Squarefree values of polynomial discriminants

Manjul Bhargava
Princeton University

(joint work with Arul Shankar and Xiaoheng Wang)

Recent developments in Analytic Number Theory
MSRI

May 2, 2017

Squarefree values of a polynomial

The general problem of how often a multivariable integer polynomial takes squarefree values is in general unknown, even under ABC.

However, for certain naturally arising integer polynomials whose squarefree values are needed, one can hope to exploit the shape or any known extra structure of the polynomials to try to determine the density of squarefree values.

Squarefree discriminants

One important example that arises in applications is the discriminant Δ_n of a monic polynomial of degree n, which is itself a polynomial in the coefficients:

$$\begin{aligned} \Delta_2(x^2 + a_1x + a_2) &= a_1^2 - 4a_2, \\ \Delta_3(x^3 + a_1x^2 + a_2x + a_3) &= a_1^2a_2^2 - 27a_3^2 - 4a_2^3 - 4a_1^3a_3 + 18a_1a_2a_3, \\ &\vdots \end{aligned}$$

In general, Δ_n is a polynomial in n variables of weighted homogeneous degree $n(n-1)$, where the i-th coefficient a_i has weight i.

Question. When integer monic polynomials $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ of degree n are ordered by height $H(f) := \max\{|a_i|^{1/i}\}$, what is the density of $f(x)$ such that $\Delta_n(f)$ is squarefree?

Why do we care about polynomials with squarefree discriminant?

In algebraic number theory, one often considers number fields that are defined as $K_f := \mathbb{Q}[x]/(f(x))$ for some irreducible integer polynomial $f(x)$.

One is also then interested in constructing the ring of integers in K_f.

If the discriminant of $f(x)$ is squarefree, then the ring of integers in K_f is given simply by $R_f := \mathbb{Z}[x]/(f(x))$. Moreover, K_f is then monogenic, and has squarefree discriminant.

A Related Question. When integer monic polynomials $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ of degree n are ordered by height $H(f) := \max\{|a_i|^{1/i}\}$, what is the density of $f(x)$ such that $R_f := \mathbb{Z}[x]/(f(x))$ is the ring of integers in $K_f := \mathbb{Q}[x]/(f(x))$?

Conjectured Answer (Hendrik Lenstra). The density is $6/\pi^2$, independent of n!

Statement of main theorems

Brakenhoff later gave explicit conjectured densities for squarefree discriminants:

$$\text{Let } \lambda_n(p) = \begin{cases} 1 & \text{if } n = 1, \\ 1 - \frac{1}{p^2} & \text{if } n = 2, \\ 1 - \frac{2}{p^2} + \frac{1}{p^3} & \text{if } n = 3, \\ 1 - \frac{1}{p} + \frac{(p-1)^2(1-(-p)^{2-n})}{p^2(p+1)} & \text{if } n \geq 4 \end{cases}$$

for $p \neq 2$; also, let $\lambda_1(2) = 1$ and $\lambda_n(2) = 1/2$ for $n \geq 2$.

Let $\lambda_n := \prod_p \lambda_n(p)$.

Theorem 1. *Let $n \geq 1$ be an integer. Then when monic integer polynomials $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ of degree n are ordered by $H(f) := \max\{|a_1|, |a_2|^{1/2}, \ldots, |a_n|^{1/n}\}$, the density having squarefree discriminant $\Delta_n(f)$ exists and is equal to $\lambda_n > 0$.*

Note: $\lambda = \lim_{n\to\infty} \lambda_n \approx 35.8232\%$.

Statement of main theorems II

How often does $R_f := \mathbb{Z}[x]/(f(x))$ give the ring of integers in $K_f := \mathbb{Q}[x]/(f(x))$?

Our second main theorem states that this is in fact is the case for *most* monic integer polynomials $f(x)$:

Theorem 2. *The density of irreducible monic integer polynomials $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ of degree n, when ordered by $H(f) := \max\{|a_1|, |a_2|^{1/2}, \ldots, |a_n|^{1/n}\}$, such that $\mathbb{Z}[x]/(f(x))$ is the ring of integers in its fraction field is $\prod_p(1 - 1/p^2) = \zeta(2)^{-1}$.*

Note that $\zeta(2)^{-1} \approx 60.7927\%$.

Statement of main theorems III

Note that if $f(x)$ is an integral irreducible monic polynomial with squarefree discriminant, then $K_f := \mathbb{Q}[x]/(f(x))$ is a number field that is monogenic and has squarefree discriminant (and thus Galois group S_n).

Moreover, if $H(f) < X$, then $|\mathrm{Disc}(K_f)| \ll X^{n(n-1)}$.

Corollary 3. *Let $n > 1$. The number of isomorphism classes of number fields of degree n and absolute discriminant less than X that are monogenic and have associated Galois group S_n is $\gg X^{1/2+1/n}$.*

This gives the best-known lower bounds for the number of degree-n number fields of bounded discriminant. Moreover, we conjecture that this gives the optimal lower bound for *monogenic* number fields of degree n of bounded discriminant.

All number fields constructed here also have squarefree discriminant.

How can one handle squarefree values of multivariable polynomials of this discriminant type?

Let $g(x_1, \ldots, x_n)$ be a polynomial with integer coefficients.

To count squarefree values taken by g, we need to sieve away those points $a \in \mathbb{Z}^n$ where g is a multiple of p^2 for some large prime p.

If $g(a) \equiv 0 \pmod{p^2}$ for some $a \in \mathbb{Z}^n$, then this can happen in two distinct ways:

- We have $g(a') \equiv 0 \pmod{p^2}$ $\forall a' \equiv a \pmod{p}$, in which case we say that $g(a)$ is *strongly* a multiple of p^2.
- Otherwise, we say $g(a)$ is *weakly* a multiple of p^2.

In other words, in the first case, $g(a)$ is a multiple of p^2 for "mod p reasons" while, in the second case, $g(a)$ is a multiple of p^2 for "mod p^2 reasons". (Example: both cases occur for $f(x, y) = xy$.)

It is natural to try to estimate how often each happens separately!

Strong multiples of p^2 can be handled by algebro-geometric techniques

To estimate strong multiples of p^2, we use the following theorem:

Theorem (based on work of Ekedahl). *Let V be any subvariety of $\mathbb{A}^n_{\mathbb{Z}}$ of codimension $k \geq 1$. Then*

$$\#\{a \in \mathbb{Z}^n : ||a|| < X \text{ and } a \pmod p \in V(\mathbb{F}_p) \text{ for some } p > M\}$$
$$= O\left(\frac{X^n}{M^{k-1}} + X^{n-k+1}\right)$$

where the implied constant depends only on V.

Sketch of Proof for $k = 2$:

WLOG $V = \{g(x_1, \ldots, x_{n-1}) = h(x_1, \ldots, x_n) = 0\}$.

Fix $x_1, \ldots, x_{n-1}$ with $|x_i| < X$. Then $g(x_1, \ldots, x_{n-1})$ has only boundedly many prime factors $p > M$; for each such prime p, there are only boundedly many $x_n \pmod p$ such that $h(x_1, \ldots, x_n) \equiv 0 \pmod p$. So the total number of possible $x_1, \ldots, x_n$ is $O(X^{n-1}(X/M + 1)) = O(X^n/M + X^{n-1})$. $\square$

Strong multiples of p^2 can be handled by algebro-geometric techniques

To handle strong multiples, we observe that if $g(a_1, \ldots, a_n)$ is a multiple of p^2 for mod p reasons, then $g(a_1, \ldots, a_n)$ and $g_n(a_1, \ldots, a_n)$ will both be multiples of p: i.e., $(a_1, \ldots, a_n)$ will lie on a fixed codimension 2 variety modulo p.

So we can use the Ekedahl-type estimate from the previous page.

This argument holds for any multivariable integer polynomial!

It thus remains to estimate the number of weak multiples of p^2, i.e., integer values of f that are multiples of p^2 genuinely for mod p^2 reasons.

Main idea: Transform weak multiples into strong multiples!

The case of discriminant polynomials

The idea is to embed the space of monic polynomials into a bigger space, where there are more symmetries, and where we can embed such polynomials so that the mod p^2 reasons are changed to mod p reasons!

To do this, we must first understand how a polynomial can have discriminant a multiple of p^2 — and when it is for mod p reasons and when for mod p^2 reasons.

Lemma 4. *A monic integral polynomial has discriminant a multiple of p^2 for mod p reasons if and only if modulo p it has a root of multiplicity at least 3 or two roots of multiplicity at least 2.*

Such multiples of p^2 for the discriminant are thus handled by our Ekedahl sieve method.

The case of discriminant polynomials (cont'd)

When is the discriminant a multiple of p^2 for mod p^2 reasons?

Lemma 5. *A monic integral polynomial $f(x)$ has discriminant a multiple of p^2 for $\mathrm{mod}\ p^2$ reasons if and only if there exists $k \in \mathbb{Z}$ such that $f(x+k)$ has constant coefficient divisible by p^2 and linear coefficient divisible by p.*

How can we lift such polynomials to a bigger space, so that the mod p^2 condition changes to a mod p condition?

We show that there exist $n \times n$ integer symmetric matrices A and B such that $\det(Ax - B) = f(x)$, and such that the polynomial $\Delta_n(\det(Ax - B))$ in the nonzero entries of such pairs (A, B) is a multiple of p^2 for mod p reasons.

The case of discriminant polynomials (cont'd)

If $n = 5$, we take A and B given by:

$$A = \begin{pmatrix} & & & & 1 \\ & & & 1 & \\ & & 1 & & \\ & 1 & & & \\ 1 & & & & \end{pmatrix}, \; B = \begin{pmatrix} & & 0 & p & 0 \\ & & 1 & 0 & 0 \\ 0 & 1 & -c_1 & -c_2/2 & 0 \\ p & 0 & -c_2/2 & -c_3 & -c_4/2 \\ 0 & 0 & 0 & -c_4/2 & -c_5 \end{pmatrix}.$$

Then

$$\det(Ax - B) = f(x) = x^5 + c_1x^4 + c_2x^3 + c_3x^2 + pc_4x + p^2c_5.$$

We may view $\mathrm{Disc}(\det(Ax - B)) = \Delta_n(f)$ as a polynomial in the 12 variables of B. Then Disc is a multiple of p^2 in these 12 coordinates for mod p reasons, even though $\Delta_n(f)$ as a polynomial in $c_1, \ldots, c_5$ was a multiple of p^2 for mod p^2 reasons!

The case of discriminant polynomials (cont'd)

$$A = \begin{pmatrix} & & & & 1 \\ & & & 1 & \\ & & 1 & & \\ & 1 & & & \\ 1 & & & & \end{pmatrix}, \quad B = \begin{pmatrix} & & 0 & p & 0 \\ & & 1 & 0 & 0 \\ 0 & 1 & -c_1 & -c_2/2 & 0 \\ p & 0 & -c_2/2 & -c_3 & -c_4/2 \\ 0 & 0 & 0 & -c_4/2 & -c_5 \end{pmatrix}.$$

$$\det(Ax - B) = f(x) = x^5 + c_1x^4 + c_2x^3 + c_3x^2 + pc_4x + p^2c_5. \quad (1)$$

Let G_0 be the subgroup of $\mathrm{SO}(A)$ that keeps the top 2×2 left corner of B zero. Then G_0 acts on pairs (A, B), preserving A and the shape of B. The action of G_0 also preserves Equation (1).

The invariants for the action of G_0 on this 12-dimensional representation V are the five coefficients of $\det(Ax - B)$, together with one additional invariant, which we call the *Q-invariant*. Evaluating Q on the above pair (A, B), we find that $Q(A, B) = p$!

The case of discriminant polynomials (cont'd)

Thus $Q(A,B)^2 \mid \mathrm{Disc}(A,B) := \Delta_n(\det(Ax-B))$. It now suffices to count orbits of $G_0(\mathbb{Z})$ on integer points of this 12-dimensional representation V satisfying $H(A,B) := H(\det(Ax-B)) < X$ and $\mathrm{Disc}(A,B) \neq 0$, such that the Q-invariant is larger than M.

Theorem. *The number of $G_0(\mathbb{Z})$-orbits on $V(\mathbb{Z})$ having nonzero discriminant, height less than X, and Q-invariant greater than M is $O_\epsilon(X^{n(n+1)/2+\epsilon}/M)$.*

Corollary. *The number of monic integer polynomials of degree 5 having nonzero discriminant, height less than X, and discriminant a multiple of p^2 for $\mathrm{mod}\ p^2$ reasons for some $p > M$ is $O_\epsilon(X^{n(n+1)/2+\epsilon}/M)$.*

The latter corollary is exactly the kind of estimate that is needed to complete the squarefree sieve on the discriminants of degree 5 monic polynomials. (But there was nothing special about the degree 5 . . .).
□

Summary

Theorem 1. *Let $n \geq 1$ be an integer. Then when monic integer polynomials $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ of degree n are ordered by $H(f) := \max\{|a_1|, |a_2|^{1/2}, \ldots, |a_n|^{1/n}\}$, the density having squarefree discriminant $\Delta_n(f)$ exists and is equal to $\lambda_n > 0$.*

Theorem 2. *The density of irreducible monic integer polynomials $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ of degree n, when ordered by $H(f) := \max\{|a_1|, |a_2|^{1/2}, \ldots, |a_n|^{1/n}\}$, such that $\mathbb{Z}[x]/(f(x))$ is the ring of integers in its fraction field is $\prod_p (1 - 1/p^2) = \zeta(2)^{-1}$.*