{P|p}e_P=[K:\mathbb{Q}]$.

Therefore we have proved that m divides $[K:\mathbb{Q}]$ and so $D(C_F)^{\inf}\subseteq m\mathbb{Z}_{\ge 1}$.

For the second part of the argument let $x=x(t),y=y(t)$, polynomials of degree k. Typically $F(x(t),y(t))$ will be an irreducible polynomial of degree mk in which case if $F(x(\alpha),y(\alpha))=0$, then $(x(\alpha),y(\alpha))\in C$ with $[K:\mathbb{Q}]=mk$ for most pairs $x(t),y(t)$ by the Hilbert irreducibility theorem where $K=\mathbb{Q}(x(\alpha),y(\alpha))$. Therefore $mk\in D(C_F)^{\inf}$, that is, $m\mathbb{Z}_{\ge 1}\subseteq D(C_F)^{\inf}$. The result follows. □

Proposition 10.6 for $m\ge 2$ and $p=2$, yields that if $F(x,y):=f(x,y)-2g(x,y)$ where f is homogenous of degree m and irreducible mod 2, while $g(x,y)$ is a polynomial of degree $\le m-1$ with $g(0,0)$ odd. Then $D(C_F)^{\inf}=m\mathbb{Z}_{\ge 1}$.

Proof of Theorem 1.8. We will determine what proportion of $F(x,y)=\sum_{i+j\le m}f_{i,j}x^iy^j\in\mathbb{Z}[x,y]$ with $f_{0,0},f_{0,m},f_{m,0}\ne 0$ (so that $H_f=\{(0,0,m),(0,m,0),(m,0,0)\}$) satisfy the hypotheses of Proposition 10.6 for some $m\ge 2$ and $p=2$:

We assume each $|f_{i,j}|\le T$ for T large, and then take $f(x,y)=\sum_{i+j=m}f_{i,j}x^iy^j$ with $g(x,y)=\sum_{i+j<m}f_{i,j}x^iy^j$. The hypothesis for g requires $f_{i,j}$ even for all $0<i+j<m$ and $f_{0,0}\equiv 2 \pmod 4$; these happen for probability $(1/2)^{m(m+1)/2-1}\cdot 1/4=1/2^{(m^2+m+2)/2}$. The hypothesis for $f(x,y)$ requires $f(x,1)$ to be an irreducible polynomial mod 2 of degree m, which we saw happens with probability $\frac{1}{m}(1+O(2^{-m/2}))$. Therefore in total $\ll 1m2^{(m^2+m+2)/2}$ of polynomials F satisfy the hypotheses of Proposition 10.6 (with $p=2$) and so have $D(C_F)^{\inf}=m\mathbb{Z}_{\ge 1}$.

We have proved the result for $I_F=\mathcal{M}_{3,d}$. However the proof changes little if we remove (i,j,k) from I_F whenever $1\le k\le m-1$, which gives the complete result. □

11. Odd degree points on low degree hypersurfaces and Springer's Theorem

Theorem 11.1 (Springer)**.** *Let $F(x_1,\dots,x_m)$ be a homogeneous quadratic, then $F(x_1,\dots,x_m)$ has a rational point if and only if it has a point in a number field of degree d for any odd degree d.*

Proof. First we show that if F has an odd degree point then it has a rational point. Let P be a point of lowest odd degree on F, and suppose $d>1$. Write the field as $\mathbb{Q}(\alpha)$ where α has minimal polynomial $g(t)$ of degree d. Now suppose $P=(x_1(\alpha),\dots,x_m(\alpha))$, where we can assume $D=\max_j\deg x_j(t)\le d-1$ so that $F(x_1(t),\dots,x_m(t))$ has degree $2D$. Now $g(t)$ divides $F(x_1(t),\dots,x_m(t))$ and $h(t)=F(x_1(t),\dots,x_m(t))/g(t)$ has degree $2D-d$ which is odd and $<d$, so $h(t)$ must have an irreducible factor of odd degree $<d$ which contradicts the minimality of d, so the only possible minimal odd degree is $d=1$ and thus F has a rational point.

Now, suppose $F(x_1,\dots,x_m)$ has a rational point $Q=(q_1,\dots,q_m)$. For polynomials $x_1(t),\dots,x_m(t)$ of degree d, the polynomial $G(t)=F(tx_1(t)+q_1,\dots,tx_m(t)+q_m)/t$, generically gives degree $2d+1$ points for each $d\ge 0$. □

Proposition 11.2 (Coray)**.** *A cubic form $F(x_1, \dots, x_m)$ has a rational point if and only if it has a degree 2 point.*

Proof. First we show that if F has a point of degree 2 then it has a rational point. Let P be a point of even degree. Write the field as $\mathbb{Q}(\alpha)$ where α has minimal polynomial $g(t)$ of degree 2. Now suppose $P = (x_1(\alpha), \dots, x_m(\alpha))$, where $D = \max \deg x_j(t) = 1$ (to see this note that $D > 0$ else P is a rational point, and also by construction $D \leq \deg g - 1 = 1$). Then $F(x_1(t), \dots, x_m(t))$ has degree 3 and is divisible by $g(t)$, so that $h(t) = F(x_1(t), \dots, x_m(t))/g(t)$ is a linear polynomial and, solving for t, thus F has a rational point.

Now, suppose $F(x_1, \dots, x_m)$ has a rational point $Q = (q_1, \dots, q_m)$. The polynomial $F(t) = F(a_1t + q_1, \dots, a_mt + q_m)/t$ has degree 2 and is generically irreducible, so that F has a point of degree 2. □

Therefore suppose that a cubic form F has a degree 2 point. By Proposition 11.2 it has a rational point. If that rational point is non-singular then $D(C_f)^{\inf} \supset \mathbb{Z}_{\geq 2}$ by Theorem 1.3, in particular it will have infinitely many non-singular points of degree 2.

11.1. **Odd degree points on hyperelliptic curves.** Bhargava, Gross, and Wang [1, Corollary 8], showed that for any fixed odd integer m the proportion of hyperelliptic curves of genus g that contain points of degree m, tends to 0 as $g \to \infty$. So if a curve does have odd degree points, what degrees are they?

Conjecture 11.3 (Bhargava)**.** 100% *of the locally soluble hyperelliptic curves which have odd degree points will have an odd degree point of lowest degree* exactly *g or $g+1$ (whichever is odd).*

In this section we will prove Proposition 1.11. Part (a) establishes "half" of Bhargava's conjecture. It remains to show that 0% of such curves have points of odd degree $< g$.

Without loss of generality we may restrict our attention to $C : y^2 = f(x)$ where the leading coefficient of $f(x)$ is not a square, $f(x)$ is squarefree, and f has even degree $2g + 2$ (so that C has genus g: To see that recall (from the introduction) that if $f(x)$ has odd degree d then there is a bi-rational transformation between the algebraic points of $y^2 = f(x)$ and those of $Y^2 = F(X)$ where $F(t) = t^{d+1}f(1/t)$ has (even) degree $d + 1$ We could have begun by translating $x \to x + m$ to ensure that $f(0)$ is not a square, so that the leading coefficient of $F(x)$ is not a square.

It is evident that every positive even integer $2k$ is in $D(C)^{\infty}$, by substituting in a generic polynomial of degree k for y and an arbitrary constant x, in which case almost all of these substitutions will lead to an algebraic point of degree $2k$.

Proof of Proposition 1.11. As explained above we write C as $y^2 = f(x)$ where $f(x)$ has degree $2g + 2$, and the leading coefficient of f is not a square.

Suppose that P is rational. By a translation of x we may suppose that $P = (0, y_0)$, so that $f(x) = y_0^2 + c_1x + \cdots + c_dx^d$ for some $c_j \in \mathbb{Q}$ where $d = 2g + 2$, and we assume that $y_0 \neq 0$. We select $y = y_0 + y_1t + \cdots + y_mt^m + ut^{m+1}$ for some $0 \leq m \leq g$, where the $y_1, y_2, \dots, y_m$ are selected so that the coefficient of t^j in y^2 equals c_j; note that this is possible since y_j does not appear in the coefficients of t^i with $i < j$, and only in the monomial $2y_0y_j$ in the coefficient for t^j. Thus $2y_0y_1 = c_1, 2y_2y_0 = c_2 - y_1^2$, etc. Note that u is a free variable.

By construction $f(t)-y^2$ is divisible by t^{m+1}, and $(f(t)-y^2)/t^{m+1}$ has degree $2g+1-m$, which will be irreducible for most choices of u, and so $2g+1-m \in D(C)^\infty$ for $0 \le m \le g$, and therefore $[g+1, 2g+1] \cap \mathbb{Z}$ in $D(C)^\infty$.

Finally we can take $y = y_0 + tw(t)$ with $\deg w = \ell \ge g$ so that $(y^2 - f(t))/t$ has degree $2\ell+1$ and so all odd integers $\ge 2g+1$ belong to $D(C)^\infty$.

Otherwise, suppose that $P = (\alpha, \beta)$ be a point of odd degree $m > 1$, so that β is a root of $y^2 - f(\alpha)$. Then $\beta \in \mathbb{Q}(\alpha)$ else $2|[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\alpha)]$ which divides $m = [\mathbb{Q}(\alpha,\beta) : \mathbb{Q}]$, a contradiction. Therefore we can write $\beta = h(\alpha)$ where $h(x) \in \mathbb{Q}[x]$ has degree $\le m-1$. Let $G(x)$ be the minimum polynomial for α which has degree m so that $h(\alpha)^2 - f(\alpha) = \beta^2 - f(\alpha) = 0$ and therefore $G(x)$ divides $h(x)^2 - f(x)$.

We write $h(x)^2 - f(x) = G(x)R(x)$ where $R(x)$ is some polynomial in $\mathbb{Q}[x]$. The polynomial $h(x)^2 - f(x)$ has even degree because both $h(x)^2$ and $f(x)$ have even degree, and there cannot be cancellation of the leading terms as the leading coefficient of f is not a square. Therefore $G(x)R(x)$ has even degree and $G(x)$ has odd degree, so $R(x)$ has odd degree as well. Now $R(x)$ has an irreducible factor $Q(x)$ of odd degree, so that $h(\gamma)^2 = f(\gamma)$ for any γ for which $Q(\gamma) = 0$, yielding a point of odd degree. Now $\deg R \ge \deg Q \ge m$ by minimality, so that

$$\begin{aligned} 2m &\le m + \deg R = \deg(h(x)^2 - f(x)) \\ &= \max\{2\deg h(x), \deg f(x)\} \le 2\max\{m-1, g+1\} \end{aligned}$$

and so $m \le g+1$.

Now write $H(x) = h(x) + a(x)G(x)$ for an arbitrary polynomial $a(x)$ of degree $r \ge g+1-m$. Then $H(\alpha) = \beta$ so that $H(\alpha)^2 - f(\alpha) = \beta^2 - f(\alpha) = 0$ and therefore we can write $H(x)^2 - f(x) = G(x)R(x)$ for some $R(x) \in \mathbb{Q}[x]$. Again there is no cancelation as the leading coefficient of f is not a square, so $G(x)R(x)$ has odd degree. For a typical $a(x)$, $R(x)$ is irreducible with

$$\begin{aligned} \deg R &= \deg(H(x)^2 - f(x)) - m \\ &= \max\{2\deg H(x), \deg f(x)\} - m \\ &= \max\{2r+m, 2g+2-m\} = 2r+m. \end{aligned}$$

As we range over the possible values of r we deduce that $D(C)^\infty \supset \mathbb{Z}_{\ge 2g+2-m}$.

Finally, if $1 \notin D(C)$ then $D(C)^\infty$ contains all the integers $\ge \max_{3\le m\le g+1} 2g+2-m = 2g-1$. Combining this with our first result we deduce that $\mathcal{E}(C)$ is a subset of the odd integers in $\le \max\{1, 2g-3\}$ as claimed. □

The simplest such question that we cannot answer is whether there a curve $C : y^2 = f(x)$ with f of degree 8 (genus 3) which has no points in fields of degree 3?

References

[1] Manjul Bhargava, Benedict H. Gross and Xiaoheng Wang, *A positive proportion of locally soluble hyperelliptic curves over $\mathbb{Q}$ have no point over any odd degree extension*, J. Amer. Math. Soc. **30** (2017), 451–493

[2] Manjul Bhargava, *Galois groups of random integer polynomials and van der Waerden's conjecture*, Ann. Math. (to appear)

[3] Lea Beneish and Christopher Keyes, *Fields generated by points on superelliptic curves* Journal of Number Theory **278** (2026), 380-421.

[4] Pete L. Clark, Marko Milosevic and Paul Pollack, *Typically bounding torsion* J. Number Theory **192** (2018), 150–167.

[5] S.D. Cohen, *The distribution of Galois groups and Hilbert's irreducibility theorem*, Proc. London Math. Soc.**43** (1981), 227–250.
[6] D. Coray. *Algebraic points on cubic hypersurfaces*, Acta Arithmetica **30**, Issue 3, (1976) 267-296
[7] Junsoo Ha, *Irreducible polynomials with several prescribed coefficients* Finite Fields Appl. **40** (2016), 10–25.
[8] Henryk Iwaniec, *On the problem of Jacobsthal*, Demonstratio Math. **11** (1978), 225–231.
[9] Christopher Keyes, *Growth of points on hyperelliptic curves over number fields*, Journal de théorie des nombres de Bordeaux **34** (2022) 271–294.
[10] Barry Mazur, Karl Rubin and Michael Larsen. *Diophantine stability*, Amer J Math **140** (2018), 571–616.
[11] Robert J. Lemke Oliver and Frank Thorne, *Upper bounds on polynomials with small Galois group*, Mathematika **66** (2020), 1054–1059.
[12] Robert J. Lemke Oliver and Frank Thorne, *Rank growth of elliptic curves in non-Abelian extensions* International Mathematics Research Notices, **24** (2021), 18411–18441.
[13] Robert J. Lemke Oliver and Frank Thorne, *Upper bounds on number fields of given degree and bounded discriminant*, Duke Math. J. **171** (2022), 3077–3087.
[14] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem* Aspects of Mathematics, 3rd Edition, (1997). x+218.
[15] Tonny Albert Springer, *Sur les formes quadratiques d'indice zéro* R. Acad. Sci. Paris 234 (1952), 1517–1519.