Density of power-free values of polynomials

Number Theory Down Under 8
Melbourne (online)

Kostadinka Lapkova
joint work with Stanley Yao Xiao

Graz University of Technology

7.10.2020

Introduction

We say that an integer n is *k-free* if there is no prime p, such that p^k divides n.
Let $F \in \mathbb{Z}[x_1, \ldots, x_n]$ be a polynomial of degree d.
Let us define the main quantity we want to estimate

$$N_{F,k}(B) := \#\{\mathbf{x} \in \mathbb{Z}^n : |x_i| \leq B, i = 1, \ldots, n; F(\mathbf{x}) \text{ is } k\text{-free}\}$$

- The goal is to find an *asymptotic formula* for $N_{F,k}(B)$ when there is no prime p such that $p^k \mid F(\mathbf{x})$ for every $\mathbf{x} \in \mathbb{Z}^n$;
- find out how k is related to d;
- the smaller k, and farther from d, the harder the problem.

Introduction, $n = 1$

The expected asymptotic formula for some $c_{F,k} > 0$

$$N_{F,k}(B) \sim c_{F,k} B$$

has been shown in the following chronological order:

- $k \geq d$ (Ricci, 1933);
- $k = d - 1$ (Erdős, 1953):

$$N_{F,d-1}(B) \gg \frac{B}{(\log \log B)^2};$$

- $k = d - 1$ (Hooley, 1967);
- $k \geq (3d + 1)/4$ (Browning, 2011).

Introduction, $n = 2$, F-homogeneous

The expected asymptotic formula

$$N_{F,k}(B) \sim c_{F,k} B^2$$

has been proven in the following cases:

- $k \geq (d-1)/2$ (Greaves, 1992);
- $k > 7d/16$ (Browning, 2011);
- $k > 7d/18$ (Xiao, 2017).

Since F is a form, one can use geometry of numbers methods.

Introduction, $n = 2$, F-inhomogeneous

A lower bound for certain k's

$$N_{F,k}(B) \gg c_{F,k} B^2$$

has been proven by:

- Hooley, 2009;
- Browning, 2011.

In another paper from 2009 Hooley proves an asymptotic formula for certain classes of inhomogeneous polynomials in 2 variables.

Introduction, $n \geq 1$

The most difficult case is $k = 2$ for square-free values of $F(\mathbf{x})$. Then

$$N_{F,2}(B) \sim c_{F,2} B^n$$

has been established by:

- Poonen, 2003, modulo the *abc*-conjecture, and differently defined density (not exactly $N_{F,2}$);
- Bhargava et al., 2014-2016, for special cases of invariant polynomials.

We will use, however, the methods of the previously mentioned works of Hooley and Browning.

Main results

We say that a polynomial F is *k-admissible* if for any prime p there exists an integer n-tuple $(m_1, \ldots, m_n)$ for which $p^k \nmid F(m_1, \ldots, m_n)$.

Theorem 1 (L-Xiao,2019)

Let $k \geq 2$ be a positive integer and let F be a k-admissible square-free polynomial $F(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_n]$ of degree d, for any $n \geq 1$. Then there exists $C_{F,k} > 0$, such that the asymptotic relation

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

holds whenever $k \geq (3d+1)/4$.

Here $C_{F,k} = \prod_p \left(1 - \rho_F(p^k)/p^{kn}\right)$, where

$$\rho_F(m) = \# \left\{ \mathbf{s} \in (\mathbb{Z}/m\mathbb{Z})^n : F(\mathbf{s}) \equiv 0 \pmod{m} \right\}.$$

Prime arguments

We can specialize our Theorem 1 to prime arguments. Let us have primes $p_i, i = 1, \ldots, n$ and $\mathbf{p} := (p_1, \ldots, p_n)$. Consider the quantity

$$\mathcal{N}_{F,k}(B) := \#\left\{\mathbf{p} \in \mathbb{Z}^n : |p_i| \leq B, i = 1, \ldots, n; F(\mathbf{p}) \text{ is } k\text{-free}\right\}$$

Theorem 2 (Prime inputs)

We have

$$\mathcal{N}_{F,k}(B) \sim C'_{F,k} \frac{B^n}{(\log B)^n}$$

for some $C'_{F,k} > 0$ *and* $k \geq (3d+1)/4$

Here $C'_{F,k} = \prod_p \left(1 - \rho_F^*(p^k)/\varphi(p^k)^n\right)$ with

$$\rho_F^*(m) = \#\left\{\mathbf{s} \in (\mathbb{Z}/m\mathbb{Z})^n, \gcd(s_i, s_j) = 1 \text{ for } i < j : F(\mathbf{s}) \equiv 0 \pmod{m}\right\}.$$

Prime arguments and Erdős

Conjecture [Erdős,1953]

For the irreducible polynomial $f(x) \in \mathbb{Z}[x]$ of degree d with no fixed $(d-1)$-th power prime divisor the set $f(\mathbb{P}) = \{f(p), p - \text{prime}\}$ contains infinitely many $(d-1)$-free values.

- (Heath-Brown,Browning,Helfgott,...)
- (Reuss, 2013) $d \geq 3$

We can extend this conjecture of Erdős for any number of variables.

Conjecture, $n \geq 1$

For any $n \geq 1$ and an irreducible polynomial $F(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_n]$ of degree d, which is $(d-1)$-admissible, the set $F(\mathbb{P}^n) = \{f(p_1, \ldots, p_n), p_i - \text{prime}\}$ contains infinitely many $(d-1)$-free values.

Main results (cont.)

An immediate corollary of Theorem 1 is the following.

Corollary 3 ($k = d - 1$)

For any square-free k-admissible polynomial $F(\mathbf{x}) \in \mathbb{Z}[\mathbf{x}]$ and $d \geq 5$ we have

$$N_{F,d-1} \sim C_{F,d-1} B^n.$$

And this is a corollary of Theorem 2, which solves the extension of the conjecture of Erdős for $d \geq 5$.

Corollary 4

For any square-free k-admissible polynomial $F(\mathbf{x}) \in \mathbb{Z}[\mathbf{x}]$ and $d \geq 5$ we have

$$\mathcal{N}_{F,d-1} \sim C'_{F,d-1} \frac{B^n}{(\log B)^n}.$$

Main results (cont.)

We can fill up the missing cases for the asymptotic of $N_{F,d-1}$ for $d = 3, 4$.

Theorem 5 (L-Xiao,2020)

For any square-free k-admissible polynomial $F(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_n]$ in $n \geq 1$ variables and $d \geq 3$ we have

$$N_{F,d-1} \sim C_{F,d-1} B^n.$$

However, our method still cannot prove the expected asymptotic formula for prime arguments:

$$\mathcal{N}_{F,d-1} \overset{?}{\sim} C'_{F,d-1} \frac{B^n}{(\log B)^n}, \quad \text{for } d = 3, 4, \text{ and any } n \geq 1.$$

Sketch of the proof; sieving

Let us recall

- Theorem 1 : $N_{F,k} \sim C_{F,k} B^n, \quad k \geq (3d+1)/4;$
- Theorem 5 : $N_{F,d-1} \sim C_{F,d-1} B^n, \quad d \geq 3.$

For the proofs of both theorems we apply the simple sieve of Hooley

$$N_1(B) - N_2(B) - N_3(B) \leq N_{F,k}(B) \leq N_1(B)$$

for certain quantities N_1, N_2, N_3, to be defined soon.
The difference in the proofs of the two theorems is only in the estimate of N_3. For this we use

- Theorem 1 : the determinant method like in [Browning, 2011];
- Theorem 5 : sieving argument à la [Hooley, 2009].

Sketch of the proof; simple sieve

For parameters $\xi_1 < \xi_2$ we define

$$N_1(B) = \#\{\mathbf{x} \in \mathbb{Z}^n : \|\mathbf{x}\| \le B, \quad p^k | F(\mathbf{x}) \implies p > \xi_1\},$$

$$N_2(B) = \#\{\mathbf{x} \in \mathbb{Z}^n : \|\mathbf{x}\| \le B, p^k | F(\mathbf{x}) \implies p > \xi_1, \\ \exists \xi_1 < p \le \xi_2 \text{ s.t. } p^2 | F(\mathbf{x})\},$$

and

$$N_3(B) = \#\{\mathbf{x} \in \mathbb{Z}^n : \|\mathbf{x}\| \le B, p^k | F(\mathbf{x}) \implies p > \xi_1, \\ p^2 \nmid F(\mathbf{x}) \text{ for } \xi_1 < p \le \xi_2 \text{ and } \exists p > \xi_2 \text{ s.t. } p^k | F(\mathbf{x})\}.$$

Then the initial simple sieve

$$N_1(B) - N_2(B) - N_3(B) \le N_{F,k}(B) \le N_1(B)$$

holds, since it is equivalent to

$$\boxed{\begin{array}{l} k\text{-free such that} \\ \forall p \in (\xi_1, \xi_2] \quad p^2 \nmid F(\mathbf{x}) \end{array}} \le N_{F,k}(B) \le \boxed{\begin{array}{l} k\text{-free or divisible by } p^k \\ \text{for some } p > \xi_1 \end{array}}$$

Sketch of the proof; $N_1(B)$

It is straightforward to show that

$$N_1(B) = B^n \prod_{p \leq \xi_1} \left(1 - \frac{\rho_F(p^k)}{p^{nk}}\right) + O_\varepsilon\left(B^{n-1+\varepsilon}\right).$$

Lemma 6

Let F be a square-free polynomial in n variables with integer coefficients, and such that for all primes p, p^k does not divide F identically. Then for any $k \geq 2$ we have $\rho_F(p^k) = O_F\left(p^{nk-2}\right)$.

It follows that the infinite product $C_{F,k} = \prod_p \left(1 - \rho_F(p^k)/p^{kn}\right)$ converges. When $B \to \infty$ we get

$$N_1(B) = \text{Main Term} + \text{Error Term},$$

so it is enough to show that $N_2(B), N_3(B)$ are error terms.

Sketch of the proof; $N_2(B)$

Recall that for $\mathbf{x} \in \mathbb{Z}^n$ counted by $N_2(B)$ there exists a prime $p \in (\xi_1, \xi_2]$ such that $p^2 \mid F(\mathbf{x})$. Then there are two possibilities:

- $p^2 \mid F(\mathbf{x}), p \nmid \frac{\partial F}{\partial x_1}(\mathbf{x})$
  Here for $f(x) := F(x, x_2, \ldots, x_n)$ we have $p \nmid \Delta(f)$ and we reduce the argument to polynomials in one variable. We use that $\rho_f(p^k) \leq d$ is independent of the coefficients of f. Then the contribution is

$$\ll_d B^{n-1} \sum_{\xi_1 < p \leq \xi_2} \left(\frac{B}{p^2} + 1 \right) \ll_d \frac{B^n}{\xi_1} + \frac{B^{n-1}\xi_2}{\log \xi_2}$$

  Actually, we choose $(\xi_1, \xi_2) = (\log B/nk, B(\log B)^{1/2})$ (Theorem 1) and $(\xi_1, \xi_2) = (\log_3 B/\log_4 B, B(\log B)^{1/n})$ (Theorem 5).
- $p^2 \mid F(\mathbf{x}), p \mid \frac{\partial F}{\partial x_1}(\mathbf{x})$
  These we estimate by the Ekedahl's sieve.

Sketch of the proof; $N_2(B)$

For the second case we apply

Ekedahl's sieve

Let $\mathcal{B}$ be a compact region in $\mathbb{R}^n$ having finite measure, and let Y be any closed subscheme of $\mathbb{A}^n_{\mathbb{Z}}$ of co-dimension $s \geq 2$. Let r and M be positive real numbers. Then we have

$$\#\{\mathbf{x} \in r\mathcal{B} \cap \mathbb{Z}^n : \mathbf{x} \pmod p \in Y(\mathbb{F}_p) \text{ for some prime } p > M\}$$

$$= O\left(\frac{r^n}{M^{s-1}\log M} + r^{n-s+1}\right).$$

We work with the variety $Y_F := \{\mathbf{x} \in \mathbb{C}^n : F(\mathbf{x}) = \frac{\partial F}{\partial x_1}(\mathbf{x}) = 0\}$. Then if $N^*(p;B) = \{\mathbf{x} \in \mathbb{Z}^n : \|\mathbf{x}\| \leq B, \mathbf{x}(p) \in Y_F(\mathbb{F}_p)\}$ the second group counted in $N_2(B)$ is bounded from above by

$$\# \bigcup_{p > \xi_1} N^*(p;B) \ll \frac{B^n}{\xi_1 \log \xi_1} + B^{n-1}$$

$N_3(B)$ for $N_{F,k}$, Theorem 1

We can reduce the argument to one variable case, by fixing $x_2, \ldots, x_n$. Again $f(x) = F(x, x_2, \ldots, x_n)$, $f \in \mathbb{Z}[x], \deg f \leq d$ and one needs to estimate

$$\#\{(x,y,z) \in \mathbb{Z}^3 : f(x) = yz^k, B_1/2 \leq x \leq B_1, B_2/2 \leq y \leq B_2, \\ B_3/2 \leq z \leq B_3\}$$

By the determinant method one can estimate the number of points in a box, lying on a surface, which is bounded by a quantity that is

- independent on the coefficients of f;
- gives power saving for $N_3(B)$;
- but only if $k \geq (3d+1)/4$.

$N_3(B)$ for $N_{F,d-1}$, Theorem 5

Using Ekedahl's sieve we can essentially assume that F is absolutely irreducible. To estimate $N_3(B)$ it is enough to evaluate the number of elements in a set of the type

$$\{\mathbf{x} \in \mathbb{Z}^n : \|\mathbf{x}\| \leq B, F(\mathbf{x}) = u_1 u_2 q^{d-1}, \text{ for prime } q > \xi_2\},$$

where $u_1 \mid \prod_{p<\xi_1} p^{d-2}$ and $u_2 \mid \prod_{\xi_1<p\leq\xi_2} p$. For this sake estimate the number of solutions $\pmod{u_1 u_2 \mathcal{D}}$ of the system of equations

$$F(\mathbf{m}) \equiv 0 \pmod{u_1}$$

$$F(\mathbf{m}) \equiv 0 \pmod{u_2}$$

$$F(\mathbf{m}) \equiv u_1 u_2 s^{d-1} \pmod{\mathcal{D}}, s = 0, 1, \ldots, \mathcal{D} - 1,$$

for a parameter $\mathcal{D}$ coprime to $u_1 u_2$. Apply trivial bound for the first and Lang-Weil bound for the other congruences, delicate choice of $\mathcal{D}$.

Thank you!