ALMOST PRIME SOLUTIONS TO DIOPHANTINE SYSTEMS OF HIGH RANK

ÁKOS MAGYAR AND TATCHAI TITICHETRAKUN

Abstract. Let $\mathcal{F}$ be a family of r integral forms of degree k in n variables $\mathbf{x} = (x_1, ..., x_n)$. We study the number of solutions $\mathbf{x} \in [1, N]^n$ to the diophantine system $\mathcal{F}(\mathbf{x}) = \mathbf{v}$ under the restriction that each of the x_i's has a bounded number of prime factors depending only on the parameters n, k and r. We show that the system $\mathcal{F}$ have the expected number of almost prime solutions under the same conditions as was established for integer solutions by Birch.

1. Introduction.

In general, proving the existence of solutions to a diophantine system has an integer solution is impossible, however the problem becomes much more feasible assuming that the system is sufficiently large with respect to certain notions of rank, or have high degree of symmetry. Indeed, it was shown by Birch [3] and later extended by Schmidt [22], that local to global type asymptotic formulas can be attained for homogeneous equations whose rank is exponentially large with respect to its degree, using the classical Hardy-Littlewood method of exponential sums.

It is natural expect that similar results should hold when the solutions are restricted to special sequences such as the primes or almost primes. For diagonal systems this has been done by Hua [16], who, extending the methods of Vinogradov [26], derived asymptotics for the number of solutions consisting of primes. For diagonal quadratic and cubic equations various further refinements were obtained [27], [17], [5] considering both prime and almost prime solutions combining the circle and sieve methods.

However it was shown only recently [6] that local to global type principles hold for the number of prime solutions for any diophantine system whose rank is sufficiently large with respect to the degree and number of equations. The methods there employed certain ideas from arithmetic combinatorics, a process of regularizing the system, leading to exceedingly strong, i.e. tower-exponential type, conditions on the rank. It is expected that such results should hold under similar rank conditions as was established for the existence of integer solutions. The aim of the present article is to show this when the primes are replaced by the almost primes, i.e. numbers with a bounded number of prime factors. This might also serve as a step toward a different approach to count prime solutions at least for translation invariant systems, considering the primes as a dense subset of the almost primes. Solutions to translation invariant systems in dense subsets of integers have been established recently in [15], [18], [19].

In another direction, the existence of almost prime solutions to the system $\mathcal{F}(\mathbf{x}) = \mathbf{v}$ were proved by Bourgain, Gamburd and Sarnak [2], provided the system of forms $\mathcal{F}$ preserved by sufficiently large group of linear transformations $\Gamma \subseteq GL_n(\mathbb{Z})$. Their results are very strong in the sense that they do not require the largeness of the rank of the system however, apart from quadratic forms, examples of systems exhibiting such high degree of symmetry are quite rare.

1991 Mathematics Subject Classification. 11D72, 11P32.
The second author is supported by NSERC grant 22R44824 and ERC-AdG. 321104.

To state our main results let $\mathcal{F} = (F_1, \ldots, F_r)$ be a family of homogeneous polynomials of degree k in the variables $\mathbf{x} = (x_1, \ldots, x_n)$. For $0 < \varepsilon < 1$ and $N \geq 1$ let $\mathbf{P}_N^\varepsilon$ denote set of natural numbers $m \leq N$ such that each prime divisor of m is at least N^ε. Note that each $m \in \mathbf{P}_N^\varepsilon$ at most $l = [1/\varepsilon]$ prime factors. For given $\mathbf{v} \in \mathbb{Z}^n$ let

$$\mathcal{M}_{\mathcal{F}}^\varepsilon(N) := |\{\mathbf{x} \in (\mathbf{P}_N^\varepsilon)^n;\ \mathcal{F}(\mathbf{x}) = \mathbf{v}\},$$

that is the number of almost prime solutions $x \in [1, N]^n$ to the system $\mathcal{F}(\mathbf{x}) = \mathbf{v}$. For a fixed prime p define the local density

$$\sigma_p^*(\mathbf{v}) := \lim_{t \to \infty} \frac{(p^t)^r M(p^t, \mathbf{v})}{\phi^n(p^t)}, \tag{1.1}$$

provided the limit exists, where $M(p^t, \mathbf{v})$ represents the number of solutions to the equation $\mathcal{F}(\mathbf{x}) = \mathbf{v}$ in the multiplicative group of reduced residue classes $mod\, p^t$, denoted by $U_{p^t}^n$, and ϕ is Euler's totient function. As almost primes are concentrated in reduced residue classes the general local to global principle suggests that

$$\mathcal{M}_{\mathcal{F}}^\varepsilon(N) \approx_\varepsilon N^{n-kr} \,(log\, N)^{-n} J(N^{-k}\mathbf{v}) \prod_p \sigma_p^*(\mathbf{v}) =: N^{n-kr} \,(log\, N)^{-n} \mathfrak{S}^*(N, \mathbf{v}), \tag{1.2}$$

as $N \to \infty$, where $J(\mathbf{u})$ is the so-called singular integral representing the density of real solutions $\mathbf{x} \in [0, 1]^n$ to $\mathcal{F}(\mathbf{x}) = \mathbf{u}$, see [3],[22].

Following [3], define the rank of the system, $Rank(\mathcal{F})$ as the codimension of the singular variety $V_{\mathcal{F}}^* \subseteq \mathbb{C}^n$, consisting of points $\mathbf{z} \in \mathbb{C}^n$ where the Jacobian $\partial\mathcal{F}/\partial\mathbf{z}$ drops rank. Note that for a single quadratic form $F(\mathbf{x}) = Ax \cdot x$ this agrees with the rank of the underlying matrix A. Our main result is the following.

Theorem 1.1. *Let $\mathcal{F} = (F_1, \ldots, F_r)$ be a system of r integral forms of degree k in n such that*

$$Rank(\mathcal{F}) > r(r + 1)(k - 1)2^{k-1}. \tag{1.3}$$

Then there exists a constant $\varepsilon = \varepsilon(k, r) > 0$ such that

$$\mathcal{M}_{\mathcal{F}}^\varepsilon(N) \geq c_{n,k,r}\ N^{n-kr} \,(log\, N)^{-n} \mathfrak{S}^*(N, \mathbf{v}), \tag{1.4}$$

for some constant $c_{n,k,r} > 0$. In particular one may take $\varepsilon = (64\, n^{3/2} r^2 (r + 1)(r + 2)k(k + 1))^{-1}$.

Moreover if the equation $\mathcal{F}(\mathbf{x}) = \mathbf{v}$ has a nonsingular solution in $\mathbb{U}_p$, the p-adic integer units for all primes p, and if it has a nonsingular real solution in the cube $[\delta, 1 - \delta]^n$, then

$$\mathfrak{S}^*(N, \mathbf{v}) = J(N^{-k}\mathbf{v}) \prod_p \sigma_p^*(\mathbf{v}) \geq c(\delta) > 0. \tag{1.5}$$

The validity of (1.5) follows from the fact that $J(\mathbf{u}) \geq c(\delta) > 0$ provided that the equation $\mathcal{F}(\mathbf{x}) = \mathbf{u}$ has a nonsingular real point in the cube $[\delta, 1-\delta]^n$, see [22], Sec.9 and [3], Sec.6. Thus the conditions on the existence of almost prime solutions are essentially the same as those of for integer solutions, the only difference being the natural requirement to have local solutions among the p-adic units.

The key to prove Theorem 1.1 is to study a weighted sum over the solutions with weights that are concentrated on numbers having few prime factors. Such weights have been defined by Goldston, Pintz and Yildirim [10] in their seminal work on gaps between the primes. For given $0 < \eta < 1$, let $R := N^\eta$ and define

$$\Lambda_R(m) := \sum_{d|m} \mu(d)\, f(\frac{log\, d}{log\, R}), \tag{1.6}$$

where μ is the Möbius function. We will eventually choose $f(x) = (1-x)_+^{4n}$ and follow the Fourier analytic approach in [24] as opposed to the contour integration method of [10]. Using the so-called "W-trick" introduced by Green and Tao in [12] to bypass the contribution of small primes, let $\omega = \omega_{\mathcal{F}}$ be a fixed positive integer depending only on the system $\mathcal{F}$ and let $W := \prod_{p\leq\omega} p$, the product of primes up to ω. Note that if $\mathbf{x} \in (\mathbf{P}_N^{\varepsilon})^n$ and $p|x_i$ implies $p \geq N^{\varepsilon} > \omega$ for sufficiently large N, hence $(x_i, W) = 1$ for each $1 \leq i \leq n$. We will write $(\mathbf{x}, W) = 1$ in this case. Under the conditions of Theorem 1.1 our key estimates will be

Theorem 1.2. *Let $\mathcal{F} = (F_1, \ldots, F_r)$ be a system of r integral forms of degree k in n variables satisfying the rank condition* (1.3)*. Then there exists $\eta = \eta(r,k) > 0$ such that for $R \leq N^{\eta}$*

$$\sum_{\substack{\mathbf{x}\in[N]^n\\ (\mathbf{x},W)=1,\ \mathcal{F}(\mathbf{x})=\mathbf{v}}} \Lambda_R^2(x_1x_2\cdots x_n) = \ c_n(f)\, N^{n-rk}(log\, R)^{-n}\mathfrak{S}^*(N,\mathbf{v})\,(1+o_{\omega\to\infty}(1)), \tag{1.7}$$

where

$$c_n(f) = \int_0^{\infty} f^{(n)}(x)^2\, \frac{x^{n-1}}{(n-1)!}\, dx, \text{ and one may take } \ \eta(r,k) = \frac{1}{8r^2(r+1)(r+2)k(k+1)}.$$

In addition, for given $0 < \varepsilon < \eta \leq \eta(r,k)$,

$$\sum_{\substack{\mathbf{x}\in[N]^n\backslash(\mathbf{P}^{\varepsilon}(N))^n\\ (x,W)=1, \mathcal{F}(\mathbf{x})=\mathbf{v}}} \Lambda_R^2(x_1x_2\cdots x_n) \leq\ c'_{n+1}(f)\left(\frac{\varepsilon}{\eta}\right)^2\ N^{n-rk}(log\, R)^{-n}\mathfrak{S}^*(N,\mathbf{v})\,(1+o_{\omega\to\infty}(1)), \tag{1.8}$$

with

$$c'_{n+1}(f) = 2n\int_0^{\infty} f^{(n+1)}(x)^2\, \frac{x^{n-1}}{(n-1)!}\, dx.$$

In the proof of Theorem 1.2 we'll use the asymptotic for the number of integer solutions $\mathbf{x} \in [N]^n$ to $\mathcal{F}(\mathbf{x}) = \mathbf{v}$ subject to the congruence condition $\mathbf{x} \equiv \mathbf{s}$ $(mod\ D)$, where D is a modulus bounded by a sufficiently small power N. This follows in a straightforward manner from the Birch-Davenport variant of the circle method described in [3] and is summarized in

Proposition 1.1. *Let $\mathcal{F} = (F_1, \ldots, F_r)$ be a family of integral forms of degree k satisfying the rank condition* (1.3)*, and For given $D \in \mathbb{N}$ and $\mathbf{s} \in \mathbb{Z}^n$ let*

$$\mathcal{R}_N(D,\mathbf{s};\mathbf{v}) := |\{\mathbf{x}\in[N]^n;\ \mathbf{x}\equiv\mathbf{s}\ (mod\ D),\ \mathcal{F}(\mathbf{x})=\mathbf{v}\}|. \tag{1.9}$$

Then there exists a constant $\delta' = \delta'(k,r) > 0$ such that the following holds.

(i) If $0 < \eta \leq \eta(r,k) := \frac{1}{4r^2(r+1)(r+2)k^2}$ then for every $1 \leq D \leq N^{\frac{\eta}{1+\eta}}$ and $\mathbf{s} \in \mathbb{Z}^n$ one has the asymptotic

$$\mathcal{R}_N(D,\mathbf{s};\mathbf{v}) = N^{n-rk}D^{-n}\, J(N^{-k}\mathbf{v}) \prod_p \sigma_p(D,\mathbf{s},\mathbf{v}) + O(N^{n-rk-\delta'}D^{-n}). \tag{1.10}$$

(ii) Moreover if

$$Rank\,(\mathcal{F}) > (r(r+1)(k-1)+rk)2^k \tag{1.11}$$

then the asymptotic formula (1.10) *holds for* $\eta \leq \frac{1}{4r(r+2)k}$.

Here $\sigma_p(D, \mathbf{s}, \mathbf{v})$ represents the density of the solutions among the p-adic numbers, more precisely

$$\sigma_p(D, \mathbf{s}, \mathbf{v}) = \lim_{l \to \infty} \sigma_p^l(D, \mathbf{s}, \mathbf{v}), \quad \sigma_p^l(D, \mathbf{s}, \mathbf{v}) = p^{-l(n-r)} |\{\mathbf{x} \in \mathbb{Z}_{p^l}^n;\ \mathcal{F}(D\mathbf{x} + \mathbf{s}) \equiv \mathbf{v}\ (mod\ p^l)\}|. \tag{1.12}$$

The product form of the main term in (1.10) will allow as to write the expressions on the left side of (1.7) and (1.8) as an integral over an Euler product, which can be asymptotically evaluated using the sieve methods. To understand the local factors of The Euler product one needs to analyze the number of solutions to the system $\mathcal{F}(\mathbf{x}) = \mathbf{v}$ mod p, this has been done it [7] based on adapting Birch's method to finite fields. Here the W-trick is quite useful as one has to consider sufficiently large primes for which the rank of the *mod* p - reduced variety $V_{\mathcal{F}} = \{\mathcal{F}(\mathbf{x}) = \mathbf{v}\}$ remains sufficiently large.

The information needed about the Euler factors

$$\gamma_p(\mathbf{v}) := \frac{P^{-n}}{\sigma_p(\mathbf{v})} \sum_{\substack{\mathbf{s} \in \mathbb{Z}_p^n, \\ \mathcal{F}(s) \equiv \mathbf{v}\ (mod\ p)}} \mathbf{1}_{p | s_1 \cdots s_n}\, \sigma_p(p, \mathbf{s}, \mathbf{v}), \tag{1.13}$$

is summarized in

Proposition 1.2. *Let* $\mathcal{F}$ *be a family of* r *integral forms of degree* k. *If* $rank(\mathcal{F}) > r(r+1)(k-1)2^k$ *then for all sufficiently large primes* $p > \omega_{\mathcal{F}}$ *one has*

$$\gamma_p(\mathbf{v}) = \frac{n}{p} + O(p^{-2}). \tag{1.14}$$

1.1. **Outline and Notations.** The facts about the number of solutions to diophantine systems among integers in a given residue class with respect to a small modulus will be given in Section 4 and will be used throughout the paper. The arguments are straightforward generalizations of those of Birch discussed in [3]. In Section 3 we carry out the analysis of certain local factors attached the primes, and prove Proposition 1.2. Here we rely on certain results obtained in [7] on the number of solutions of diophantine systems over finite fields, and some well-known facts in algebraic geometry [8], [23] about the size and the stability of the dimension of homogeneous algebraic sets when reduced *mod* p . Somewhat unusually, we will prove our main results in Section 2, using the results of Section 3 and Section 4. This is to separate our main arguments relying on the sieve of Goldston-Pintz-Yildirim [10], from those to count integer solutions of diophantine systems based on the Hardy-Littlewood method of exponential sums.

The symbols $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ denote the integers, the rational numbers, the real numbers, and the complex numbers, respectively. We write $\mathbb{Z}_N$ for the group $\mathbb{Z}/N\mathbb{Z}$ as well as Z_N^* for the multiplicative group reduced residue classes (*mod* N). If X is a set then $\mathbf{1}_X$ denotes a characteristic function for X in a specified ambient space, and on occasion, the set X is replaced by a conditional statement which defines it. The Landau o and O notation is used throughout the work. The notation $f \lesssim g$ is sometimes used to replace $f = O(g)$, we will assume that the parameters n, k and r and usually do not denote the dependence on them. If the implicit constants depend on further parameters $m, l, \varepsilon, \delta, \ldots$ we indicate them as a subscript, thus we'll write $f \lesssim_{m,l,\varepsilon,\delta\ldots} g$, $f = O_{k,\varepsilon,\delta\ldots}(g)$ e.t.c. By $o_{\omega\to\infty}(1)$ we denote a quantity that tends to 0 as $\omega \to \infty$, and note that this implies also that $N \to \infty$ as well always assume that N is sufficiently large with respect to ω.

2. Proof of the main results.

In this section we introduce the Euler product representation of the weighted sums over the solutions defined in (1.7) and (1.8), and prove Theorems 1.1 and 1.2 using the main results of Section 3 and Section 4.

Let ϕ_N be the indictor function of the cube $[1,N]^n$, μ the Möbius function and write $\sum'$ for sums restricted to square-free numbers. We'll also use the customary notations $[a,b]$ and (a,b) for the least common multiple and greatest common factor of the numbers a and b. If $\mathbf{b}=(b_1,\ldots,b_n)\in\mathbb{Z}^n$ is such that $(b_i,W)=1$ for all $1\le i\le n$, then we write $(\mathbf{b},W)=1$. We write $a|b$ If a divides b and $\mathbf{1}_{a|b}$ for the indicator function of this relation. We start by making a few immediate observations about the local factors $\sigma_p(D,\mathbf{s},\mathbf{v})$ defined in (1.12).

Lemma 2.1. *Let D, W be square free numbers such that $(D,W)=1$ and let p be a prime. If $(p,DW)=1$ then*

$$\sigma_p(DW,\mathbf{t},\mathbf{v})=\sigma_p(\mathbf{v}). \tag{2.1}$$

If $p|D$ and $\mathbf{t}\equiv\mathbf{s}$ (mod D) then one has

$$\sigma_p(DW,\mathbf{t},\mathbf{v})=\sigma_p(p,\mathbf{t},\mathbf{v})=\sigma_p(p,\mathbf{s},\mathbf{v}). \tag{2.2}$$

Similarly, if $p|W$ and $\mathbf{t}\equiv\mathbf{b}$ (mod W) then

$$\sigma_p(DW,\mathbf{t},\mathbf{v})=\sigma_p(p,\mathbf{t},\mathbf{v})=\sigma_p(p,\mathbf{b},\mathbf{v}). \tag{2.3}$$

Proof. To see (2.1) note that for any $l\in\mathbb{N}$ the transformation $\mathbf{x}\to DW\mathbf{x}+\mathbf{t}$ is one-one and onto on $\mathbb{Z}^n_{p^l}$. If $p|D$ then $D=pD'$ with $(p,D'W)=1$, and one may write $DW\mathbf{x}+\mathbf{t}=p(D'W\mathbf{x})+\mathbf{t}$ and the first equality in (2.2) follows by making a change of variables $\mathbf{y}:=D'W\mathbf{x}$ on $\mathbb{Z}^n_{p^l}$. Also $p\mathbf{y}+\mathbf{t}=p(\mathbf{y}+\mathbf{u})+\mathbf{s}$ and the second equality follows by replacing $\mathbf{y}$ with $\mathbf{y}+\mathbf{u}$. Interchanging the role of D and W (2.3) follows. $\square$

Let $\mathcal{F}=(F_1,\ldots,F_r)$ be system of integral forms satisfying the rank condition (1.3), $R:=N^{\frac{\eta}{2(1+\eta)}}$, with $\eta=\eta(r,k)$ as defined in (1.10). Let $W=\prod_{p\le\omega}p$ for a sufficiently large constant $\omega=\omega_{\mathcal{F}}$, let $(\mathbf{b},W)=1$ and define the sum:

$$S_{W,\mathbf{b}}(N):=\sum_{\substack{\mathbf{x}\equiv\mathbf{b}\ (mod\ W)\\ \mathcal{F}(\mathbf{x})=\mathbf{v}}}\Lambda_R^2(x_1x_2\cdots x_n)\,\phi_N(\mathbf{x}), \tag{2.4}$$

and for $\omega<q$, q prime

$$S_{W,q,\mathbf{b}}(N):=\sum_{\substack{\mathbf{x}\equiv\mathbf{b}\ (mod\ W)\\ \mathcal{F}(\mathbf{x})=\mathbf{v}}}\mathbf{1}_{q|x_1\ldots x_n}\ \Lambda_R^2(x_1x_2\cdots x_n)\,\phi_N(\mathbf{x}). \tag{2.5}$$

Lemma 2.2. *We have*

$$S_{W,\mathbf{b}}(N)=N^{n-dr}J(N^{-d}\mathbf{v})W^{-n}\mathfrak{S}_{W,\mathbf{b}}(\mathbf{v})\sideset{}{'}\sum_{(D,W)=1}h_D(R)\,\gamma_D(\mathbf{v})\ +O(N^{n-rk-\delta}), \tag{2.6}$$

and similarly

$$S_{W,q,\mathbf{b}}(N)=N^{n-dr}J(N^{-d}\mathbf{v})W^{-n}\mathfrak{S}_{W,\mathbf{b}}(\mathbf{v})\sideset{}{'}\sum_{(D,W)=1}h_D(R)\,\gamma_{[D,q]}(\mathbf{v})\ +O(N^{n-rk-\delta}), \tag{2.7}$$

where

$$\mathfrak{S}_{W,\mathbf{b}}(\mathbf{v}):=\prod_{p|W}\sigma_p(p,\mathbf{b},\mathbf{v})\prod_{p\nmid W}\sigma_p(\mathbf{v}), \tag{2.8}$$

$$\gamma_D(\mathbf{v}) := D^{-n} \sum_{\substack{\mathbf{s}\in\mathbb{Z}_D^n \\ \mathcal{F}(\mathbf{s})\equiv\mathbf{v}\ (mod\ D)}} \mathbf{1}_{D|s_1\cdots s_n} \prod_{p|D} \frac{\sigma_p(p,\mathbf{s},\mathbf{v})}{\sigma_p(\mathbf{v})}, \tag{2.9}$$

and

$$h_D(R) := \sum_{[d_1,d_2]=D} \mu(d_1)\mu(d_2)\, f(\frac{\log\, d_1}{\log\, R})\, f(\frac{\log\, d_2}{\log\, R}). \tag{2.10}$$

Proof. By definition (1.6)

$$\begin{aligned} S_{W,\mathbf{b}}(N) &= \sum_{\substack{\mathbf{x}\equiv\mathbf{b}\ (mod\ W) \\ \mathcal{F}(\mathbf{x})=\mathbf{v}}} \phi_N(\mathbf{x}) \sum_{[d_1,d_2]|x_1\cdots x_n}{}' \mu(d_1)\mu(d_2)\, f(\frac{\log\, d_1}{\log\, R})\, f(\frac{\log\, d_2}{\log\, R}) \\ &= \sum_D{}' \sum_{[d_1,d_2]=D} \mu(d_1)\mu(d_2)\, f(\frac{\log\, d_1}{\log\, R})\, f(\frac{\log\, d_2}{\log\, R}) \sum_{\substack{\mathbf{x}\equiv\mathbf{b}\ (mod\ W) \\ \mathcal{F}(\mathbf{x})=\mathbf{v}}} \mathbf{1}_{D|x_1\cdots x_n}\phi_N(\mathbf{x}) \end{aligned} \tag{2.11}$$

The inner sum in $\mathbf{x}$ on last line of equation (2.11) is zero unless $(D,W)=1$ which we will assume from now on. Indeed if there is a prime p such that $p|D$ and $p|W$, then $p|x_i$ for some $1\leq i\leq n$ and hence $b_i\equiv x_i\equiv 0\ (mod\ p)$ contradicting our assumption $(b_i,W)=1$. The conditions $D|x_1\cdots x_n$ and $\mathbf{x}\equiv\mathbf{b}\ (mod\ W)$ depend only on $\mathbf{x}\ (mod\ DW)$, thus one may write

$$\sum_{\substack{\mathbf{x}\equiv\mathbf{b}\ (mod\ W) \\ \mathcal{F}(\mathbf{x})=\mathbf{v}}} \mathbf{1}_{D|x_1\cdots x_n}\phi_n(\mathbf{x}) = \sum_{\substack{\mathbf{t}\in\mathbb{Z}_{DW}^n,\ \mathbf{t}\equiv\mathbf{b}\ (mod\ W) \\ \mathcal{F}(\mathbf{t})\equiv\mathbf{v}\ (mod\ DW)}} \mathbf{1}_{D|t_1\cdots t_n} \sum_{\substack{\mathbf{x}\equiv\mathbf{t}\ (mod\ DW) \\ \mathcal{F}(\mathbf{x})=\mathbf{v}}} \phi_N(\mathbf{x}). \tag{2.12}$$

Since $D\leq R^2\leq N^{\frac{\eta}{1+\eta}}$; by Proposition 1.1 this further equals to

$$\sum_{\substack{\mathbf{t}\in\mathbb{Z}_{DW}^n,\ \mathbf{t}\equiv\mathbf{b}\ (mod\ W) \\ \mathcal{F}(\mathbf{t})\equiv\mathbf{v}\ (mod\ DW)}} \mathbf{1}_{D|t_1\cdots t_n} \left(N^{n-kr}(DW)^{-n} J(N^{-k}\mathbf{v}) \prod_p \sigma_p(DW,\mathbf{t},\mathbf{v})\ +\ O(N^{n-kr-\delta'}D^{-n}) \right). \tag{2.13}$$

To estimate the contribution of the error terms to the sum $S_{W,\mathbf{b}}(N)$ given in (2.11), note that for a given D the number of pairs d_1,d_2 for which $[d_1,d_2]=D$ is $\lesssim_\tau D^\tau$ for all $\tau>0$, and the summation in D is restricted to $D\leq R^2$ as the function $f(x)$ is supported on $x\leq 1$. Thus the total error obtained in (2.11) is bounded by

$$E_{W,\mathbf{b}}(N) \lesssim_\tau N^{n-kr-\delta'}\, W^n \sum_{D\leq R^2} D^\tau \lesssim N^{n-kr-\delta'/2}. \tag{2.14}$$

The main term can be evaluated by a routine calculation using the Chinese Remainder Theorem and the properties of the local factors $\sigma(D,,\mathbf{v})$ given in lemma 2.1. Indeed, to every $\mathbf{t}\in\mathbb{Z}_{DW}^n$ satisfying $\mathbf{t}\equiv\mathbf{b}\ (mod\ W)$ there is a unique $\mathbf{s}\in\mathbb{Z}_D^n$ such that $\mathbf{t}\equiv\mathbf{s}\ (mod\ D)$, and in that case $\mathcal{F}(\mathbf{s})\equiv\mathbf{v}\ (mod\ DW)$ is equivalent to $\mathcal{F}(\mathbf{s})\equiv\mathbf{v}\ (mod\ D)$ using out assumption that $\mathcal{F}(\mathbf{b})\equiv\mathbf{v}\ (mod\ W)$. Thus

$$\sum_{\substack{\mathbf{t}\in\mathbb{Z}^n_{DW},\ \mathbf{t}\equiv\mathbf{b}\ (mod\ W)\\ \mathcal{F}(\mathbf{t})\equiv\mathbf{v}\ (mod\ DW)}} \mathbf{1}_{D|t_1\cdots t_n} \prod_{p|W}\sigma_p(p,\mathbf{b},\mathbf{v})\prod_{p|D}\sigma_p(p,\mathbf{t},\mathbf{v})\prod_{p\nmid DW}\sigma_p(\mathbf{v})$$

$$= \prod_{p|W}\sigma_p(p,\mathbf{b},\mathbf{v})\prod_{p\nmid W}\sigma_p(\mathbf{v}) \sum_{\substack{\mathbf{s}\in\mathbb{Z}^n_D\\ \mathcal{F}(\mathbf{s})\equiv\mathbf{v}\ (mod\ D)}} \mathbf{1}_{D|s_1\cdots s_n}\prod_{p|D}\frac{\sigma_p(p,\mathbf{s},\mathbf{v})}{\sigma_p(\mathbf{v})}. \tag{2.15}$$

Then (2.6) follows from (2.11)-(2.15), and to see the validity of (2.7) it is enough to remark that carrying out the calculation in (2.11) for the sum $S_{W,q,\mathbf{b}}(N)$ the only difference is that the indicator function $\mathbf{1}_{D|x_1\ldots x_n}$ is replaced by $\mathbf{1}_{[D,q]|x_1\ldots x_n}$ and hence (2.12)-(2.15) remains true with D replaced by $[D,q]$. □

The sum

$$S_W(f,\gamma) := \sideset{}{'}\sum_{(D,W)=1} \gamma_D(\mathbf{v})h_D(R) \tag{2.16}$$

can be asymptotically evaluated by sieve methods, see [10], [24]; we will sketch the approach in [24] and indicate how to modify the argument to obtain an asymptotic for the related sum

$$S_{W,q}(f,\gamma) := \sideset{}{'}\sum_{(D,W)=1} \gamma_{[D,q]}(\mathbf{v})h_D(R) \tag{2.17}$$

needed for the "concentration" estimate (1.7).

Lemma 2.3. *([?], Prop. 10) Let $\gamma_D(\mathbf{v})$ be a multiplicative function satisfying estimate* (1.14)*. Then one has*

$$S_W(f,\gamma) = \Big(\frac{\phi(W)}{W}log\,R\Big)^{-n}\int_0^\infty (f^{(n)}(x))^2\,\frac{x^{n-1}}{(n-1)!}\,dx\ +\ o_{\omega\to\infty}(1). \tag{2.18}$$

Moreover if $q>\omega$ is a prime then

$$S_{W,q}(f,\gamma)\ =\ \frac{n}{q}\Big(\frac{\phi(W)}{W}log\,R\Big)^{-n}\int_0^\infty \Big(f^{(n)}(x)-f^{(n)}\big(x+\frac{log\,q}{log\,R}\big)\Big)^2\,\frac{x^{n-1}}{(n-1)!}\,dx\ +\ o_{\omega\to\infty}(1), \tag{2.19}$$

Proof. We specify $f(x)=(1-x)_+^{4n}$, the function $e^x f(x)$ is compactly supported and $4n-1$ continuously differentiable hence its Fourier transform, denoted by $\widehat{f}(t)$, satisfies $|\widehat{f}(t)|\lesssim(1+|t|)^{-4n}$. Substituting the Fourier inversion formula

$$e^x f(x) = \int_{\mathbb{R}} e^{-itx}\widehat{f}(t)\,dt$$

into (2.13) one obtains

$$h_D(R) = \int_{\mathbb{R}}\int_{\mathbb{R}}\sum_{[d_1,d_2]=D}\mu(d_1)\mu(d_2)d_1^{-\frac{1+it_1}{log\,R}}d_2^{-\frac{1+it_2}{log\,R}}\widehat{f}(t_1)\widehat{f}(t_2)\,dt_1dt_2 =: \int_{\mathbb{R}}\int_{\mathbb{R}} g_D(t_1,t_2)\,dt_1dt_2. \tag{2.20}$$

The function $g_D(t_1,t_2)H_D(R)$ is multiplicative in D hence

$$\sideset{}{'}\sum_{(D,W)=1} g_D(t_1,t_2)\gamma_D(\mathbf{v}) = \prod_{p>\omega}(1+g_p(t_1,t_2))\gamma_p(\mathbf{v}),$$

which gives

$$S_W(f,\gamma) = \int_{\mathbb{R}}\int_{\mathbb{R}} \prod_{p>\omega}(1 - \frac{\gamma_p(\mathbf{v})}{p^{\frac{1+it_1}{log\,R}}} - \frac{\gamma_p(\mathbf{v})}{p^{\frac{1+it_2}{log\,R}}} + \frac{\gamma_p(\mathbf{v})}{p^{\frac{2+it_1+it_2}{log\,R}}})\ \widehat{f}(t_1)\widehat{f}(t_2)\, dt_1 dt_2. \tag{2.21}$$

By Proposition 1.2

$$log\left|1 - \frac{\gamma_p(\mathbf{v})}{p^{\frac{1+it_1}{log\,R}}} - \frac{\gamma_p(\mathbf{v})}{p^{\frac{1+it_2}{log\,R}}} + \frac{\gamma_p(\mathbf{v})}{p^{\frac{2+it_1+it_2}{log\,R}}}\right| \leq 3n\,p^{-1-\frac{1}{log\,R}} + O(p^{-2}).$$

By the well-know asymptotic

$$\sum_p p^{-1-\frac{1}{log\,R}} = log\,log\,R + O(1),$$

we see that the integrand in (2.21) is bounded by $C(log\,R)^{3n}(1+|t_1|)^{-4n}(1+|t_2|)^{-4n}$. Integrating over the range $|t_1|,|t_2| > \sqrt{log\,R}$ gives

$$S_W(f,\gamma) \;=\; \int_{|t_1|,|t_2|\leq\sqrt{log\,R}} \prod_{p>\omega}(1 - \frac{\gamma_p(\mathbf{v})}{p^{\frac{1+it_1}{log\,R}}} - \frac{\gamma_p(\mathbf{v})}{p^{\frac{1+it_2}{log\,R}}} + \frac{\gamma_p(\mathbf{v})}{p^{\frac{2+it_1+it_2}{log\,R}}})\ \widehat{f}(t_1)\widehat{f}(t_2)\, dt_1 dt_2 + O(log^{-n} R).$$

Let, for $Re(s) > 1$,

$$\zeta_W(s) := \prod_{p>\omega}(1 - \frac{1}{p^s})^{-1} = \zeta(s)\prod_{p\leq\omega}(1 - \frac{1}{p^s}).$$

From (1.14) it is easy to see that

$$\prod_{p>\omega}(1 - \frac{\gamma_p(\mathbf{v})}{p^{\frac{1+it_1}{log\,R}}} - \frac{\gamma_p(\mathbf{v})}{p^{\frac{1+it_2}{log\,R}}} + \frac{\gamma_p(\mathbf{v})}{p^{\frac{2+it_1+it_2}{log\,R}}}) \;=\; \frac{\zeta_W^n(1+s_1+s_2)}{\zeta_W^n(1+s_1)\zeta_W^n(1+s_2)}\,(1 + o\omega \to \infty(1)), \tag{2.22}$$

with $s_1 = 1 + \frac{1+it_1}{log\,R}$, $s_2 = 1 + \frac{1+it_2}{log\,R}$. On the range $|t_1|,|t_2| \leq \sqrt{log\,R}$ one has that

$$\prod_{p\leq\omega}(1 - p^{-s}) = \prod_{p\leq\omega}(1 - p^{-1})(1 + o_{\omega\to\infty}(1)) = \frac{\phi(W)}{W}(1 + o\omega \to \infty(1)).$$

Thus from the basic property $\zeta(s) = (s-1)^{-1} + O(1)$ for s near 1, it follows

$$\zeta_W(s) = \frac{1}{s-1}\frac{\phi(W)}{W}\,(1 + o\omega \to \infty(1)).$$

Substituting this into (2.22) gives

$$S_W(f,\gamma) \;=\; (\frac{\phi(W)}{W}log\,R)^{-n}\int_{|t_1|,|t_2|\leq\sqrt{log\,R}} \frac{(1+it_1)^n(1+it_2)^n}{(2+it_1+it_2)^n}\,\widehat{f}(t_1)\widehat{f}(t_2)\, dt_1 dt_2 \;+\; o(1).$$

Note that by the quick decrease of $\widehat{f}(t)$ the integration in t_1 and t_2 can be extended to $\mathbb{R}$ by making an error of $o(1)$. Finally, using the identities

$$(2 + it_1 + it_2)^{-n} = \int_0^\infty e^{-x(2+it_1+t_2)}\,\frac{x^{(n-1)}}{(n-1)!}\,dx, \tag{2.23}$$

and

$$f^{(n)}(x) = (-1)^n \int_{\mathbb{R}} e^{-x(1+it)}(1+it)^n \widehat{f}(t)\,dt \tag{2.24}$$

obtained by integration by parts, one may write

$$S_W(f,\gamma) \;=\; (\frac{\phi(W)}{W}log\,R)^{-n}\int_0^\infty (f^{(n)}(x))^2\,\frac{x^{(n-1)}}{(n-1)!}\,dx + o_{\omega\to\infty}(1).$$

This shows (2.15).

To show (2.19) we modify the above argument as follows. We have

$$S_{W,q}(f,\gamma) \;=\; \int_{\mathbb{R}}\int_{\mathbb{R}} \sideset{}{'}\sum_{(D,W)=1} g_D(t_1,t_2)\,\gamma_{[D,q]}(\mathbf{v})\,\widehat{f}(t_1)\widehat{f}(t_2)\,dt_1dt_2. \tag{2.25}$$

For the inner sum we separate the cases $q\nmid D$ and $q|D$ in which case we change variables $D:=qD$, this gives

$$\sideset{}{'}\sum_{(D,W)=1} g_D(t_1,t_2)\,\gamma_{[D,q]}(\mathbf{v}) \;=\; \gamma_q(\mathbf{v})(1+g_q(t_1,t_2)) \sideset{}{'}\sum_{\substack{(D,W)=1\\ q\nmid D}} g_D(t_1,t_2)\,\gamma_{[D,q]}(\mathbf{v}) \;=$$

$$\frac{\gamma_q(\mathbf{v})(1+g_q(t_1,t_2))}{1+g_q(t_1,t_2)\gamma_q(\mathbf{v})}\prod_{\substack{p>\omega\\ p\neq q}}(1-\frac{\gamma_p(\mathbf{v})}{p^{\frac{1+it_1}{log\,R}}}-\frac{\gamma_p(\mathbf{v})}{p^{\frac{1+it_2}{log\,R}}}+\frac{\gamma_p(\mathbf{v})}{p^{\frac{2+it_1+it_2}{log\,R}}}).$$

Note that this differs from the integrand in(2.22) only by that additional factor

$$\frac{\gamma_q(\mathbf{v})(1+g_q(t_1,t_2))}{1+g_q(t_1,t_2)\gamma_q(\mathbf{v})} == \frac{n}{q}(1-q^{-\frac{1+it_1}{log\,R}})(1-q^{-\frac{1+it_2}{log\,R}})\,(1+o(1)), \tag{2.26}$$

as by our assumption $q>\omega$ hence $\gamma_q(\mathbf{v})=\frac{n}{q}(1+o(1)$. Thus we have the analogue of (2.22)

$$S_{W,q}(f,\gamma) \;=\; \frac{n}{q}(\frac{\phi(W)}{W}\,log\,R)^{-n}\int_{\mathbb{R}}\int_{\mathbb{R}}\frac{(1+it_1)^n(1+it_2)^n}{(2+it_1+it_2)^n}\;\times \tag{2.27}$$

$$(1-e^{-\frac{(1+it_1)log\,q}{log\,R}})(1-e^{-\frac{(1+it_2)log\,q}{log\,R}})\,\widehat{f}(t_1)\widehat{f}(t_2)\,dt_1dt_2\;+\;o(1).$$

Finally, using (2.23) and (2.24) the one may rewrite the integral in (2.27) as

$$\int_0^\infty\left(\int_R(e^{-x(1+it)}-e^{-(x+\frac{log\,q}{log\,R})(1+it)})\,(1+it)^n\,\widehat{f}(t)\,dt\right)^2\frac{x^{n-1}}{(n-1)!}\;dx \tag{2.28}$$

$$=\int_0^\infty\left(\int_R f^{(n)}(x)-f^{(n)}(x+\frac{log\,q}{log\,R})\right)^2\frac{x^{n-1}}{(n-1)!}\;dx.$$

□

We turn to the proof of our main results now. First we prove Theorem 1.2 which follows from Lemma 2.2. and Lemma 2.3 by routine calculation using the properties of the local factors $\sigma_p(p,\mathbf{b},\mathbf{v})$ given in Lemma 2.1.

Proof of Theorem 1.2. Let $\eta\le\frac{\eta(r,k)}{2(1+\eta(r,k))}$ with $\eta(r,k)$ be as specified in (1.7) Then by (2.6) and (2.15) one has

$$\sum_{\substack{\mathbf{x}\in[N]^n\\ (\mathbf{x},W)=1,\ \mathcal{F}(\mathbf{x})=\mathbf{v}}}\Lambda_R^2(x_1x_2\cdots x_n) \;=\; \sum_{\substack{\mathbf{b}\in\mathbb{Z}_W^n\\ (\mathbf{b},W)=1}} S_{N,W,\mathbf{b}}(\mathbf{v}) \tag{2.29}$$

$$= c_n(f)\,N^{n-dr}J(N^{-d}\mathbf{v})\,(log\,R)^{-n}\phi(W)^{-n}\,(1+o_{\omega\to\infty}(1))\sum_{\substack{\mathbf{b}\in\mathbb{Z}_W^n\\ (\mathbf{b},W)=1}}\mathfrak{S}_{W,\mathbf{b}}(\mathbf{v})\;+\;O(N^{n-kr-\delta'}).$$

By Lemma 2.1 and the Chinese Remainder Theorem

$$\phi(W)^{-n} \sum_{\substack{\mathbf{b}\in\mathbb{Z}_W^n \\ (\mathbf{b},W)=1}} \mathfrak{S}_{W,\mathbf{b}}(\mathbf{v}) = \prod_{p|W} \Big(\phi(p)^{-n} \sum_{\substack{\mathbf{b}\in\mathbb{Z}_p^n \\ (\mathbf{b},p)=1}} \sigma_p(p,\mathbf{b};\mathbf{v}) \Big) \prod_{p\nmid W} \sigma_p(\mathbf{v}). \tag{2.30}$$

Note that $\sigma_p(\mathbf{v}) = 1 + O(p^{-2})$ and hence $\prod_{p\nmid W} \sigma_p(\mathbf{v}) = 1 + o_{\omega\to\infty}(1)$. For a fixed $l \in \mathbb{N}$ and prime $p \leq \omega$, by (1.10)

$$\phi(p)^{-n} p^{-l(n-r)} \sum_{\substack{(\mathbf{b},p)=1 \\ \mathcal{F}(\mathbf{b})\equiv\mathbf{v}\ (mod\ p)}} |\{\mathbf{x}\in\mathbb{Z}_{p^l}^n;\ \mathcal{F}(p\mathbf{x}+\mathbf{b}) = \mathbf{v}\}| \tag{2.31}$$

$$= \phi(p)^{-n} p^{-l(n-r)} p^n |\{\mathbf{y}\in\mathbb{Z}_{p^l}^n;\ (\mathbf{y},p)=1,\ \mathcal{F}(\mathbf{y}) = \mathbf{v}\}| = \frac{p^{ln}}{\phi^n(p^l)}\ \mathcal{M}(p^l;\mathbf{v}),$$

where $\mathcal{M}(p^l;\mathbf{v})$ is the number of solutions to $\mathcal{F}(\mathbf{y}) \equiv \mathbf{v}\ (mod\ p^l)$ in the reduced residue classes $\mathbf{y}\in\mathbb{Z}_{p^l}^n$, $(\mathbf{y},p)=1$. Taking the limit $l\to\infty$, and recalling definition (1.12)

$$\phi(p)^{-n} \sum_{\substack{(\mathbf{b},p)=1 \\ \mathcal{F}(\mathbf{b})\equiv\mathbf{v}\ (mod\ p)}} \sigma_p(p,\mathbf{b};\mathbf{v}) = \sigma_p^*(\mathbf{v}),$$

and then by (2.30)

$$\phi(W)^{-n} \sum_{\substack{(\mathbf{b},W)=1 \\ \mathcal{F}(\mathbf{b})\equiv\mathbf{v}\ (mod\ W)}} \mathfrak{S}_{W,\mathbf{b}}(\mathbf{v}) = \prod_{p|W} \sigma_p^*(\mathbf{v})\ (1 + o_{\omega\to\infty}(1)) = \mathfrak{S}^*(\mathbf{v})\,(1 + o_{\omega\to\infty}(1)).$$

This proves (1.7).

To prove (1.8) note that to estimate a sum over $\mathbf{x}\in[N]^n\backslash(\mathbf{P}^\varepsilon(N))^n$ under the restriction $(\mathbf{x},W)=1$ one needs to sum only over those $\mathbf{x}=(x_1,\ldots,x_n)$ for which $q|x_1\ldots x_n$ for some prime $\omega < q \leq N^\varepsilon$. Thus, recalling the definition of the sums $S_{W,q,\mathbf{b}}(N)$ given in (2.5) we have that

$$\sum_{\substack{\mathbf{x}\in[N]^n\backslash(\mathbf{P}^\varepsilon(N))^n \\ (\mathbf{x},W)=1,\,\mathcal{F}(\mathbf{x})=\mathbf{v}}} \Lambda_R^2(x_1\ldots x_n) \leq \sum_{\omega<q\leq N^\varepsilon} \sum_{\substack{(\mathbf{x},W)=1, \\ \mathcal{F}(\mathbf{x})=\mathbf{v}}} \mathbf{1}_{q|x_1\ldots x_n}\, \Lambda_R^2(x_1\ldots x_n)\phi_N(\mathbf{x}) = \sum_{\omega<q\leq N^\varepsilon} S_{W,q,\mathbf{b}}(N).$$

Let us make the simple observation that $|f^{(n)}(x) - f^{(n)}(x+\tau)| \leq \tau\,|f^{(n+1)}(x)|$ for $0\leq x,\tau\leq 1$ for our choice $f(x) = (1-x)_+^{4n}$. Then by estimates (2.7) and (2.19)

$$\sum_{\omega<q\leq N^\varepsilon} S_{W,q,\mathbf{b}}(N) \leq \frac{n}{q}\left(\frac{log\,q}{log\,R}\right)^2 c_{n+1}(f)\, N^{n-rk}(log\,R)^{-n}\mathfrak{S}^*(N,\mathbf{v})(1+o_{\omega\to\infty}(1)) + O(N^{n-rk-\delta}).$$

Write $\varepsilon' := \varepsilon/\eta$, so that $N^\varepsilon = R^{\varepsilon'}$ with $R = N^\eta$. The sum over the primes $\omega < q \leq R^{\varepsilon'}$ can be estimated by a dyadic decomposition using the Prime Number Theorem

$$\sum_{\omega<q\leq R^{\varepsilon'}} q^{-1}\,(log\,q)^2 = \sum_{\omega\leq 2^j\leq R}\ \sum_{2^{j-1}<q\leq 2^j} q^{-1}\,(log\,q)^2 \leq\ (2+o_{\omega\to\infty}(1)) \sum_{j\leq\varepsilon' log_2 R} j\ \leq 2\,(\varepsilon')^2.$$

This implies (1.8). $\square$

Proof of Theorem (1.1). We need to choose $\varepsilon > 0$ to ensure that the expression in (1.8) is essentially less then the one in (1.7). For that one needs to compare the quantities $c_{n+1}(f)$ and

$c_n(f)$ defined in Theorem 1.5. For our choice $f(x) = (1-x)_+^{4n}$ we have that $f^{(n)}(x) = \alpha_n(1-x)_+^{3n}$ while $f^{(n+1)}(x) = 3n\alpha_n(1-x)_+^{3n}$ (with $\alpha_n = (4n)!/(3n)!$), thus by the beta function identity

$$\int_0^1 (1-x)^a x^b\, dx = \frac{a!\, b!}{(a+b+1)!}$$

it is easy to see that $c_{n+1}(f) < 16n^2\, c_n(f)$. Thus if $32n^3\,(\varepsilon/\eta)^2 \leq 1/2$ then for N and $\omega =$ sufficiently large

$$\sum_{\substack{\mathbf{x}\in(\mathbf{P}^\varepsilon(N))^n \\ \mathcal{F}(\mathbf{x})=\mathbf{v}}} \Lambda_R^2(x_1x_2\cdots x_n)\ \phi_N(\mathbf{x}) \geq\ c_n\, N^{n-dr}\,(log\, R)^{-n}\,\mathfrak{S}^*(N,\mathbf{v}) \tag{2.32}$$

for some positive constant $c_n = c_n(f) > 0$.

Finally note that if $\mathbf{x} =\in (\mathbf{P}^\varepsilon(N))^n$ then each coordinate x_i can have at most $1/\varepsilon$ prime divisors hence $\Lambda_R(x_1x_2\cdots x_n) \leq 2^{n/\varepsilon}$. Thus by (2.32) the number of solutions to $\mathcal{F}(\mathbf{x}) = \mathbf{v}$ in $\mathbf{x} \in (\mathbf{P}^\varepsilon(N))^n$ satisfies

$$\mathcal{M}_{\mathcal{F}}^\varepsilon(N)\ \geq\ c(n,k,r)\, N^{n-dr}\,(log\, N)^{-n}\,\mathfrak{S}^*(N,\mathbf{v}),$$

with $c(n,k,r) := c_n\, 2^{-2n/\varepsilon}$ for some $\varepsilon = \varepsilon(n,k,r) > 0$. In fact one may choose $\varepsilon := (4n)^{-3/2}\eta(r,k)$ with $\eta(r,k) = (8r^2(r+1)(r+2)k(k+1))^{-1}$ given in (1.7). This proves Theorem 1.1 $\square$

3. The local factors.

In this section we study the Euler factors $\gamma_p(\mathbf{v})$ and prove the asymptotic formula (1.14). Recall

$$\sigma_p(p,\mathbf{s},\mathbf{v}) = \lim_{l\to\infty} \sigma_p^l(p,\mathbf{s},\mathbf{v}), \qquad \text{where}$$

$$\sigma_p^l(p,\mathbf{s},\mathbf{v}) = p^{-l(n-r)}\,|\{\mathbf{x}\in\mathbb{Z}_{p^l}^n;\ \mathcal{F}(p\,\mathbf{x}+\mathbf{s}) \equiv 0\ (mod\ p^l)\}|.$$

Note that this factor is non-zero only if $\mathcal{F}(\mathbf{s}) \equiv \mathbf{v}$ $(mod\ p)$. We call a point $\mathbf{s}\in\mathbb{Z}_p^n$ *non-singular* if the Jacobian $Jac_{\mathcal{F}}(\mathbf{s})$ has full rank ($= r$) over the finite field $\mathbb{Z}_p$. In this case it is easy to calculate factors $\sigma_p^l(p,\mathbf{s},\mathbf{v})$ explicitly.

Lemma 3.1. *Let $\mathbf{s}\in\mathbb{Z}_p^n$ be a non-singular solution to the equation $\mathcal{F}(\mathbf{s}) \equiv \mathbf{v}$ $(mod\ p)$. Then*

$$\sigma_p^l(p,\mathbf{s},\mathbf{v}) = p^r. \tag{3.1}$$

Proof. We proceed by induction on l. For $l = 1$ we have $\mathcal{F}(p\mathbf{x}+\mathbf{s}) \equiv \mathcal{F}(\mathbf{s}) \equiv \mathbf{v}$ $(mod\ p)$ for all $\mathbf{x}\in\mathbb{Z}_p^n$ thus $\sigma_p^1(p,\mathbf{s},\mathbf{v}) = p^r$. Let $l = 2$. We'd like to count $\mathbf{x}\in\mathbb{Z}_{p^2}^n$ satisfying

$$\mathcal{F}(p\mathbf{x}+\mathbf{s}) \equiv \mathcal{F}(\mathbf{s}) + p\ Jac_{\mathcal{F}}(\mathbf{s})\cdot\mathbf{x}\ \equiv \mathbf{v}\ \ (mod\ p^2).$$

Since $\mathcal{F}(\mathbf{s}) - \mathbf{v} = p\mathbf{u}$ this reduces to

$$Jac_{\mathcal{F}}(\mathbf{s})\cdot\mathbf{x} \equiv -\mathbf{u}\ \ (mod\ p).$$

By assumption the map $Jac_{\mathcal{F}}(\mathbf{s}) : \mathbb{Z}_p^n \to \mathbb{Z}_p^n$ has full rank, thus the above equation has p^{n-r} solution in $\mathbb{Z}_p^n$ and hence p^{2n-r} solutions $\mathbf{x}\in\mathbb{Z}_{p^2}^n$. It follows that $\sigma_p^2(p,\mathbf{s},\mathbf{v}) = p^r$. For $l \geq 3$ we show that

$$\sigma_p^l(p,\mathbf{s},\mathbf{v}) = \sigma_p^{l-1}(p,\mathbf{s},\mathbf{v}).$$

Note that if $\mathbf{x} \equiv \mathbf{y}$ $(mod\ p^{l-1})$ then $\mathcal{F}(p\mathbf{x}+\mathbf{s}) \equiv \mathcal{F}(p\mathbf{y}+\mathbf{s})$ $(mod\ p^l)$. For given $\mathbf{y} \in \mathbb{Z}^n_{p^{l-1}}$ write $\mathbf{y} = p^{l-2}\mathbf{u} + \mathbf{z}$ with $\mathbf{z} \in \mathbb{Z}^n_{p^{l-2}}$ and $\mathbf{u} \in \mathbb{Z}^n_p$. Then

$$\mathcal{F}(p\mathbf{y}+\mathbf{s}) \equiv \mathcal{F}(p^{l-1}\mathbf{u}+p\mathbf{z}+\mathbf{s}) \equiv \mathcal{F}(p\mathbf{z}+\mathbf{s}) + p^{l-1} Jac_{\mathcal{F}}(\mathbf{s}) \cdot \mathbf{u} \ \ (mod\ p^l). \tag{3.2}$$

Thus $\mathcal{F}(p\mathbf{y}+\mathbf{s}) \equiv \mathbf{v}$ $(mod\ p^l)$ implies that

$$\mathcal{F}(p\mathbf{z}+\mathbf{s}) \equiv \ (mod\ p^{l-1}), \tag{3.3}$$

the number such $\mathbf{z} \in \mathbb{Z}^n_{p^{l-2}}$ is $p^{-n}p^{(l-1)(n-r)}\sigma_p^{l-1}(p,\mathbf{s},\mathbf{v})$. For a given $\mathbf{z}$ satisfying (3.3) write $\mathcal{F}(p\mathbf{z}+\mathbf{s}) = p^{l-1}\mathbf{b}+\mathbf{v}$, then (3.2) holds if and only if

$$Jac_{\mathcal{F}}(\mathbf{s}) \cdot \mathbf{u} \equiv -\mathbf{b} \quad (mod\ p). \tag{3.4}$$

By our assumption $Jac_{\mathcal{F}}(\mathbf{s})$ has full rank $(= r)$ above $\mathbb{Z}^n_p$ thus the number of solutions to (3.4) is p^{n-r}. Since that decomposition $\mathbf{y} = p^{l-2}\mathbf{u}+\mathbf{z}$ is unique it follows that

$$\sigma_p^l(p,\mathbf{s},\mathbf{v}) = p^n p^{-l(n-r)} p^{-n} p^{(l-1)(n-r)} p^{n-r} \sigma_p^{l-1}(p,\mathbf{s},\mathbf{v}) = \sigma_p^{l-1}(p,\mathbf{s},\mathbf{v}).$$

□

For singular values of $\mathbf{s}$ we can only get upper bounds on the local factors $\sigma_p(p,\mathbf{s},\mathbf{v})$. The case $\mathbf{s} = \mathbf{v} = \underline{0}$ suggests that one cannot get better estimates then p^{kr}.

Lemma 3.2. *Let $\mathcal{F}$ be a family of r integral forms of degree k, and assume that*

$$codim\ (V^*_{\mathcal{F}}) \geq r(r+1)(k-1)2^k + 1. \tag{3.5}$$

Then uniformly for $l \in \mathbb{N}$ and $\mathbf{s} \in \mathbb{Z}^n_p$ one has

$$\sigma_p^l(p,\mathbf{s},\mathbf{v}) \lesssim p^{r^2k}. \tag{3.6}$$

Proof. By (4.31) we have

$$\sigma_p^l(p,\mathbf{s},\mathbf{v}) = \sum_{m=0}^{l} \sum^{*}_{\mathbf{b}\in\mathbb{Z}^r_{p^m}} p^{-mn} e^{-2\pi i \frac{\mathbf{b}\cdot\mathcal{F}(p\mathbf{x}+\mathbf{s})}{p^m}} S_{\mathbf{b},p^m}(p,\mathbf{s}),$$

where the sum in $\mathbf{b}$ are taken over r-tuples with at least one coordinate not divisible by p, and $S_{\mathbf{b},p^m}(p,\mathbf{s})$ is the exponential sum defined in (4.8). If $m > rk$ then Lemma 4.4 applies with $\varepsilon = 1/r$ (and $K = codim\ (V^*_{\mathcal{F}})/2^{k-1}$) thus

$$\sum_{m>rk} \sum^{*}_{\mathbf{b}\in\mathbb{Z}^r_{p^m}} p^{-mn} |S_{\mathbf{b},p^m}(p,\mathbf{s})| \lesssim \sum_{m>rk} p^{mr} p^{-\frac{mK}{(r+1)(k-1)}+\tau} \lesssim \sum_{m>rk} p^{-m\tau/2} \lesssim 1,$$

if $\tau = \tau(r,k) > 0$ is chosen sufficiently small. Indeed, by (3.5) we have $\frac{K}{(r+1)(k-1)} - r = \tau_0(r,k) > 0$ and then (3.6) then follows from the trivial estimate $p^{-mn}|S_{\mathbf{b},p^m}(p,\mathbf{s})| \leq 1$. □

Proof of Proposition 1.2. Since $\sigma_p^{-1}(\mathbf{v}) = 1 + O(p^{-2})$ for sufficiently large primes p it is enough to show that (1.14) holds for

$$\sigma_p(\mathbf{v})\gamma_p(\mathbf{v}) := p^{-n} \sum_{\mathcal{F}(\mathbf{s})\equiv\mathbf{v}\ (mod\ p)} \mathbf{1}_{p|\mathbf{s}_1\cdots s_n} \sigma_p(p,\mathbf{s},\mathbf{v})$$

$$= p^{-n} \sum_{\substack{\mathcal{F}(\mathbf{s})\equiv 0\ (mod\ p) \\ \mathbf{s}\ non-singular}} \mathbf{1}_{p|\mathbf{s}_1\cdots s_n} \sigma_p(p,\mathbf{s},\mathbf{v}) + p^{-n} \sum_{\substack{\mathcal{F}(\mathbf{s})\equiv 0\ (mod\ p) \\ \mathbf{s}\ singular}} \mathbf{1}_{p|\mathbf{s}_1\cdots s_n} \sigma_p(p,\mathbf{s},\mathbf{v})$$

$$= p^{-n+r} \sum_{\mathcal{F}(\mathbf{s})\equiv 0\ (mod\ p)} \mathbf{1}_{p|\mathbf{s}_1\cdots s_n} - p^{-n+r} \sum_{\substack{\mathcal{F}(\mathbf{s})\equiv 0\ (mod\ p)\\ \mathbf{s}\ singular}} \mathbf{1}_{p|\mathbf{s}_1\cdots s_n} + p^{-n} \sum_{\substack{\mathcal{F}(\mathbf{s})\equiv 0\ (mod\ p)\\ \mathbf{s}\ singular}} \mathbf{1}_{p|\mathbf{s}_1\cdots s_n}\sigma_p(p,\mathbf{s},\mathbf{v})$$
$$=: \gamma_p^1(\mathbf{v}) - \gamma_p^2(\mathbf{v}) + \gamma_p^3(\mathbf{v}).$$

Let $V^*_{\mathcal{F}}(p)$ denote the locus of singular points $\mathbf{s} \in \mathbb{Z}_p^n$ of the $(mod\ p)$-reduced variety $V_{\mathcal{F}}(p) := \{\mathcal{F}(\mathbf{s}) = \mathbf{v}\}$. It is well-known fact in arithmetic geometry, see [23], that

$$codim\,(V^*_{\mathcal{F}}(p)) = codim\,(V^*_{\mathcal{F}}),$$

for all but finitely many primes p, i.e. that codimension of the singular variety does not change when the equations defining the variety are considered $mod\ p$. Also, the number of points over $\mathbb{Z}_p$ on a homogeneous algebraic set V is bounded by its degree times $p^{dim\,V}$, see [8] Prop. 12.1, hence $|V^*_{\mathcal{F}}(p)| \lesssim p^{n-codim\,(V^*_{\mathcal{F}})}$, where the implicit constant may depend on n, k and r. Thus for sufficiently large primes $p \geq \omega$ we may apply Lemma 3.1 which gives for $i = 2, 3$

$$|\gamma_p^i(\mathbf{v})| \lesssim p^{-n+r^2k} p^{n-codim\,(V^*_{\mathcal{F}})} \lesssim p^{r^2k-r(r+1)(k-1)2^{k-1}-1} \lesssim p^{-2}.$$

For $J \subseteq [1, n]$ let define the coordinate subspace $M_J := \{\mathbf{s} = (s_1, \ldots, s-n) \in \mathbb{Z}_p^n;\ s_j = 0\ \forall\ j \in J\}$. By the inclusion-exclusion principle we have that

$$\gamma_p^1(\mathbf{v}) = p^{-n+r} \sum_{j=1}^{n} (-1)^{j-1} \sum_{|J|=j} \sum_{\mathbf{s}\in M_J} \mathbf{1}_{\mathcal{F}(\mathbf{s})=\mathbf{v}}. \tag{3.7}$$

If $\mathcal{F}$ is a system of r forms then it is not hard to show that $rank(\mathcal{F}|_{M_J}) \geq rank(\mathcal{F}) - r|J|$ for any subspace M_J of codimension $|J|$, see [6], Cor. 2. By our assumption on the rank of the system $\mathcal{F}$ we have that for $1 \leq |J| \leq r + 1$

$$rank(\mathcal{F}|_{M_J}) - r|J| \geq r(r + 1)(k - 1)2^k - r(r + 1) > 2^k.$$

Then by Proposition 4 in [7] applied the the system $\mathcal{F}$ restricted to the subspace $M_J \simeq \mathbb{Z}_p^{n-j}$ one has

$$p^{-(n-j)+r} |\{\mathbf{s} \in M_J; \mathcal{F}(\mathbf{s}) = \mathbf{v}\}| = 1 + O\left(p^{-\frac{rank(\mathcal{F}|_{M_J})-r}{2^k}}\right) = 1 + O(p^{-1}) \tag{3.8}$$

This implies that corresponding to $2 \leq j \leq r + 1$ in (3.7) contribute $O(p^{-j}) = O(p^{-2})$ to the expression $\gamma_p^1(\mathbf{v})$, while the trivial fact $|M_J| = p^{n-j} \leq p^{n-r-2}$ shows that the same holds for the terms corresponding to $j \geq r + 2$. Thus, again by (3.8)

$$\gamma_p^1(\mathbf{v}) = p^{-n+r} \sum_{j=1}^{n} \sum_{\mathbf{s}\in M_{\{j\}}} \mathbf{1}_{\mathcal{F}(\mathbf{s})=\mathbf{v}} + O(p^{-2}) = \frac{n}{p} + O(p^{-2}).$$

This proves the Proposition. □

4. Appendix: Diophantine equations over $\mathbb{Z}$ and $\mathbb{Z}_p$.

In this section we sketch the proof of Proposition 2, which is a minor variant of the main result of [3], see Theorem 1 there. For a family of integral forms $\mathcal{F} = (F_1, \ldots, F_r)$ and given $d \in \mathbb{N}$, $\mathbf{s} \in \mathbb{Z}^r$, $\alpha \in \mathbb{R}^r$ define the exponential sum

$$S_N(d, \mathbf{s}, \alpha) := \sum_{\mathbf{x}\in\mathbb{Z}^n} e^{2\pi i\alpha\cdot\mathcal{F}(d\mathbf{x}+\mathbf{s})} \phi_N(d\mathbf{x} + \mathbf{s}), \tag{4.1}$$

where ϕ_N is the indicator function of a cube B_N of size N.

Then one has the analogue of Lemma 2.1 in [3]

Lemma 4.1. *Let $1 \leq d < N$, $N_1 := N/d$ and let $\mathbf{s} \in \mathbb{Z}^n$. Then*

$$|N_1^{-n} S_N(d, \mathbf{s}, \alpha)|^{2^{k-1}} \lesssim N_1^{-kn} \sum_{\mathbf{h}^1,\dots,\mathbf{h}^{k-1} \in [-N_1,N_1]^n} \prod_{j=1}^{n} \min\{N_1, \|d^k \alpha\, \Phi_j(\Phi_j(\mathbf{h}^1,\dots,\mathbf{h}^{k-1})\|^{-1}\}, \tag{4.2}$$

where for $1 \leq i \leq r$ the i=th component of the the multi-linear form Φ_j is given by

$$\Phi_j^i(\mathbf{h}^1,\dots,\mathbf{h}^{k-1}) = k! \sum_{1 \leq j_1,\dots,j_{k-1} \leq n} a^i_{j_1,\dots,j_{k-1},j}\, h^1_{j_1},\dots,h^{k-1}_{j_{k-1}},$$

and $\|\beta\|$ denotes the distance of a real number β to the closest integer.

Proof. Write

$$\mathcal{F}_{d,\mathbf{s}}(\mathbf{x}) := \mathcal{F}(d\mathbf{x} + \mathbf{s}) = d^k \mathcal{F}(\mathbf{x}) + G_{d,\mathbf{s}}(\mathbf{x}), \qquad deg\,(G_{d,\mathbf{s}}) < k. \tag{4.3}$$

Also, $\phi_N(d\mathbf{x} + \mathbf{s}) = \phi_{N_1,\mathbf{s}}(\mathbf{x})$ where $\phi_{N_1,\mathbf{s}}$ is the indicator function of the cube $B_{N_1,\mathbf{s}} = d^{-1}(B_N - \mathbf{s})$ of size N_1.

Introducing the differencing operators

$$D_{\mathbf{h}} F(\mathbf{x}) := F(\mathbf{x} + \mathbf{h}) - \mathcal{F}(\mathbf{x}),$$

as well as their multiplicative analogues

$$\Delta_{\mathbf{h}} \phi(\mathbf{x}) := \phi(\mathbf{x} + \mathbf{h}) \bar{\phi}(\mathbf{x}),$$

we have by applying the Cauchy-Schwarz inequality $k-1$-times

$$|N_1^{-n} S_N(d, \mathbf{s}, \alpha)|^{2^{k-1}}| \lesssim N_1^{-kn} \sum_{\mathbf{h}^1,\dots,\mathbf{h}^{k-1} \in \mathbb{Z}^n} \left| \sum_{\mathbf{x} \in \mathbb{Z}^n} e^{2\pi i \alpha \cdot D_{\mathbf{h}_{k-1}} \dots D_{\mathbf{h}_1} \mathcal{F}_{d,\mathbf{s}}(\mathbf{x})} \Delta_{\mathbf{h}_{k-1}} \dots \Delta_{\mathbf{h}_1} \phi_{N_1,\mathbf{s}}(\mathbf{x}) \right|. \tag{4.4}$$

By (4.3) and (**??**) we have that

$$D_{\mathbf{h}_{k-1}} \dots D_{h_1} \mathcal{F}_{d,\mathbf{s}}(\mathbf{x}) = d^k D_{\mathbf{h}_{k-1}} \dots D_{h_1} \mathcal{F}(\mathbf{x}) = d^k \sum_{j=1}^{n} x_j\, \Phi_j(\mathbf{h}_1,\dots,\mathbf{h}_{k-1}).$$

Estimate (4.2) then follows form the fact that $|\sum_{x \in I} e^{2pi\beta x}| \leq \min\{N_1, \|\beta\|^{-1}\}$ for any $\beta \in \mathbb{R}$, when the summation is taken over an interval I of length at most N_1. □

Once this is established, the rest of the arguments in [3] carry over to our situation leading the following *minor arcs* estimate. For given $1 \leq d < N$, $N_1 := N/d$ and $0 < \theta < 1$ define the system of *major arcs*

$$\mathcal{M}(\theta) := \bigcup_{1 \leq q \leq N_1^{(k-1)r\theta}} \bigcup_{(\mathbf{a},q)=1} \mathcal{M}_{\mathbf{a},q}(\theta), \qquad \textit{where} \tag{4.5}$$

$$\mathcal{M}_{\mathbf{a},q}(\theta) := \{\alpha \in [0,1]^r;\ |\alpha_i - a_i/q| \leq q^{-1} N_1^{-k+(k-1)r\theta},\ 1 \leq i \leq r\}.$$

Lemma 4.2. *[*[3]*, Lemma 3.3] If $\{d^k\alpha\} \notin \mathcal{M}(\theta)$ then one has for every $\tau > 0$*

$$|S_N(d, \mathbf{s}, \alpha)| \leq C_\tau\ N_1^{n-K\theta+\tau}. \tag{4.6}$$

We need the above estimate in slightly different form, depending only on α.

Lemma 4.3. *Let $0<\theta,\varepsilon<1$ and let $0<\eta\leq \varepsilon r(1-k^{-1})\theta$. If $d\leq N^{\frac{\eta}{1+\eta}}$ then for $\alpha\notin\mathcal{M}(\theta)$ one has uniformly for $\mathbf{s}\in\mathbb{Z}^n$*

$$|S_N(d,\mathbf{s},\alpha)|\lesssim_\tau\ N_1^{n-\frac{K}{1+\varepsilon}\theta+\tau}\qquad (\forall\ \tau>0). \tag{4.7}$$

Proof. If $d^k\alpha\in\mathcal{M}_{\mathbf{a},q}(\theta)$ (mod 1), then there is $q\leq N_1^{r(k-1)\theta}$ and $a_i\in\mathbb{Z}$ such that $(a_i,q)=1$ and $|d^k\alpha_i-a_i/q|\leq q^{-1}N_1^{-k+(k-1)r\theta}$. This implies that $|\alpha_i-a_i'/q_1|\leq q_1^{-1}N_1^{-k+(k-1)r\theta}$ for some $q_1\leq d^kN_1^{(k-1)r\theta}$ and $a_i'\in\mathbb{Z}$ for which $(a_i',q_1)=1$. If $d\leq N^{\frac{\eta}{1+\eta}}$ then $d\leq N_1^\eta$ and hence $q_1\leq N_1^{k\eta+r(k-1)\theta}\leq N_1^{(1+\varepsilon)r(k-1)\theta}$. This implies that $\alpha\notin\mathcal{M}((1+\varepsilon)\theta$. By taking the contrapositive and changing variables $\theta:=(1+\varepsilon)\theta$ the Lemma follows. ☐

As a first application we give an estimate for the Gauss sums

$$S_{\mathbf{a},q}(d,\mathbf{s}):=\sum_{\mathbf{x}\in\mathbb{Z}_q^n} e^{2\pi i\frac{\mathbf{a}\cdot\mathcal{F}(d\mathbf{x}+\mathbf{s})}{q}}. \tag{4.8}$$

Lemma 4.4. *Let $q\in\mathbb{N}$ and $1\leq d<q^{\frac{\varepsilon}{k}}$. Then for any $\mathbf{a}\in\mathbb{Z}^r$ such that $(\mathbf{a},q)=1$ and $\mathbf{s}\in\mathbb{Z}^d$ one has*

$$|S_{\mathbf{a},q}(d,\mathbf{s})|\lesssim_\tau q^{n-\frac{K}{(1+\varepsilon)r(k-1)}+\tau}\qquad (\forall\ \tau>0). \tag{4.9}$$

Proof. Note that $S_{\mathbf{a},q}(d,\mathbf{s})=S_N(d,\mathbf{s},\mathbf{a}/q)$ with $N=dq$, as $\mathbf{x}\in[0,q)^n$ if $d\mathbf{x}+\mathbf{s}\in B_N=[0,dq)^n+\mathbf{s}$. Moreover if $r(k-1)\theta<1$ then for any $1\leq q'\leq q^{r(k-1)\theta}<q$ and $(\mathbf{a}',q')=1$

$$\left|\frac{\mathbf{a}}{q}-\frac{\mathbf{a}'}{q'}\right|\geq\frac{1}{qq'}>\frac{1}{q'}\ q^{-k+r(k-1)\theta}.$$

This implies that $\mathbf{a}/q\notin\mathcal{M}(\theta)$. Since $d<q^{\frac{\varepsilon}{k}}$ we can choose θ so that $r(k-1)\theta<1$ but $d<q^\eta$ for $\eta:=\varepsilon r(1-k^{-1})\eta$. The (4.7) implies that

$$|S_{\mathbf{a},q}(d,\mathbf{s})|\lesssim_\tau q^{n-\frac{K}{(1+\varepsilon)}\theta+\tau}\lesssim_\tau q^{n-\frac{K}{(1+\varepsilon)r(k-1)}+\tau}\qquad (\forall\ \tau>0),$$

choosing θ sufficiently close to $\frac{1}{r(k-1)}$. ☐

Taking $d=1$ and letting $\varepsilon\to 0$ in (4.9) one has

$$S_{\mathbf{a},q}(1,\mathbf{s})=S_{\mathbf{a},q}(1,0)\lesssim_\tau\ q^{n-\frac{K}{r(k-1)}+\tau}.$$

Next, to apply [3], Lemma 4.4 adapted to our situation, we make the assumption that

$$K>(1+\varepsilon)r(r+1)(k-1). \tag{4.10}$$

Then one can chose small positive numbers δ and θ_0 so that

$$\delta+2r(r+2)\theta_0\ <1 \tag{4.11}$$

and

$$2\delta\theta_0^{-1}\ <\ K(1+\varepsilon)^{-1}-r(r+1)(k-1). \tag{4.12}$$

Lemma 4.5. *Let δ,θ_0 satisfy (4.10)-(4.11), and let $0<\eta\leq\varepsilon(1-k^{-1})\theta_0$. Then for $1\leq d\leq N^{\frac{\eta}{1+\eta}}$ and $\mathbf{s}\in\mathbb{Z}^n$ one has*

$$\int_{\alpha\notin\mathcal{M}(\theta_0)}|S_N(d,\mathbf{s},\alpha)|\,d\alpha\lesssim\ N_1^{n-dr-\delta}. \tag{4.13}$$

If in addition we make the assumption that

$$\eta < \delta k^{-1} r^{-1}, \tag{4.14}$$

then it is easy to see that

$$N_1^{n-dr-\delta} = N^{n-dr} d^{-n}\, N^{-\delta} d^{kr+\delta} \leq N^{n-dr} d^{-n}\, N^{-\delta+(kr+\delta)\eta(1+\eta)^{-1}} \leq N^{n-dr-\delta'} d^{-n}, \tag{4.15}$$

for some $\delta' > 0$.

Going back to Proposition 1.2, we have under the conditions of Lemma 4.5 and (4.14)

$$\mathcal{R}_N(d,\mathbf{s},\mathbf{v}) = \int e^{-2\pi i\,\alpha\cdot\mathbf{v}}\, S_N(d,\mathbf{s};\alpha)\, d\alpha = \int_{\mathcal{M}'(\theta_0)} e^{-2\pi i\,\alpha\cdot\mathbf{v}}\, S_N(d,\mathbf{s};\alpha)\, d\alpha + O(N^{n-rd-\delta'} d^{-n}),$$

for any set $\mathcal{M}'(\theta_0) \supseteq \mathcal{M}(\theta_0)$. From now on we will write

$$r(k-1)\theta_0 = \kappa, \tag{4.16}$$

and define

$$\mathcal{M}'(\theta_0) := \bigcup_{1\leq q\leq N_1^{\kappa}} \bigcup_{(\mathbf{a},q)=1} \mathcal{M}'_{\mathbf{a},q}(\theta_0), \quad \textit{where} \tag{4.17}$$

$$\mathcal{M}'_{\mathbf{a},q}(\theta_0) := \{\alpha \in [0,1]^r;\ |\alpha_i - a_i/q| \leq N_1^{-k+\kappa},\ 1 \leq i \leq r\}. \tag{4.18}$$

Next, for given $\alpha \in \mathcal{M}'_{\mathbf{a},q}(\theta_0)$, writing $\alpha = \mathbf{a}/q + \beta$ one has the following approximation of the sum $S_N(d,\mathbf{s};\alpha$ (see [3], Lemma 5.1).

Lemma 4.6. *Let $0 < \eta \leq \frac{1}{2},\ d \leq N^{\frac{\eta}{1+\eta}},\ \mathbf{s} \in \mathbb{Z}^n$. Then for $\alpha \in \mathcal{M}'_{\mathbf{a},q}(\theta_0)$*

$$S_N(d,\mathbf{s};\alpha) = N^n d^{-n} q^{-n} S_{\mathbf{a},q}(d,\mathbf{s})\, I(N^k\beta) \;+\; O(N^{n-1+2\eta+\kappa} d^{-n}), \tag{4.19}$$

where

$$I(\gamma) := \int_{\mathbb{R}^r} e^{2\pi i\gamma\cdot\mathcal{F}(\mathbf{y})} \phi(\mathbf{y})\, d\mathbf{y}. \tag{4.20}$$

Proof. Writing $\mathbf{x} := q\mathbf{y} + \mathbf{z}$ with $\mathbf{z} \in [0,q)^n$, we have

$$S_N(d,\mathbf{s};\alpha) = \sum_{\mathbf{z}\in\mathbb{Z}_q^n} e^{2\pi i\frac{\mathbf{a}\cdot\mathcal{F}(d\mathbf{z}+\mathbf{s})}{q}} \sum_{\mathbf{y}\in\mathbb{Z}^n} e^{2\pi i\beta\cdot\mathcal{F}(qd\mathbf{y}+d\mathbf{z}+\mathbf{s})} \phi_N(qd\mathbf{y}+d\mathbf{z}+\mathbf{s}). \tag{4.21}$$

As $\mathbf{y}$ varies by $O(1)$ in the range $|qd\mathbf{y}| \lesssim N$, the variation in the exponent is

$$O(|\beta| N^{k-1} qd) = O(N^{-1+2\kappa+\eta}).$$

Thus the error in replacing the sum $\sum e^{2\pi i\beta\cdot\mathcal{F}(qd\mathbf{y}+d\mathbf{z}+\mathbf{s})} \phi_N(qd\mathbf{y}+d\mathbf{z}+\mathbf{s})$ by the integral

$$\int_{\mathbf{y}\in\mathbb{R}^r} e^{2\pi i\beta\cdot\mathcal{F}(qd\mathbf{y}+d\mathbf{z}+\mathbf{s})} \phi_N(qd\mathbf{y}+d\mathbf{z}+\mathbf{s})\, d\mathbf{y},$$

is $O(N^{n-1+2\kappa+\eta}) + O((N/dq)^{n-1})$. By a change of variables $\mathbf{y} := N^{-1}(qd\mathbf{y} + d\mathbf{z} + s)$ we have

$$\int_{\mathbf{y}\in\mathbb{R}^r} e^{2\pi i\beta\cdot\mathcal{F}(qd\mathbf{y}+d\mathbf{z}+\mathbf{s})} \phi_N(qd\mathbf{y}+d\mathbf{z}+\mathbf{s})\, d\mathbf{y} = N^n d^{-n} q^{-n} I(N^k\beta).$$

Summing over $\mathbf{z} \in \mathbb{Z}_q^n$, using (4.21) and (4.8) proves (4.19). ◻

For $\mu \in \mathbb{R}^r$ and $\Phi > 0$, write

$$J(\mu;\Phi) := \int_{|\gamma_i|\leq\Phi} I(\gamma)\, e^{-2\pi i \gamma\cdot\mu}\, d\gamma,$$

and define

$$J(\mu) := \lim_{\Phi\to\infty} J(\mu;\Phi). \tag{4.22}$$

By Lemma 5.2 and Lemma 5.3 in [3], $J(\mu)$ exists, continuous and uniformly bounded by

$$\int_{\mathbb{R}^r} |I(\gamma)|\, d\gamma < \infty.$$

Also using assumption (4.9) and estimate (4.10) we have that the so-called *singular series*

$$\mathfrak{S}(d,\mathbf{s};\mathbf{v}) := \sum_{q=1}^{\infty} \sum_{(\mathbf{a},q)=1} q^{-n} e^{-2\pi i \frac{\mathbf{a}\cdot\mathbf{v}}{q}} S_{\mathbf{a},q}(d,\mathbf{s}) \tag{4.23}$$

is absolute convergent. In fact,

$$\sum_{q\geq N_1^{\kappa}} \sum_{(\mathbf{a},q)=1} q^{-n} |S_{\mathbf{a},q}(d,\mathbf{s})| \lesssim N^{-\delta}. \tag{4.24}$$

Indeed, as $\kappa = r(k-1)\theta_0$ we have by assumption (4.10)

$$\frac{2\delta}{\kappa} < \frac{K}{(1+\varepsilon)r(k-1)} - r - 1.$$

Then by estimate (4.9)

$$\sum_{q\geq N_1^{\kappa}} \sum_{(\mathbf{a},q)=1} q^{-n} |S_{\mathbf{a},q}(d,\mathbf{s})| \lesssim_{\tau} \sum_{q\geq N_1^{\kappa}} q^{-\frac{2\delta}{\kappa}+\tau} \lesssim_{\tau} N_1^{-2\delta+\tau} \lesssim_{\tau} N^{-2\delta+\delta\eta+\tau} \lesssim N^{-\delta}.$$

Summarizing we have

Proposition 4.1. *Let $\mathcal{F} = (F_1,\ldots,F_r)$ be a family of integral forms of degree k satisfying the rank condition*

$$K := \frac{codim\, V_{\mathcal{F}}^*}{2^{k-1}} > r(r+1)(k-1). \tag{4.25}$$

There exists a constant $\delta' = \delta'(k,r) > 0$ such that the following holds.

(i) If $0 < \eta \leq \frac{1}{4r^2(r+1)(r+2)k^2}$ then for every $1 \leq d \leq N^{\frac{\eta}{1+\eta}}$ and $\mathbf{s} \in \mathbb{Z}^n$ one has the asymptotic

$$\mathcal{R}_N(d,\mathbf{s};\mathbf{v}) = N^{n-rk} d^{-n} \mathfrak{S}(d,\mathbf{s},\mathbf{v})\, J(N^{-k}\mathbf{v}) \;+\; O(N^{n-rk-\delta'} d^{-n}). \tag{4.26}$$

(ii) Moreover if

$$K > 2r(r+1)(k-1) + 2rk, \tag{4.27}$$

then the asymptotic formula (4.26) holds for $\eta \leq \frac{1}{4r(r+2)k}$.

Proof. First we show that if $0 < \varepsilon \le 1$ satisfies $\varepsilon < \frac{K}{r(r+1)(k-1)} - 1$ and $\eta > 0$ is such that

$$\eta < \frac{1}{4r(r+2)k} \ \min\left\{\varepsilon,\ \frac{K-(1+\varepsilon)r(r+1)(k-1)}{rk(1+\varepsilon)}\right\}, \tag{4.28}$$

then (4.26) holds for $1 \le d \le N^{\frac{\eta}{1+\eta}}$ and $\mathbf{s} \in \mathbb{Z}^n$.

Set the parameters θ_0 and δ as

$$\theta_0 := \frac{1}{2r(r+2)k+1}\ ,\quad \delta := \frac{\theta_0}{2}\min\left\{1,\ \frac{K}{1+\varepsilon} - r(r+1)(k-1)\right\},$$

to satisfy conditions (4.11) and (4.12). Then for

$$\eta < \frac{1}{4r(r+2)k} \ \min\left\{\varepsilon,\ \frac{K-(1+\varepsilon)r(r+1)(k-1)}{rk(1+\varepsilon)}\right\},$$

we have that $\eta < \varepsilon(1-k^{-1}\theta_0$ and $\eta < \theta_0 k^{-1}r^{-1}$ hence both the conditions of Lemma 4.5 and (4.14) are fulfilled.

Thus by (4.16), (4.19), (4.24) and using the fact that $|\mathcal{M}'(\theta_0)| \le N_1^{(r+1)\kappa - rk + r\eta} \le N^{-rk+\frac{2}{3}}$ (by our choice of $\theta_0,\ \eta$), we have that

$$\begin{aligned}
\mathcal{R}_N(d,\mathbf{s},\mathbf{v}) &= \sum_{q\le N_1^\kappa}\sum_{\mathbf{a}}\int_{\mathcal{M}'_{\mathbf{a},q}(\theta_0)} e^{-2\pi i\,\alpha\cdot\mathbf{v}} S_N(d,\mathbf{s};\alpha)\,d\alpha \ +\ O(N^{n-rk-\delta'}d^{-n})\\
&= N^n d^{-n}\left(\sum_{q\le N_1^\kappa} q^{-n}e^{-2\pi i\,\frac{\mathbf{a}\cdot\mathbf{v}}{q}} S_{\mathbf{a},q}(d,\mathbf{s})\int_{|\beta_i|\le N_1^{-k+\kappa}} e^{-2\pi i\beta\cdot\mathbf{v}} I(N^k\beta)\,d\beta \ +\ O(N^{-rk-\frac{1}{3}+2\kappa+\eta})\right)\\
&= N^{n-rk}d^{-n}\left(\sum_{q\le N_1^\kappa} q^{-n}e^{-2\pi i\,\frac{\mathbf{a}\cdot\mathbf{v}}{q}} S_{\mathbf{a},q}(d,\mathbf{s})J(N^{-k}\mathbf{v};d^kN_1^\kappa) + O(N^{-\delta'})\right)\\
&= N^{n-rk}d^{-n}\ \mathfrak{S}(d,\mathbf{s};\mathbf{v})J(N^{-k}\mathbf{v}) \ +\ O(N^{n-rk-\delta'}d^{-n}),
\end{aligned} \tag{4.29}$$

for some $\delta' = \delta'(r,k) > 0$.

Indeed, the first line is (4.16), the second line follows from (4.19) and the above remark on the size of the major arcs, the third line by a scaling $\beta := N^k\beta$ and the last line from (**??**) and (4.24) together with the estimate $2\kappa + \eta \le \frac{k-1}{k(r+2)} + \frac{1}{4r(r+2)k} \le \frac{1}{r+2}(1-\frac{3}{4k}) < \frac{1}{3}$.

If $K > r(r+1)(k-1)$ then $\frac{K}{r(r+1)(k-1)} - 1 \ge \frac{1}{r(r+1)(k-1)}$ thus one may choose ε slightly larger than $\frac{1}{r(r+1)k}$. This gives $\eta \le \frac{1}{4r^2(r+1)(r+2)k^2}$ by (4.28). If $K > 2r(r+1)(k-1)+2rk$ then one may choose ε slightly larger than 1, which gives $\eta \le \frac{1}{4r(r+2)k}$. This proves the Proposition. □

Finally, consider the singular series

$$\mathfrak{S}(d,\mathbf{s},\mathbf{v}) = \sum_{q=1}^{\infty} q^{-n}\sum_{(\mathbf{a},q)=1} e^{-2\pi i\frac{\mathbf{a}\cdot\mathbf{v}}{q}} S_{\mathbf{a},q}(d,\mathbf{s}), \tag{4.30}$$

where writing $\mathcal{F}_{d,\mathbf{s}}(\mathbf{x}) := \mathcal{F}(d\mathbf{x}+\mathbf{s})$

$$S_{\mathbf{a},q}(d,\mathbf{s}) = \sum_{\mathbf{x}\in\mathbb{Z}_q^n} e^{2\pi i\frac{\mathcal{F}_{d,\mathbf{s}}(\mathbf{x})\cdot a}{q}}.$$

By the well-known multiplicative properties of the inner sums in (4.30)

$$\mathfrak{S}(d,\mathbf{s},\mathbf{v}) = \prod_{p\ prime} \sigma_p(d,\mathbf{s},\mathbf{v}),$$

with local factors

$$\sigma_p(d,\mathbf{s},\mathbf{v}) = \sum_{m=0}^{\infty} p^{-mn} \sum_{(\mathbf{a},p^m)=1} e^{-2\pi i \frac{\mathbf{a}\cdot\mathbf{v}}{p^m}} S_{\mathbf{a},p^m}(d,\mathbf{s}).$$

By estimate (4.9) and assumption (4.10) we have $\sigma_p(d,\mathbf{s},\mathbf{v}) = 1 + O(p^{-1-\delta'})$ and hence the product is absolutely and uniformly convergent. Finally, by a straightforward calculation we have

$$\sigma_p^l(d,\mathbf{s};\mathbf{v}) := \sum_{m=0}^{l} p^{-mn} \sum_{(\mathbf{a},p^m)=1} e^{-2\mathfrak{p}i \frac{\mathbf{a}\cdot\mathbf{v}}{p^m}} S_{\mathbf{a},p^m}(d,\mathbf{s}) = p^{-l(n-r)} \left|\{\mathbf{x} \in \mathbb{Z}_{p^l}^n;\ \mathcal{F}_{d,\mathbf{s}}(\mathbf{x}) = \mathbf{v}\}\right|. \tag{4.31}$$

Proposition 1.1 follows immediately from Proposition 4.1.

References

[1] A. Balog, *Linear equations in primes*, Mathematika 39.2 (1992): 367-378

[2] J. Bourgain, A. Gamburd, P. Sarnak *Affine linear sieve, expanders, and sum-product*, Invent. Math. 179, (2010): 559-644

[3] B. Birch, *Forms in many variables*, Proc. Royal Soc. London. Ser. A. 265/1321 (1962): 245-263.

[4] J. Brdern,J. Dietmann,J. Liu,T. Wooley *A Birch-Goldbach theorem* Archiv der Mathematik, 94(1), (2010): 53-58

[5] J. Brdern, *A sieve approach to the Waring-Goldbach problem II. On the seven cubes theorem.* Acta Arithmetica-Warszava, 72, (1995): 211-227.

[6] B. Cook, A. Magyar, *Diophantine equations in the primes*, Invent. Math. 198/3, (2014): 701-737

[7] B. Cook, A. Magyar, *On restricted arithmetic progressions over finite fields* Online J. Anal. Comb., v.7, (2012): 1-10

[8] S. Ghorpage and G. Lachaud *Etale cohomology, Lefshetz theorems and number of points of singular verieties over finite fields*, Moscow Math. J. (2) (2002), 589-631

[9] D. Goldston, Y. Motohashi, J. Pintz, J., C. Yildirim, *Small gaps between primes exist.* Proc. Japan Acad. Sci. Ser. A, 82.4 (2006): 61-65.

[10] D. Goldston, J. Pintz, Yildirim, *Primes in tuples I*, Ann. of Math. 170 (2009): 819-862

[11] B. Green and T. Tao, *The primes contain arbitrary long arithmetic progressions*, Annals of Math. 167 (2008), 481-547

[12] B. Green, T. Tao, *Linear equations in the primes*, Ann. of Math.(2) 171.3 (2010): 1753-1850.

[13] B. Green T. Tao, *Yet another proof of Szemerédi's theorem*, An irregular mind. Springer Berlin Heidelberg, (2010) 335-342.

[14] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics Vol. 52. Springer (1977)

[15] K. Henriot, *Logarithmic bounds for translation-invariant equations in squares.* International Mathematics Research Notices (2015): rnv062.

[16] L.K. Hua, *Additive theory of prime numbers*, Translations of Mathematical Monographs Vol. 13." Am. Math. Soc., Providence (1965).

[17] J. Liu, *Integral points on quadrics with prime coordinates*, Monats. Math. 164.4 (2011): 439-465.

[18] E. Keil, *Translation invariant quadratic forms in dense sets*, arXiv preprint arXiv:1308.6680 (2013).

[19] M.L. Smith, *On solution-free sets for simultaneous quadratic and linear equations.* Journal of the London Mathematical Society 79.2 (2009): 273-293.

[20] W. Duke, Z. Rudnick, P. Sarnak, *Density of integer points on affine homogeneous varieties*, Duke Math. J. 71.1 (1993): 143-179.

[21] K.F. Roth, *On certain sets of integers*, J. London Math. Soc. 1.1 (1953): 104-109.

[22] W. Schmidt, *The density of integral points on homogeneous varieties*, Acta Math. 154.3 (1985): 243-296.
[23] G. Shimura, *Reduction of algebraic varieties with respect to a discrete valuation of the basic field*, Amer. J. Math. (1955): 134-176.
[24] T. Tao, The prime tuples conjecture, sieve theory, and the work of Goldston-Pintz-Yildirim, Motohashi-Pintz, and Zhang, (2013)
[25] E.C. Titchmarsh, The theory of the Riemann zeta-function. v. 196. Oxford Univ. Press: Oxford, 1951.
[26] I.M. Vinogradov, *Representations of an odd integer as a sum of three primes* Goldbach Conjecture 4 (2002): 61.
[27] J. Liu, T. D. Wooley, and G. Yu *The quadratic WaringGoldbach problem.* Journal of number theory 107.2 (2004): 298-321.