Counting points parametrized by infinitely many polynomial conditions

UROP+ Final Paper, Summer 2017

Avi Zeff
Mentor: Soohyun Park
Project suggested by Prof. Bjorn Poonen

August 31, 2017

Abstract

We count points satisfying polynomial equations modulo infinitely many primes. In particular we show that the number $\varrho(N)$ of points $(x_1, \ldots, x_n)$ such that every x_i is a positive integer and $\gcd(x_1, \ldots, x_\ell) = 1$ where $x_1^k + \cdots + x_n^k = N$ for a given positive integer N is of order $N^{n/k-1}$, using the circle method and the sieve of Erasthotenes. More generally we show that the density δ of points in $\mathbb{Z}^n$ at which m polynomials are relatively prime is lower bounded by a certain positive function of the degrees of the polynomial and the dimension n by upper bounding the number of simultaneous solutions of m polynomials in $\mathbb{F}_p^n$ for every prime p.

1 Introduction

It is often of interest to count the number of objects satisfying infinitely many conditions which can be mapped to lattice points on a variety satisfying conditions modulo each prime (see e.g. [3]). If we wish to find a global solution to some problem, we can often piece together "local" solutions modulo each prime in order to obtain a "global" solution over the integers by the Chinese remainder theorem. However, this is often more difficult if we need to satisfy infinitely many conditions. For example, as we will see in section 3, we need to upper bound the number of simultaneous solutions of the polynomial system in $\mathbb{F}_p^n$ for every prime p in order to estimate the density of points $x \in \mathbb{Z}^n$ such that two, or m, relatively prime polynomials in n dimensions evaluated at x are relatively prime.

We first investigate a modification of Waring's problem. We find in Theorem 2.4 the estimate for the number $\varrho(N)$ of solutions to $x_1^k + \cdots + x_n^k = N$ over positive integers

$$\varrho(N) = \frac{1}{\zeta(\ell)} \frac{\Gamma(1+1/k)^n}{\Gamma(n/k)} N^{n/k-1} \mathfrak{S}(N) + O(N^{n/k-1-\theta})$$

for some $\theta > 0$ provided $n \geq 2^k + \ell + 1$. We can understand this in terms of a main factor $cN^{n/k-1}$, which gives the expected result for a smoothed version of the problem where c is a constant term

depending on n, k, and ℓ, and the singular series $\mathfrak{S}(N)$, which adjusts the result to account for the fact that the solutions are also restricted by congruence relations. In order to show that the number of solutions is of the order $N^{n/k-1}$ we also need to show that $\mathfrak{S}(N)$ is bounded between two positive constants. The argument largely follows that of chapters 4, 5, and 7 of [2], which derive the analogous results for the unmodified Waring's problem, adapted and supplemented to allow for the new result.

We then move to the case of multiple general polynomials in n variables over all of $\mathbb{Z}^n$, where we will show that the density mentioned δ is lower bounded by

$$\exp\left(-n\vartheta(\sqrt{A}) - \left(\log\zeta(2) - P(2) + \frac{1}{\sqrt{A}}\right) A\log(2A)\right),$$

where $A = (n-1)\left(\sum_i \deg f_i + \prod_i \deg f_i\right)\min_i \deg f_i$ and $\vartheta(x)$ is Chebyshev's first function $\sum_{p\leq x}\log p$. In order to find this bound we use the identity that

$$\sum_{d|\gcd(A_1,\ldots,A_m)} \mu(d)$$

is 1 if $A_1,\ldots,A_m$ are relatively prime and 0 otherwise to write the density as a Dirichlet series and then factor it into a product over the primes. The problem then reduces to that of upper bounding the number of common solutions of two, or m, polynomials in $\mathbb{F}_p^n$. We find such a bound using the properties of resultants and induction on the dimension n.

1.1 Acknowledgements

The author thanks Soohyun Park for her mentoring and guidance, Professor Bjorn Poonen for suggesting this problem, and the MIT Department of Mathematics UROP+ program for providing the opportunity and funding for this research.

2 A modified version of Waring's problem

Let $\varrho(N)$ be the number of ways that N can be written as the sum of n kth powers of positive integers $x_1^k + \cdots + x_n^k$ such that $\gcd(x_1,\ldots,x_\ell) = 1$. Our method is to find a simpler form for the exponential sum

$$\sum_{x=1}^{N} \varrho(x)e(\alpha x),$$

where $e(u) = e^{2\pi iu}$, and by an inverse discrete Fourier transform express $\varrho(N)$ in terms of the integral of this exponential sum times $e(-\alpha N)$. We will then divide the interval $[0,1]$ into major and minor arcs. The major arcs make up relatively little of the interval but the exponential sum is large on them, while the minor arcs make up the bulk of the interval but on them the exponential sum is small. We can then extract a main term from the integral over the major arcs and show that the contribution from the minor arcs is of smaller order than this main term.

However, it turns out that the main term that we get from the major arcs has an arithmetic factor, denoted the singular series, whose nature is not entirely clear. Thus in order to show that $\varrho(N)$ has the order stated we need to show that the singular series is bounded between two positive

constants. We do this by factoring it into a product over primes and then showing that the factors from all sufficiently large primes converge and that no factor is zero.

Let

$$T(\alpha) = \sum_{x=1}^{P} e(\alpha x^k)$$

and

$$U(\alpha) = \sum_{\substack{x_1,\dots,x_\ell=1 \\ \gcd(x_1,\dots,x_\ell)=1}}^{P} e(\alpha(x_1^k + \cdots + x_\ell^k)).$$

Then we have

$$T(\alpha)^{n-\ell} U(\alpha) = \sum_{x=1}^{N} \varrho(x) e(\alpha x)$$

provided P is sufficiently large, in particular with $P \geq N^{1/k}$. Taking the inverse Fourier transform we obtain

$$\varrho(N) = \int_0^1 T(\alpha)^{n-\ell} U(\alpha) e(-\alpha N)\, d\alpha.$$

Now fixing δ to depend on N let $\mathfrak{M}_{a,q}$ for some coprime a, q be the interval consisting of the points $\frac{a}{q} + \beta$ for $|\beta| < P^{\delta-k}$ for coprime a and q with $1 \leq a \leq q \leq P^\delta$ with the larger half of the interval around 1 wrapping around modulo 1, and let $\mathfrak{M}$ be the collection of the $\mathfrak{M}_{a,q}$ for all such a, q. Further let $\mathfrak{m}$ be the complement of $\mathfrak{M}$ on $[0, 1]$.

Consider the integral from above over the major arcs $\mathfrak{M}_{a,q}$. Let

$$S_{a,q} = \sum_{z=1}^{q} e\left(\frac{a}{q} z^k\right),$$

$$\sigma_{a,q} = \sum_{\substack{z_1,\dots,z_\ell \\ \gcd(z_1,\dots,z_\ell,q)=1}} e\left(\frac{a}{q}(z_1^k + \cdots + z_\ell^k)\right),$$

$$I(\beta) = \int_0^P e(\beta \xi^k)\, d\xi,$$

and

$$f(q) = \prod_{p \mid q} \left(1 - \frac{1}{p^\ell}\right)^{-1}.$$

Then we have the following:

Lemma 2.1. *For α in $\mathfrak{M}_{a,q}$ we have:*
a) $T(\alpha) = q^{-1} S_{a,q} I(\beta) + O(P^{2\delta})$
b) $U(\alpha) = \frac{1}{\zeta(\ell)} \frac{f(q)}{q}^{-\ell} \sigma_{a,q} I(\beta)^\ell + O(P^{\ell-1+(\ell+1)\delta})$, *where $\zeta(s)$ is the Riemann zeta function.*

Proof of a) (following [2]). Reordering the sum by congruence classes we have

$$T(\alpha) = \sum_{z=1}^{q} e\left(\frac{a}{q}z^k\right) \sum_{y=0}^{\frac{P-z}{q}} e(\beta(qy+z)^k).$$

By the Euler-Maclaurin formula we can replace the inner summation by the integral

$$\frac{1}{q}\int_0^P e(\beta\xi^k)\,d\xi = q^{-1}I(\beta)$$

up to error $P^k|\beta| = O(P^\delta)$, so we have

$$T(\alpha) = \sum_{z=1}^{q} e\left(\frac{a}{q}z^k\right)\left(q^{-1}I(\beta) + O(P^\delta)\right) = q^{-1}S_{a,q}I(\beta) + O(P^{2\delta})$$

□

Proof of b). Collecting the terms of each x_i in the same congruence classes modulo q as above we have

$$\begin{aligned}
U(\alpha) &= \sum_{1\le z_1,\dots,z_\ell\le q} \sum_{\substack{x_1,\dots,x_\ell=1\\ x_i\equiv z_i \pmod q\\ \gcd(x_1,\dots,x_\ell)=1}}^{P} e\left(\left(\frac{a}{q}+\beta\right)(x_1^k+\cdots+x_\ell^k)\right)\\
&= \sum_{1\le z_1,\dots,z_\ell\le q} e\left(\frac{a}{q}(z_1^k+\cdots+z_\ell^k)\right) \sum_{\substack{1\le x_1,\dots,x_\ell\le P\\ x_i\equiv z_i \pmod q\\ \gcd(x_1,\dots,x_\ell)=1}} e(\beta(x_1^k+\cdots+x_\ell^k))\\
&= \sum_{1\le z_1,\dots,z_\ell\le q} e\left(\frac{a}{q}(z_1^k+\cdots+z_\ell^k)\right) \sum_{\substack{1\le x_1,\dots,x_\ell\le P\\ x_i\equiv z_i \pmod q}} e(\beta(x_1^k+\cdots+x_\ell^k)) \sum_{d\mid \gcd(x_1,\dots,x_\ell)} \mu(d)\\
&= \sum_{1\le z_1,\dots,z_\ell\le q} e\left(\frac{a}{q}(z_1^k+\cdots+z_\ell^k)\right) \sum_{d=1}^{P}\mu(d) \sum_{\substack{1\le x_1,\dots,x_\ell\le P\\ x_i\equiv z_i \pmod q\\ d\mid \gcd(x_1,\dots,x_\ell)}} e(\beta(x_1^k+\cdots+x_\ell^k)).
\end{aligned}$$

Let

$$W(z,q,d) = \sum_{\substack{1\le x\le P\\ x\equiv z \pmod q\\ d\mid x}} e(\beta x^k).$$

If $(q,d) > 1$ and $(q,d) \nmid z$, then $W(z,q,d) = 0$ since there are no x satisfying the restrictions. If $(q,d) = 1$, then the condition that $x \equiv z \pmod q$ and $d|x$ implies that $x \equiv a \pmod{qd}$ for exactly one a between 1 and qd by the Chinese remainder theorem. Therefore we have

$$W(z,q,d) = \sum_{y=0}^{\frac{P-a}{qd}} e(\beta(qdy+a)^k).$$

By the same argument as in the proof of a) this is equal to

$$\int_0^{\frac{P-a}{qd}} e(\beta(qd\eta+a)^k)\,d\eta$$

up to error in $O(\beta P^k) = O(P^\delta)$. Letting $\xi = qd\eta + a$, we have for $(q,d)=1$

$$W(z,q,d) = \frac{1}{qd}\int_0^P e(\beta\xi^k)\,d\xi + O(P^\delta) = \frac{1}{qd}I(\beta) + O(P^\delta).$$

Now

$$U(\alpha) = \sum_{1\le z_1,\dots,z_\ell\le q}\sum_{d=1}^{P}\mu(d)\prod_{i=1}^{\ell}W(z_i,q,d).$$

If $(z_1,\dots,z_\ell,q) > 1$, we see that the inner sum is equal to 0, since from the first equation above in which we first collected the x_i by congruence classes any such x_i cannot be coprime. Therefore we consider only the case in which $(z_1,\dots,z_\ell,q)=1$. If (d,q) is greater than 1, since $(z_1,\dots,z_\ell,q)=1$ it does not divide at least one of the z_i, so $\prod_{i=1}^{\ell}W(z_i,q,d)=0$. This leaves only the case in which $(q,d)=1$, in which case $\prod_{i=1}^{\ell}W(z_i,q,d) = \frac{1}{q^\ell d^\ell}I(\beta)^\ell + O(d^{1-\ell}P^{\ell-1+\delta})$. Therefore

$$\begin{aligned}U(\alpha) &= \frac{1}{q^\ell}I(\beta)^\ell \sum_{\substack{1\le z_1,\dots,z_\ell\le q\\(z_1,\dots,z_\ell,q)=1}} e\left(\frac{a}{q}(z_1^k+\cdots+z_\ell^k)\right)\sum_{\substack{1\le d\le P\\(q,d)=1}}\frac{\mu(d)}{d^\ell} + O(P^{\ell-1+(\ell+1)\delta}\log P)\\ &= \frac{1}{q^\ell}\sigma_{a,q}I(\beta)^\ell\sum_{\substack{d\ge 1\\(q,d)=1}}\frac{\mu(d)}{d^\ell} + O(P^{\ell-1+(\ell+1)\delta}\log P),\end{aligned}$$

since the error accrued by extending the sum to infinity is of order $\frac{1}{P}$ and can be neglected. Now consider the product

$$\prod_{p\nmid q}\left(1-\frac{1}{p^\ell}\right).$$

If we expand this out, we see that it is exactly equal to the infinite sum above. On the other hand, it is also equal to

$$\left(\prod_p\left(1-\frac{1}{p^\ell}\right)\right)\left(\prod_{p\mid q}\left(1-\frac{1}{p^\ell}\right)\right)^{-1} = \frac{f(q)}{\zeta(\ell)}$$

which gives us the desired result. □

Having obtained an estimate for each factor of the integrand over the major arcs, we now combine them to get an estimate for the total contribution of the integral over the major arcs. Let

$$\mathfrak{S}(N,B) = \sum_{q=1}^{B}\frac{f(q)}{q^n}\sum_{\substack{1\le a\le q\\(a,q)=1}}S_{a,q}^{n-\ell}\sigma_{a,q}e\left(-\frac{a}{q}N\right).$$

Lemma 2.2. *The contribution from the major arcs is*

$$\int_{\mathfrak{M}} T(\alpha)^{n-\ell} U(\alpha) e(-\alpha N)\, d\alpha = \frac{1}{\zeta(\ell)} \frac{\Gamma(1+1/k)^n}{\Gamma(n/k)} P^{n-k} \mathfrak{S}(N, P^\delta) + O(P^{n-k-\theta})$$

for some $\theta > 0$.

Proof. Combining our results from Lemma 2.1, we have that for $\alpha \in \mathfrak{M}_{a,q}$

$$T(\alpha)^{n-\ell} U(\alpha) = \frac{f(q)}{\zeta(\ell)} q^{-\ell} I(\beta)^n S_{a,q}^{n-\ell} \sigma_{a,q} + O(P^{n-1+(\ell+1)\delta} \log P).$$

Multiplying by $e(-\alpha N)$ and integrating over $|\beta| < P^{\delta-k}$ gives

$$\frac{f(q)}{\zeta(\ell)} q^{-n} S_{a,q}^{n-\ell} e\left(-\frac{a}{q}N\right) \sigma_{a,q} \int_{|\beta|<P^{\delta-k}} I(\beta) e(-\beta N)\, d\beta + O(P^{n-k-1+(\ell+2)\delta} \log P).$$

Summing over a and q up to $q \le P^\delta$, this becomes $\frac{1}{\zeta(\ell)} \mathfrak{S}(N, P^\delta)$ times the integral plus the error term. The integral is evaluated in [2] in the proofs of Lemma 4.3 and Theorem 4.1 by a change of variables and an application of Fourier's integral theorem and gives $\frac{\Gamma(1+1/k)^n}{\Gamma(n/k)} P^{n-k}$ plus negligible error, and the error term summed over $q \le P^\delta$ and $a \le q$, $(a,q) = 1$ is in $O(P^{n-k-1+(\ell+4)\delta} \log P)$. Since we can choose $\delta < \frac{1}{\ell+4}$ this implies the error term given. □

In order to obtain an asymptotic formula it remains only to bound the contribution from the minor arcs $\mathfrak{m}$.

Lemma 2.3. *For $n \ge 2^k + \ell + 1$, the contribution from the minor arcs is*

$$\int_{\mathfrak{m}} T(\alpha)^{n-\ell} U(\alpha) e(-\alpha N)\, d\alpha = O(P^{n-k-\theta})$$

for some $\theta > 0$.

Proof. Lemma 4.1 of [2] shows that for $s \ge 2^k + 1$ we have $\int_{\mathfrak{m}} |T(\alpha)|^s\, d\alpha = O(P^{s-k-\epsilon})$ for some $\epsilon > 0$ depending on δ by using Dirichlet's theorem on Diophantine approximation to show that the denominator of any such approximation must be large and then applying the Weyl and Hua inequalities. Choosing $s = n - \ell$ and using the fact that $U(\alpha) = O(P^\ell)$ everywhere the result follows. □

We are now prepared to prove our first main theorem. Let $\mathfrak{S}(N) = \lim_{B\to\infty} \mathfrak{S}(N, B)$.

Theorem 2.4. *For $n \ge 2^k + \ell + 1$ we have*

$$\varrho(N) = \frac{1}{\zeta(\ell)} \frac{\Gamma(1+1/k)^n}{\Gamma(n/k)} N^{n/k-1} \mathfrak{S}(N) + O(N^{n/k-1-\theta})$$

for some $\theta > 0$.

Proof. We can choose any P sufficiently large that in any sum of $\sum x_i^k = N$ every $x_i \le P$. If we choose $P = \lfloor N^{1/k} \rfloor$ this is sufficient, so applying Lemmas 2.2 and 3.3 with $P = \lfloor N^{1/k} \rfloor$ immediately gives the result with negligible error. □

In order to show that $\rho(N) \asymp N^{n/k-1}$, where $f(x) \asymp g(x)$ indicates that $\lim_{x\to\infty} \frac{f(x)}{g(x)}$ is nonzero and finite, we now need to examine the singular series $\mathfrak{S}(N)$.

Let $A(q) = \frac{f(q)}{q^n} \sum_{\substack{1\le a\le q\\(a,q)=1}} S_{a,q}^{n-\ell} \sigma_{a,q} e\left(-\frac{a}{q}N\right)$, so that $\mathfrak{S}(N) = \sum_{q=1}^{\infty} A(q)$. Then we claim the following.

Lemma 2.5. *$A(q)$ is multiplicative.*

Proof. We first show that if $(a_1, q_1) = (a_2, q_2) = (q_1, q_2) = 1$, then letting $q = q_1q_2$ and $a \equiv a_1q_2 + a_2q_1 \pmod q$ we have $\sigma_{a,q} = \sigma_{a_1,q_1}\sigma_{a_2,q_2}$. Write

$$\begin{aligned}
\sigma_{a,q} &= \sum_{\substack{1\le z_1,\dots,z_\ell\le q\\(z_1,\dots,z_\ell,q)=1}} e\left(\frac{a}{q}(z_1^k+\cdots+z_\ell^k)\right) = \sum_{d\mid q}\mu(d) \sum_{1\le z_1,\dots,z_\ell\le q} e\left(\frac{a}{q}((dz_1)^k+\cdots+(dz_\ell)^k)\right)\\
&= \sum_{d_1\mid q_1}\sum_{d_2\mid q_2}\mu(d_1)\mu(d_2)\\
&\qquad \sum_{1\le z_{1,1},\dots,z_{\ell,1}\le q_1} \sum_{1\le z_{1,2},\dots,z_{\ell,2}\le q_2} e\left(\frac{a}{q}\left((z_{1,1}q_2+z_{1,2}q_1)^k+\cdots+(z_{\ell,1}q_2+z_{\ell,2}q_1)^k\right)\right)\\
&= \sum_{d_1\mid q_1}\sum_{d_2\mid q_2}\mu(d_1)\mu(d_2) \sum_{1\le z_{1,1},\dots,z_{\ell,1}\le q_1} \sum_{1\le z_{1,2},\dots,z_{\ell,2}\le q_2}\\
&\qquad e\left(\left(\frac{a_1}{q_1}+\frac{a_2}{q_2}\right)\left((z_{1,1}q_2)^k+(z_{1,2}q_1)^k+\cdots+(z_{\ell,1}q_2)^k+(z_{\ell,2}q_1)^k\right)\right)\\
&= \sum_{d_1\mid q_1}\sum_{d_2\mid q_2}\mu(d_1)\mu(d_2) \sum_{1\le z_{1,1},\dots,z_{\ell,1}\le q_1} \sum_{1\le z_{1,2},\dots,z_{\ell,2}\le q_2}\\
&\qquad e\left(\frac{a_1}{q_1}((z_{1,1}q_2)^k+\ldots+(z_{\ell,1}q_2)^k)+\frac{a_2}{q_2}((z_{1,2}q_1)^k+\cdots+(z_{\ell,2}q_1)^k)\right)\\
&= \left(\sum_{d_1\mid q_1}\mu(d) \sum_{1\le z_{1,1},\dots,z_{\ell,1}\le q_1} e\left(\frac{a_1}{q_1}(z_{1,1}^k+\cdots+z_{\ell,1}^k)\right)\right)\\
&\qquad \cdot\left(\sum_{d_2\mid q_2}\mu(d) \sum_{1\le z_{1,2},\dots,z_{\ell,2}\le q_2} e\left(\frac{a_2}{q_2}(z_{1,2}^k+\cdots+z_{\ell,2}^k)\right)\right)
\end{aligned}$$

since $(q_1, q_2) = 1$ so removing their powers simply rearranges the order of the inner sums. We saw above that

$$\sigma_{a,q} = \sum_{d\mid q}\mu(d) \sum_{1\le z_1,\dots,z_\ell\le q} e\left(\frac{a}{q}((dz_1)^k+\cdots+(dz_\ell)^k)\right),$$

so this is simply $\sigma_{a_1,q_1}\sigma_{a_2,q_2}$. Now we have from the proof of Lemma 5.1 in [2] that for similar

a_1, a_2, q_1, q_2 we have $S_{a,q} = S_{a_1,q_1} S_{a_2,q_2}$, so it follows that

$$\begin{aligned}
&\left(\sum_{\substack{1 \le a_1 \le q_1 \\ \gcd(a_1,q_1)=1}} S_{a_1,q_1}^{n-\ell} \sigma_{a_1,q_1} e\left(-\frac{a_1}{q_1} N\right) \right) \left(\sum_{\substack{1 \le a_2 \le q_2 \\ \gcd(a_2,q_2)=1}} S_{a_2,q_2}^{n-\ell} \sigma_{a_2,q_2} e\left(-\frac{a_2}{q_2} N\right) \right) \\
&= \sum_{\substack{1 \le a_1 \le q_1 \\ \gcd(a_1,q_1)=1}} \sum_{\substack{1 \le a_2 \le q_2 \\ \gcd(a_2,q_2)=1}} (S_{a_1,q_1} S_{a_2,q_2})^{n-\ell} \sigma_{a_1,q_1} \sigma_{a_2,q_2} e\left(-\left(\frac{a_1}{q_1} + \frac{a_2}{q_2}\right) N\right) \\
&= \sum_{\substack{1 \le a \le q \\ \gcd(a,q)=1}} S_{a,q}^{n-\ell} \sigma_{a,q} e\left(-\frac{a}{q} N\right).
\end{aligned}$$

Since $f(q)q^{-n}$ is clearly multiplicative the result follows. □

Let

$$\chi(p) = \sum_{j=0}^{\infty} A(p^j).$$

Lemma 2.6. *For $n \ge 2^k + 1$, we have*

$$\mathfrak{S}(N) = \prod_p \chi(p)$$

and there exists a fixed $\epsilon > 0$ such that $|\chi(p) - 1| \ll p^{-1-\epsilon}$ where the implied constant depends only on ϵ.

Proof. The factorization of $\mathfrak{S}$ follows immediately from Lemma 2.5. By applying Weyl's inequality to $S_{a,q}$ we see immediately that $S_{a,q} \ll q^{1-2^{1-k}+\epsilon}$ for any $\epsilon > 0$, where the implied constant depends only on ϵ. For $q = p^j$ for some positive integer j $\gcd(z_1, \dots, z_\ell, q)$ is 1 unless p divides all of the z_i. There are ℓ^j sets of z_i for which this is the case, so as $p \to \infty$ $\sigma_{a,q} = O(S_{a,q}^{\ell})$. Therefore

$$A(p^j) \ll \sum_{a=1}^{p^j} p^{(-2^{1-k}+\epsilon)jn} \ll \sum_{a=1}^{p^j} p^{(-2-2^{1-k}+2^k\epsilon)j} \ll p^{-1-2^{1-k}+2^k\epsilon}.$$

Choosing ϵ sufficiently small it follows that

$$|\chi(p) - 1| \ll \sum_{j=1}^{\infty} p^{-1-\epsilon} \ll p^{-1-\epsilon}.$$

□

Remark. It immediately follows that there exists a p_0 such that $\frac{1}{2} \le \prod_{p>p_0} \chi(p) \le \frac{3}{2}$. Indeed this is enough to show that $\mathfrak{S}(N)$ is upper bounded by a constant, so in order to show that $\varrho(N) \asymp N^{n/k-1}$ we need only find a constant lower bound.

Let $M(q)$ be the number of solutions to

$$z_1^k + z_2^k + \cdots + z_n^k \equiv N \pmod{q}$$

with $1 \le z_i \le q$ such that $\gcd(z_1, \dots, z_\ell, q) = 1$. The primary tools that we use to establish a lower bound on $\mathfrak{S}(N)$ are Lemma 2.6 and a connection between the factors $\chi(p)$ and $M(q)$ in the following lemma.

Lemma 2.7. *For any integer $\nu \ge 1$ we have*

$$\sum_{j=1}^{\nu} A(p^j) = \frac{f(p)}{p^{\nu(n-1)}} M(p^\nu) = \frac{M(p^\nu)}{p^{\nu(n-1)}(1-p^{-\ell})},$$

so that

$$\chi(p) = \lim_{\nu\to\infty} \frac{f(p)}{p^{\nu(n-1)}} M(p^\nu) = \lim_{\nu\to\infty} \frac{M(p^\nu)}{p^{\nu(n-1)}(1-p^{-\ell})}.$$

Proof. Write

$$M(q) = \frac{1}{q} \sum_{t=1}^{q} \sum_{\substack{1\le z_1,\dots,z_\ell\le q\\ \gcd(z_1,\dots,z_\ell,q)=1}} \sum_{1\le z_{\ell+1},\dots,z_n\le q} e\left(\frac{t}{q}(z_1^k + z_2^k + \cdots + z_n^k - N)\right).$$

Collect together the t sharing a greatest common factor $\frac{q}{q_1}$ with q. Then we have

$$\begin{aligned}
M(q) &= \frac{1}{q} \sum_{q_1\mid q} \sum_{\substack{1\le u\le q_1\\ (u,q_1)=1}} \sum_{\substack{1\le z_1,\dots,z_\ell\le q\\ \gcd(z_1,\dots,z_\ell,q)=1}} \sum_{1\le z_{\ell+1},\dots,z_n\le q} e\left(\frac{u}{q_1}(z_1^k + z_2^k + \cdots + z_n^k - N)\right)\\
&= \frac{1}{q} \sum_{q_1\mid q} \sum_{\substack{1\le u\le q_1\\ (u,q_1)=1}} \left(\frac{q}{q_1}\right)^{n-\ell} S_{u,q_1}^{n-\ell} e\left(-\frac{u}{q_1}N\right) \sum_{\substack{1\le z_1,\dots,z_\ell\le q\\ \gcd(z_1,\dots,z_\ell,q)=1}} e\left(\frac{u}{q_1}(z_1^k + \cdots + z_\ell^k)\right)\\
&= \frac{1}{q} \sum_{q_1\mid q} \sum_{\substack{1\le u\le q_1\\ (u,q_1)=1}} \left(\frac{q}{q_1}\right)^{n-\ell} S_{u,q_1}^{n-\ell} e\left(-\frac{u}{q_1}N\right)\\
&\qquad \sum_{0\le j_1,\dots,j_\ell<q/q_1} \sum_{1\le l_1,\dots,l_\ell\le q_1} e\left(\frac{u}{q_1}\left((j_1q_1+l_1)^k + \cdots + (j_\ell q_1 + l_\ell)^k\right)\right) \sum_{\substack{d\mid q\\ \forall i: d\mid j_iq_1+l_i}} \mu(d)\\
&= \frac{1}{q} \sum_{q_1\mid q} \sum_{\substack{1\le u\le q_1\\ (u,q_1)=1}} \left(\frac{q}{q_1}\right)^{n-\ell} S_{u,q_1}^{n-\ell} e\left(-\frac{u}{q_1}N\right)\\
&\qquad\qquad \sum_{0\le j_1,\dots,j_\ell<q/q_1} \sum_{1\le l_1,\dots,l_\ell\le q_1} e\left(\frac{u}{q_1}(l_1^k + \cdots + l_\ell^k)\right) \sum_{\substack{d\mid q\\ \forall i: d\mid j_iq_1+l_i}} \mu(d).
\end{aligned}$$

Suppose that for particular $q_1, l_1, \dots, l_\ell$ we have $(l_1, \dots, l_\ell, q_1) > 1$. Then the innermost sum must be 0, since there exist $d > 1$ satisfying the appropriate restrictions. Therefore we can restrict the

sum over $l_1, \dots, l_\ell$ to those pairs such that $(l_1, \dots, l_\ell, q_1) = 1$. Now suppose that a particular d divides q_1. Since we have restricted $l_1, \dots, l_\ell$, it follows that either d does not divide all of the $j_i q_1 + l_i$ or $d = 1$, so we can restrict the sum over d to those d not dividing q_1 and $d = 1$. For these d with the aforementioned restrictions on the l_i, there will be exactly one j_i in any complete residue system modulo d such that $d | j_i q_1 + l_i$ for a given l_i. Therefore we have

$$\begin{aligned} M(q) &= \frac{1}{q} \sum_{q_1 | q} \sum_{\substack{1 \le u \le q_1 \\ (u, q_1) = 1}} \left(\frac{q}{q_1}\right)^{n-\ell} S_{u,q_1}^{n-\ell} e\left(-\frac{u}{q_1} N\right) \\ &\qquad \left(\left(\frac{q}{q_1}\right)^{\ell} \sigma_{u,q_1} + \sum_{\substack{d | q \\ d \nmid q_1}} \mu(d) \left(\frac{q}{q_1 d}\right)^{\ell} \sum_{\substack{1 \le l_1, \dots, l_\ell \le q_1 \\ (l_1, \dots, l_\ell, q_1) = 1}} e\left(\frac{u}{q_1}(l_1^k + \cdots + l_\ell^k)\right) \right) \\ &= \frac{1}{q} \sum_{q_1 | q} \sum_{\substack{1 \le u \le q_1 \\ (u, q_1) = 1}} \left(\frac{q}{q_1}\right)^{n} S_{u,q_1}^{n-\ell} \sigma_{u,q_1} e\left(-\frac{u}{q_1} N\right) \left(1 + \sum_{\substack{d | q \\ d \nmid q_1}} \frac{\mu(d)}{d^\ell} \right). \end{aligned}$$

Setting $q = p^\nu$, we have

$$\begin{aligned} M(p^\nu) &= p^{\nu(n-1)} \sum_{j=0}^{\nu} p^{-jn} \sum_{\substack{1 \le u \le p^j \\ (u, p^j) = 1}} S_{u,p^j}^{n-\ell} \sigma_{u,p^j} e\left(-\frac{u}{p^j} N\right) \left(1 + \sum_{l=j+1}^{\nu} \frac{\mu(p^l)}{p^{\ell l}} \right) \\ &= p^{\nu(n-1)} \sum_{j=0}^{\nu} p^{-jn} \sum_{\substack{1 \le u \le p^j \\ (u, p^j) = 1}} S_{u,p^j}^{n-\ell} \sigma_{u,p^j} e\left(-\frac{u}{p^j} N\right) - p^{\nu(n-1)-\ell} \\ &= p^{\nu(n-1)} \sum_{j=0}^{\nu} \frac{A(p^j)}{f(p^j)} - p^{\nu(n-1)-\ell} \\ &= p^{\nu(n-1)} \left(1 - p^{-\ell}\right) \sum_{j=1}^{\nu} A(p^j), \end{aligned}$$

from which the result follows. □

In order to use this connection to show that the $\chi(p)$ are nonzero we need the following result.

Lemma 2.8. *If $M(p^\gamma) \ge 1$, where γ is equal to $\tau + 1$ for $p = 2$ and $\tau + 2$ for all $p > 2$ where τ is the largest positive integer such that p^τ divides k, we have $M(p^\nu) \ge p^{(\nu-\gamma)(n-1)}(1 - p^{k-\nu})$.*

Proof. Let $a_1, a_2, \dots, a_n$ with each a_i between 1 and p^γ be the solution modulo p^γ whose existence is assumed. Choose $z_{\ell+1}, \dots, z_n$ between 1 and p^ν such that $z_i \equiv a_i \pmod{p^\gamma}$. This can be done in $p^{(\nu-\gamma)(n-\ell)}$ ways. Then $N - z_{\ell+1}^k - \cdots - z_n^k \equiv a_1^k + \cdots + a_\ell^k \pmod{p^\gamma}$, so the problem is reduced to counting the number of solutions to $z_1^k + \cdots + z_\ell^k \equiv m \pmod{p^\nu}$ where $(z_1, \dots, z_\ell, p) = 1$, given that the same congruence modulo p^γ has at least one solution with the same restriction. Let this

number of solutions be denoted $G(m,p^\nu)$, and let $G_c(m,p^\nu)$ be the number of solutions to the same congruence without the requirement that $(z_1,\dots,z_\ell,p)=1$. Then assuming $\nu\geq 2$ we have

$$\begin{aligned}
G(m,p^\nu) &= p^{-\nu}\sum_{t=1}^{p^\nu}\sum_{\substack{1\leq z_1,\dots,z_\ell\leq p^\nu\\(z_1,\dots,z_\ell,p)=1}} e\left(\frac{t}{p^\nu}(z_1^k+\cdots+z_\ell^k-m)\right)\\
&= p^{-\nu}\sum_{t=1}^{p^\nu}\sum_{1\leq z_1,\dots,z_\ell\leq p^\nu} e\left(\frac{t}{p^\nu}(z_1^k+\cdots+z_\ell^k-m)\right)\sum_{\substack{d\mid p\\ d\mid \gcd(z_1,\dots,z_\ell)}}\mu(d)\\
&= p^{-\nu}\sum_{t=1}^{p^\nu}\sum_{1\leq z_1,\dots,z_\ell\leq p^\nu} e\left(\frac{t}{p^\nu}(z_1^k+\cdots+z_\ell^k-m)\right)\\
&\qquad - p^{-\nu}\sum_{t=1}^{p^\nu}\sum_{1\leq x_1,\dots,x_\ell\leq p^{\nu-1}} e\left(\frac{t}{p^\nu}((px_1)^k+\cdots+(px_\ell)^k-m)\right)\\
&= G_c(m,p^\nu) - p^{-\nu}\sum_{t=1}^{p^\nu} e\left(-\frac{t}{p^\nu}m\right)\sum_{1\leq x_1,\dots,x_\ell\leq p^{\nu-1}} e\left(\frac{t}{p^{\nu-k}}(x_1^k+\cdots+x_\ell^k)\right)\\
&= G_c(m,p^\nu) - p^{-\nu+\ell(k-1)}\sum_{t=1}^{p^\nu} S^\ell_{t,p^{\nu-k}} e\left(-\frac{t}{p^\nu}m\right)\\
&= G_c(m,p^\nu) - p^{-\nu+\ell(k-1)}\sum_{t=1}^{p^{\nu-k}}\sum_{j=0}^{p^k-1} S^\ell_{t,p^{\nu-k}} e\left(-\frac{t+p^{\nu-k}j}{p^\nu}m\right)\\
&= G_c(m,p^\nu) - p^{-\nu+\ell(k-1)}\sum_{t=1}^{p^{\nu-k}} S^\ell_{t,p^{\nu-k}} e\left(-\frac{t}{p^\nu}m\right)\sum_{j=0}^{p^k-1} e\left(-\frac{j}{p^k}m\right).
\end{aligned}$$

If m is not divisible by p^k, then the second part is 0, and we have simply $G(m,p^\nu)=G_c(m,p^\nu)$. If $p^k|m$, then the innermost sum is p^k, so we have

$$\begin{aligned}
G(m,p^\nu) &= G_c(m,p^\nu) - p^{-\nu+\ell(k-1)+k}\sum_{t=1}^{p^{\nu-k}}\sum_{1\leq z_1,\dots,z_\ell\leq p^{\nu-k}} e\left(-\frac{t}{p^{\nu-k}}\left(z_1^k+\cdots+z_\ell^k-\frac{m}{p^k}\right)\right)\\
&= G_c(m,p^\nu) - p^{\ell(k-1)}G_c\left(\frac{m}{p^k},p^{\nu-k}\right).
\end{aligned}$$

Carrying out the procedure as at the start of the proof with 1 in place of ℓ and setting $n=\ell$ shows that $G_c(m,p^\nu)\geq p^{(\nu-\gamma)(\ell-1)}$. If $p^k\nmid m$ then it follows that $G(m,p^\nu)=G_c(m,p^\nu)\geq p^{(\nu-\gamma)(\ell-1)}$, so the total number of ways to choose $z_1,\dots,z_\ell,\dots,z_n$ satisfying the appropriate requirements is at least $p^{(\nu-\gamma)(n-1)}$. However this method only accounts for m not divisible by p^k, so we must modify our initial count to the number of ways we can choose $z_{\ell+1},\dots,z_n$ such that $N-z_{\ell+1}^k-\cdots-z_n^k$ is not divisible by p^k. We can lower bound this by allowing only z_n to vary to see that there are at least $p^{(\nu-\gamma)(n-\ell)}(1-p^{k-\nu})$ such ways to choose $z_{\ell+1},\dots,z_n$, so in total there are at least $p^{(\nu-\gamma)(n-1)}(1-p^{k-\nu})$ as desired. □

Finally we need to satisfy the condition on Lemma 2.8.

Lemma 2.9. *For $n \geq 2k$ if k is odd and $n \geq 4k$ if k is even, for every prime p we have $M(p^\gamma) \geq 1$.*

Proof. The proof in [2] of Lemma 5.6 shows that for every $N \geq 1$ there exist $z_1, z_2, \ldots, z_n$ between 1 and p^γ for every prime p such that $z_1^k + z_2^k + \cdots + z_n^k \equiv N \pmod{p^\gamma}$ with $z_1, z_2, \ldots, z_n$ not all divisible by p with n as in the statement of the theorem by distributing the N into classes by the value of the least n such that the relevant congruence is soluble and demonstrating that no two consecutive classes are both empty, so that for n satisfying the conditions stated the congruence must be soluble for all N. We can simply rearrange the z_i such that $z_1, \ldots, z_\ell$ are not all divisible by p, so that $M(p) \geq 1$ for all p. □

This gives us everything we need to lower bound $\mathfrak{S}(N)$.

Theorem 2.10. *For $n \geq 2^k + 1$ there exists some $c > 0$ independent of N such that for every $N \geq 1$ we have $\mathfrak{S}(N) \geq c$.*

Proof. The result follows immediately from Lemmas 2.9, 2.8, 2.7, and 2.6. □

Combining Theorems 2.4 and 2.10 with the observation that $\mathfrak{S}(N)$ is upper bounded by a constant as a result of Lemma 2.6 gives us the desired result:

Corollary 2.11. *For $n \geq 2^k + 1$ we have*

$$\varrho(N) \asymp N^{n/k-1}.$$

We can generalize this result by allowing each coordinate x_i to have a corresponding nonzero coefficient c_i, so that the problem is now counting the number $\varrho(N)$ of solutions to $c_1x_1^k + \cdots + c_nx_n^k = N$ such that $x_1, \ldots, x_n$ are positive integers and $\gcd(x_1, \ldots, x_\ell) = 1$. We require the c_i to be such that for every positive integer N the congruence $c_1x^k + \cdots + c_nx_n^k \equiv N$ is soluble modulo p^ν for every prime p for every sufficiently large ν, since if this is not the case Lemma 2.9 fails and therefore so does Lemma 2.8, so that $\chi(p)$ can be 0 for some p. Choose $P_1, \ldots, P_n$ each sufficiently large and write

$$T_i(\alpha) = \sum_{x=1}^{P_i} e(c_i\alpha x^k)$$

and

$$U(\alpha) = \sum_{x_1=1}^{P_1} \sum_{x_2=1}^{P_2} \cdots \sum_{x_\ell=1}^{P_\ell} e(\alpha(c_1x_1^k + \cdots + c_\ell x_\ell^k)) \sum_{d|(x_1,\ldots,x_\ell)} \mu(d),$$

so that

$$U(\alpha) \prod_{i=\ell+1}^{n} T_i(\alpha) = \sum_{x=1}^{N} \varrho(x)e(\alpha x).$$

Taking the inverse Fourier transform as before we have

$$\varrho(N) = \int_0^1 e(-\alpha N)U(\alpha) \prod_{i=\ell+1}^{n} T_i(\alpha)\, d\alpha.$$

We again separate the integral into the contributions from the major and minor arcs. Let $S_{a,q}$ be as before, but now let

$$I_i(\beta) = \int_0^{P_i} e(c_i\beta\xi^k)\,d\xi$$

and

$$\sigma_{a,q} = \sum_{\substack{1\le z_1,\dots,z_\ell\le q\\ \gcd(z_1,\dots,z_\ell,q)=1}} e\left(\frac{a}{q}\left(c_1z_1^k+\cdots+c_\ell z_\ell^k\right)\right).$$

Then we can apply similar methods to those used in the proof of Lemma 2.1 to get estimates for the components of the integrand.

Lemma 2.12. *For α in $\mathfrak{M}_{a,q}$ we have:*
a) $T_i(\alpha) = q^{-1}S_{c_ia,q}I_i(\beta) + O(P^{2\delta})$
b) $U(\alpha) = \frac{1}{\zeta(\ell)}\frac{f(q)}{q}^{-\ell}\sigma_{a,q}\prod_{i=1}^{\ell} I_i(\beta) + O\left(\frac{1}{q}\min_i P_i\log\min_i P_i\prod_{\substack{1\le j\le\ell\\ P_j\ne\min_i P_i}} P_j^{\delta}\right)$.

Proof. The proof of a) is precisely as in Lemma 2.1. The proof of b) is also similar:

$$\begin{aligned}
U(\alpha) &= \sum_{1\le z_1,\dots,z_\ell\le q} e\left(\frac{a}{q}(c_1z_1^k+\cdots+c_\ell z_\ell^k)\right)\\
&\qquad\qquad \sum_{\substack{\forall i\le\ell: 1\le x_i\le P_i\\ x_i\equiv z_i \pmod q}} e(\beta(c_1x_1^k+\cdots+c_\ell x_\ell^k)) \sum_{d\mid(x_1,\dots,x_\ell)}\mu(d)\\
&= \sum_{\substack{1\le z_1,\dots,z_\ell\le q\\ (z_1,\dots,z_\ell,q)=1}} e\left(\frac{a}{q}(c_1z_1^k+\cdots+c_\ell z_\ell^k)\right)\\
&\qquad\qquad \sum_{\substack{\forall i\le\ell: 1\le x_i\le P_i\\ x_i\equiv z_i \pmod q}} e(\beta(c_1x_1^k+\cdots+c_\ell x_\ell^k)) \sum_{\substack{d\mid(x_1,\dots,x_\ell)\\ (d,q)=1}}\mu(d)\\
&= \sum_{\substack{1\le z_1,\dots,z_\ell\le q\\ (z_1,\dots,z_\ell,q)=1}} e\left(\frac{a}{q}(c_1z_1^k+\cdots+c_\ell z_\ell^k)\right) \sum_{\substack{1\le d\le\min(P_i)\\ (q,d)=1}}\mu(d)\prod_{i=1}^{\ell}\left(\frac{1}{qd}I_i(\beta)+O(P_i^{\delta})\right)\\
&= \frac{1}{\zeta(\ell)}\frac{f(q)}{q^\ell}\sigma_{a,q}\prod_{i=1}^{\ell} I_i(\beta) + O\left(\frac{1}{q}\min(P_i)\log\min(P_i)\prod_{\substack{1\le j\le\ell\\ P_j\ne\min(P_i)}} P_j^{\delta}\right).
\end{aligned}$$

□

Let

$$\mathfrak{S}(N,B) = \sum_{q=1}^{\infty}\frac{f(q)}{q^n}\sum_{\substack{1\le a\le q\\ \gcd(a,q)=1}}\sigma_{a,q}e\left(-\frac{a}{q}N\right)\prod_{i=\ell+1}^{n} S_{c_ia,q}$$

and $\mathfrak{S}(N) = \lim_{B\to\infty}\mathfrak{S}(N,B)$. Lemma 3.3 still holds, so combining the elements of Lemma 2.12 and applying it we get the following:

Theorem 2.13. *For $n \geq 2^k + \ell + 1$ we have*

$$\varrho(N) = \frac{1}{\zeta(\ell)} \frac{1}{|c_1 c_2 \cdots c_n|^{1/k}} \frac{\Gamma(1+1/k)^n}{\Gamma(n/k)} N^{n/k-1} \mathfrak{S}(N) + O(P^{n-k-\theta})$$

for some $\theta > 0$.

Proof. The result follows from Lemma 2.12 just as in the proofs of Lemma 2.2 and Theorem 2.4, setting each $P_i = \lfloor (N/c_i)^{1/k} \rfloor$, with the only major difference being that in the evaluation of the I_i due to the presence of the coefficient c_i a factor of $c_i^{-1/k}$ emerges from the change of variable in each integral. □

Remark. Lemmas 2.5, 2.6, 2.7, and 2.8 hold just as before. The condition in Lemma 2.8, analogous to Lemma 2.9, is the condition we assumed on the c_i, and in fact Theorem 7.3 of [2] shows that it is enough to have the c_i pairwise coprime. Therefore if the c_i are pairwise coprime or more generally if the congruence $c_1 x_1^k + \cdots + c_n x_n^k \equiv N$ is soluble for every N modulo p^ν for all primes p for all sufficiently large ν then Theorem 2.10 holds, and therefore so does Corollary 2.11.

3 Relatively prime values of polynomials

Given two relatively prime polynomials f and g in $\mathbb{Z}[x_1, \ldots, x_n]$ not both everywhere divisible by the same prime, we want to estimate the density $\delta(f, g)$ of points $x \in \mathbb{Z}^n$ such that $\gcd(f(x), g(x)) = 1$. Since $\delta(f, g)$ can trivially be as high as 1 we will focus on finding a lower bound. Our method will be to express the coprimality condition on $f(x)$ and $g(x)$ as a divisor sum involving the Mobius function. We can then express $\delta(f, g)$ in terms of the density of points x such that $f(x)$ and $g(x)$ are simultaneously divisible by d, which translates into the number of simultaneous zeros of f and g modulo d divided by d^n. Since this number is a multiplicative function of d we can factor the resulting Dirichlet series as a product over primes. Then since for f and g as stated there is no prime p such that f and g are both everywhere zero modulo p, in order to lower bound $\delta(f, g)$ it remains only to upper bound the number of simultaneous solutions of f and g modulo p. We do this by considering f and g as functions f_a and g_a of $n - 1$ variables with some parameter a and induct on n. The case in which f_a and g_a are both nonzero and relatively prime is covered by the inductive hypothesis, and we can show that there are sufficiently few values of a that are not covered to be able to use the crude bound in Lemma 3.1 below. Finally we can use the properties of resultants to establish the base case $n = 1$.

We denote by $\mathrm{Res}(f, g)$ the resultant of two nonzero univariate polynomials f and g, and by $\mathrm{Res}_{x_i}(f, g)$ the resultant of two nonzero multivariate polynomials f and g with respect to the variable x_i, with all other variables taken as parameters.

We first need the following basic fact about multivariable polynomials in finite fields:

Lemma 3.1. *Let $f \in \mathbb{F}_p[x_1, \ldots, x_n]$ for some prime p not be identically zero. Then f has at most $p^{n-1} \deg f$ zeros in $\mathbb{F}_p$.*

Proof. If we regard f as a univariate polynomial in one of the x_i and treat the other variables as parameters then the result follows immediately from the fundamental theorem of algebra. □

We will also need several well-known properties of resultants (both univariate and multivariate); see for example [4].

Finally, the following bounds are in terms of Chebyshev's first function

$$\vartheta(x) = \sum_{p \le x} \log p.$$

In order to get a purely analytic bound we can use the upper bound

$$\vartheta(x) \le x + \frac{0.15}{\log^3 x}$$

for all $x > 1$ from Theorem 2.4 of [1].

Theorem 3.2. *For any two polynomials f and g in n variables, let $\delta(f,g)$ be the limit as $B \to \infty$ of $(2B+1)^{-n}|\{x \in \{-B,\dots,B\}^n : (f(x),g(x)) = 1\}|$. Then if $\gcd(f,g) = 1$ and there is no prime that divides every value of both f and g, then*

$$\delta(f,g) \ge \exp\left(-n\vartheta(\sqrt{A}) - \left(\log\zeta(2) - P(2) + \frac{1}{\sqrt{A}}\right) A \log(2A)\right)$$

where $A = (n-1)T(f,g) = (n-1)(\deg f \deg g + \deg f + \deg g)\min(\deg f, \deg g)$ and $\vartheta(x)$ is Chebyshev's first function $\vartheta(x) = \sum_{p \le x} \log p$.

Proof. Write $v(f,g)$ for the number of shared zeros modulo a prime p for polynomials f, g in n variables and $f_a(x_1,\dots,x_n) = f(x_1,\dots,x_n,a)$, and similarly for g. Let $n = 2$. Then

$$v(f,g) = \sum_{a \in \mathbb{F}_q} v(f_a,g_a) = \sum_{\substack{a \in \mathbb{F}_q \\ f_a g_a \ne 0 \\ \deg\gcd(f_a,g_a)=0}} v(f_a,g_a) + \sum_{\substack{a \in \mathbb{F}_q \\ f_a g_a \ne 0 \\ \deg\gcd(f_a,g_a)>0}} v(f_a,g_a) + \sum_{\substack{a \in \mathbb{F}_q \\ f_a g_a = 0}} v(f_a,g_a).$$

Now since f_a and g_a are univariate we have that $v(f_a,g_a) > 0$ only if $\deg\gcd(f,g) > 0$, so the first sum is zero. The second sum is over a satisfying $\mathrm{Res}(f_a,g_a) = 0$, so since $\mathrm{Res}(f_a,g_a)$ is a polynomial in a there are at most $\deg \mathrm{Res}(f_a,g_a) \le \deg f \deg g$ zeros. Since $v(f_a,g_a) \le \deg f$, the second sum is at most $(\deg f)^2 \deg g$. For the third sum if say f_a is identically 0 then f must be divisible by $x_2 - a$, so there are at most $\deg f + \deg g$ such points a. Therefore $v(f,g) \le (\deg f \deg g + \deg f + \deg g)\min(\deg f, \deg g) = T(f,g)$.

Suppose that for some $n \ge 2$ we have $v(f,g) \le p^{n-2}(n-1)T(f,g)$ provided that neither f nor g is identically 0 modulo p and $\gcd(f,g)$ has degree 0, where $T(f,g)$ is as in the statement of the theorem. Then we want to show that for polynomials f, g in $n+1$ variables we have $v(f,g) \le p^{n-1}nT(f,g)$. As in the case with $n = 2$ write

$$v(f,g) = \sum_{a \in \mathbb{F}_q} v(f_a,g_a) = \sum_{\substack{a \in \mathbb{F}_q \\ f_a g_a \ne 0 \\ \deg\gcd(f_a,g_a)=0}} v(f_a,g_a) + \sum_{\substack{a \in \mathbb{F}_q \\ f_a g_a \ne 0 \\ \deg\gcd(f_a,g_a)>0}} v(f_a,g_a) + \sum_{\substack{a \in \mathbb{F}_q \\ f_a g_a = 0}} v(f_a,g_a).$$

We can upper bound the first sum by $p^{n-1}(n-1)T(f,g)$ by the inductive hypothesis. For the second sum we use a similar method as in the case $n = 2$. For any a satisfying the requirements we have for some $i \le n$ $\mathrm{Res}_{x_i}(f_a,g_a) = 0$ for any values of the other variables. Therefore $\mathrm{Res}_{x_i}(f,g)$ is divisible by $x_{n+1} - a$. Since f and g are coprime, $\mathrm{Res}_{x_i}(f,g)$ is not identically 0, so the number of a such that $\gcd(f_a,g_a)$ has positive degree must be at most $\max_i \deg_{x_{n+1}} \mathrm{Res}_{x_i}(f,g) \le$

$\deg f \deg g$. Now for any f_a, g_a we have $v(f_a, g_a) \le p^{n-1} \deg f$, so in total the second sum is at most $p^{n-1} \deg f \deg g \min(\deg f, \deg g)$. For the third sum, if say f_a is identically 0, then f must be divisible by $x_{n+1} - a$, so there are at most $\deg f + \deg g$ points a such that f_a or g_a is 0. Therefore in total we have $v(f,g) \le p^{n-1} n T(f,g)$. By induction for every $n \ge 2$ we have $v(f,g) \le p^{n-2}(n-1)T(f,g)$.

Now we can write $\delta(f,g)$ as

$$\mathop{\mathbb{E}}_{x \in \mathbb{Z}^n} \sum_{d \mid \gcd(f(x), g(x))} \mu(d) = \sum_{d=1}^{\infty} \mu(d) \mathop{\mathbb{E}}_{x \in \mathbb{Z}^n} [d \mid \gcd(f(x), g(x))] = \sum_{d=1}^{\infty} \frac{\mu(d)\nu(d)}{d^n} = \prod_p \left(1 - \frac{\nu(p)}{p^n}\right)$$

where $\nu(x)$ is $v(f,g)$ for modulus x not necessarily prime and $[\,\cdot\,]$ is Iverson bracket notation. Therefore since for coprime f and g we have $\nu(p) < p^n$ for every p and $\nu(p) \le p^{n-2}(n-1)T(f,g)$ it follows that the product is at least

$$\left(\prod_{p \le \sqrt{(n-1)T(f,g)}} p^{-n} \right) \left(\prod_{\sqrt{p > (n-1)T(f,g)}} \left(1 - \frac{(n-1)T(f,g)}{p^2}\right) \right).$$

We can rewrite this as

$$\exp\left(-n\vartheta(\sqrt{A})\right) \prod_{p > \sqrt{A}} \prod_{k=1}^{A} \left(1 - \frac{1}{p^2 - k + 1}\right)$$

where the second product is factored repeatedly until the numerator of the fraction $\frac{a}{p^2}$ is 1. Now for a fixed $k < A$ we have $\left(1 - \frac{1}{p^2-k+1}\right) \ge \left(1 - \frac{1}{p^2}\right)^{c_k}$ for $p > \sqrt{A}$ if $c_k \ge \frac{\log(1 - \frac{1}{A-k+1})}{\log(1-\frac{1}{A})}$ and for $k = A$ $\left(1 - \frac{1}{p^2-k+1}\right)$ is at least $\frac{1}{2}$ so we need $c_k \ge -\frac{\log 2}{\log(1-\frac{1}{A})}$, so

$$\begin{aligned}
\delta(f,g) &\ge \exp\left(-n\vartheta(\sqrt{A})\right) \prod_{k=1}^{A} \prod_{p > \sqrt{A}} \left(1 - \frac{1}{p^2}\right)^{c_k} \\
&= \exp\left(-n\vartheta(\sqrt{A})\right) \prod_{k=1}^{A} \zeta(2)^{-c_k} \prod_{p \le \sqrt{A}} \left(1 - \frac{1}{p^2}\right)^{-c_k} \\
&= \exp\left(-n\vartheta(\sqrt{A})\right) \prod_{k=1}^{A} \zeta(2)^{-c_k} \exp\left(-c_k \sum_{p \le \sqrt{A}} \log\left(1 - \frac{1}{p^2}\right)\right) \\
&\ge \exp\left(-n\vartheta(\sqrt{A})\right) \prod_{k=1}^{A} \zeta(2)^{-c_k} \exp\left(c_k \sum_{p \le \sqrt{A}} \frac{1}{p^2}\right) \\
&\ge \exp\left(-n\vartheta(\sqrt{A})\right) \prod_{k=1}^{A} \zeta(2)^{-c_k} \exp\left(c_k \left(P(2) - \sum_{j > \sqrt{A}} \frac{1}{j^2}\right)\right) \\
&\ge \exp\left(-n\vartheta(\sqrt{A}) + \sum_{k=1}^{A} c_k \left(P(2) - \log\zeta(2) - \frac{1}{\sqrt{A}}\right)\right)
\end{aligned}$$

where $P(2)$ is the prime zeta function $\sum_p \frac{1}{p^s}$ evaluated at $s = 2$. Now

$$\begin{aligned}\sum_{k=1}^{A} c_k &= -\frac{\log 2}{\log(1-\frac{1}{A})} + \sum_{k=2}^{A} \frac{\log(1-\frac{1}{k})}{\log(1-\frac{1}{A})} \\ &\leq A\left(\log 2 - \sum_{k=2}^{A} \log\left(1-\frac{1}{k}\right)\right) \\ &= A\left(\log 2 + \sum_{k=2}^{A} (\log k - \log(k-1))\right) \\ &= A\log(2A).\end{aligned}$$

Therefore

$$\delta(f,g) \geq \exp\left(-n\vartheta(\sqrt{A}) - \left(\log\zeta(2) - P(2) + \frac{1}{\sqrt{A}}\right) A\log(2A)\right)$$

as desired. □

We can generalize the above theorem as follows. Let $\mathrm{Res}(f) = \mathrm{Res}(f_1, \ldots, f_n)$ denote the multivariate or Macaulay resultant of n homogenous polynomials in n variables.

Theorem 3.3. *For any m polynomials $f_1, f_2, \ldots, f_m$ in n variables, let $\delta(f)$ be the limit as $B \to \infty$ of $(2B+1)^{-n}|\{x \in \{-B, \ldots, B\}^n : (f_1(x), \ldots, f_m(x)) = 1\}|$. Then if $\gcd(f_1, \ldots, f_m) = 1$ and there is no prime that divides every value of every polynomial, then*

$$\delta(f) \geq \exp\left(-n\vartheta(\sqrt{A}) - \left(\log\zeta(2) - P(2) + \frac{1}{\sqrt{A}}\right) A\log(2A)\right)$$

where $A = (n-1)T(f,g) = (n-1)\left(\prod_i \deg f_i + \sum_i f_i\right)\min_i \deg f_i$.

Proof. First let $n = m-1$. Write $\tilde{f}_i$ for the homogenous polynomial in m variables $x_1, \ldots, x_{m-1}, u$ such that setting $u = 1$ we recover f_i. Then the Macaulay resultant $\mathrm{Res}(\tilde{f}_1, \ldots, \tilde{f}_m)$ is divisible by p if there exists a common zero of $\tilde{f}_1, \ldots, \tilde{f}_m$ in $\mathbb{F}_p$. Therefore the number $v(f)$ of common zeros of $f_1, \ldots, f_m$ in $\mathbb{F}_p$ is zero unless $\mathrm{Res}(\tilde{f}_1, \ldots, \tilde{f}_m)$ is divisible by p. Since for coprime $f_1, \ldots, f_m$ $v(f) < p^m$, $v(f) < p^{m-1}\min_i \deg f_i$ and the resultant is 0 in $\mathbb{F}_p$ for only finitely many p, it follows that

$$\delta(f) = \prod_{p \mid\mid \mathrm{Res}(\tilde{f}_1, \ldots, \tilde{f}_m)|} \left(1 - \frac{\nu(p)}{p^{m-1}}\right)$$

as in the proof of Theorem 3.2 is lower bounded by a function as described in the statement of the theorem. This also suffices to prove the case $n < m-1$, since the number of zeros can be upper bounded by permitting additional variables.

Now let $n = m$. Then

$$v(f) = \sum_{a \in \mathbb{F}_p} v(f_a) = \sum_{\substack{a \in \mathbb{F}_p \\ \deg \gcd(f_{1a}, \ldots, f_{ma}) = 0 \\ \prod_i f_{ia} \neq 0}} v(f_a) + \sum_{\substack{a \in \mathbb{F}_p \\ \gcd(f_{1a}, \ldots, f_{ma}) > 0 \\ \prod_i f_{ia} \neq 0}} v(f_a) + \sum_{\substack{a \in \mathbb{F}_p \\ \prod_i f_{ia} = 0}} v(f_a)$$

using the notation from above. In the first sum for all a such that the conditions hold $v(f_a) = 0$ by the preceding paragraph, so the first sum is 0. If the conditions of the second sum hold then $\mathrm{Res}(\tilde{f}_{1_a}, \ldots, \tilde{f}_{m_a}) = 0$, so taking this as a polynomial in a of degree at most $\prod_i \deg f_i$ there are at most $\prod_i \deg f_i$ solutions for a. For the third sum in order for $\prod_i f_{i_a}$ be be identically 0 the product $\prod_i f_i$ must be divisible by $x_n - a$, so there are at most $\deg \prod_i f_i = \sum_i \deg f_i$ solutions for a. Therefore using the generic bound for v we have $v(f) \leq p^{m-2}T(f)$ where $T(f) = (\prod_i \deg f_i + \sum_i \deg f_i) \min_i \deg f_i$.

Now for any $n > m$ suppose that for m polynomials f_i in n variables we have $v(f) \leq p^{n-2}(n - m + 1)T(f)$. Then in $n + 1$ variables we have

$$v(f) = \sum_{\substack{a \in \mathbb{F}_p \\ \deg \gcd(f_{1_a}, \ldots, f_{m_a}) = 0 \\ \prod_i f_{i_a} \neq 0}} v(f_a) + \sum_{\substack{a \in \mathbb{F}_p \\ \gcd(f_{1_a}, \ldots, f_{m_a}) > 0 \\ \prod_i f_{i_a} \neq 0}} v(f_a) + \sum_{\substack{a \in \mathbb{F}_p \\ \prod_i f_{i_a} = 0}} v(f_a)$$

as above. Using the same methods as previously we get a bound of $p^{n-1}T$ for the latter two sums and using the inductive hypothesis we get a bound of $p^{n-1}(n - m + 1)T(f)$ for the second sum. Therefore we have $v(f) \leq p^{n-1}(n - m + 2)T(f)$, and so by induction for every $n \geq m$ we have $v(f) \leq p^{n-2}(n - m + 1)T(f)$. Writing

$$\delta(f) = \prod_p \left(1 - \frac{\nu(p)}{p^n}\right)$$

and noting that for f as in the statement of the theorem we have $\nu(p) < p^n$ for every p the result follows as in the proof of Theorem 3.2. □

Remark. It is interesting to note that although the bounds obtained in the proof of Theorem 3.2 are nearly as strong as we would expect from the heuristic that the zeros of each polynomial are distributed randomly and independently over $\mathbb{F}_p^n$ for every prime p, those used in the proof of Theorem 3.3 are no stronger, even though we would expect something of the order $v(f) = O(p^{n-m}A)$ for some $A = A(f)$, analogous to the Lang-Weil bounds under an intuitive expectation of the dimension of the variety. The greatest effect of such bounds on the lower bound of $\delta(f)$ would be to improve the argument of ϑ from $A^{1/2}$ to $A^{1/m}$, but they would also improve the constant in the lower-order term of the bound to $\log \zeta(m) - P(m)$ in place of $\log \zeta(2) - P(2)$. The main difficulty in proving these bounds lies in attacking the third sum over a such that some f_{i_a} is identically 0, and we could restrict our attention to polynomials such that for all a such that this is the case $v(f_a)$ is small and improve the lower bound for these; investigation in this direction may be the subject of future work.

References

[1] Axler, Christian. "New estimates for some prime functions." arXiv:1703.08032.

[2] Davenport, Harold. *Analytic Methods for Diophantine Equations and Diophantine Inequalities.* Edited by Tim Browning, Cambridge University Press, 2005.

[3] Ekedahl, Torsten. "An infinite version of the Chinese remainder theorem." Commentarii Mathematici Universitatis Sancti Pauli. Vol. 40, 53–59. Rikkyo University, 1991.

[4] Sturmfels, Bernd. “Introduction to resultants.” Proceedings of Symposia in Applied Mathematics. Vol. 53. American Mathematical Society, 1998.