Exponential sums and polynomial congruences in two variables: the quasi-homogeneous case

EXPONENTIAL SUMS AND POLYNOMIAL CONGRUENCES IN TWO VARIABLES: THE QUASI-HOMOGENEOUS CASE

JAMES WRIGHT

Abstract. We adapt ideas of Phong, Stein and Sturm and ideas of Ikromov and Müller from the continuous setting to various discrete settings, obtaining sharp bounds for exponential sums and the number of solutions to polynomial congruences for general quasi-homogeneous polynomials in two variables. This extends work of Denef and Sperber and also Cluckers regarding a conjecture of Igusa in the two dimensional setting by no longer requiring the polynomial to be nondegenerate with respect to its Newton diagram.

1. Introduction

Let $f \in \mathbb{Z}[X,Y]$ be a quasi-homogeneous polynomial in two variables by which we mean there exist two positive numbers $\kappa_1, \kappa_2 > 0$ so that $f(r^{\kappa_1}x, r^{\kappa_2}y) = rf(x,y)$ for every $r \geq 0$. Our goal is to give sharp uniform bounds on the exponential sums

$$\mathcal{S}(f;p^s) \;=\; \frac{1}{p^{2s}} \sum_{x \bmod p^s} \sum_{y \bmod p^s} e^{2\pi i f(x,y)/p^s}$$

where the parameter p^s is a power of a prime number p. We will also obtain precise estimates for the number of solutions to the polynomial congruence $f(x,y) = 0 \bmod p^s$.

We will be particularly interested in estimates of the form

$$|\mathcal{S}(f;p^s)| \;\leq\; Cs^{i(f)}p^{-s/h(f)} \tag{1}$$

and such uniform estimates will be proved for almost every prime p where C is an absolute constant depending only on the degree of f; that is, there is an exceptional finite set of primes $\mathcal{P}(f)$ and a constant $C = C_{\deg(f)}$ such that (1) holds for every $p \notin \mathcal{P}(f)$. In fact in almost every case the exponents $h(f)$ and $i(f)$ will be the same as those arising in the best uniform estimates for the corresponding euclidean oscillatory integrals

$$\left| \iint_{\mathbb{R}^2} e^{2\pi i \lambda f(x,y)} \phi(x,y)\,dxdy \right| \;\leq\; C\left[\log(|\lambda|)\right]^{i(f)} |\lambda|^{-1/h(f)} \tag{2}$$

where the *height* of f is defined as $h(f) := \sup_z\{d_z(f)\}$, the supremum being taken over all smooth local coordinate systems $z = (x,y)$ of the origin and d_z denotes the *Newton distance* of f in the coordinates z. See Section 2 for precise definitions of these notions as well as an explicit, intrinsic description of the height $h(f)$ when

1991 *Mathematics Subject Classification.* 11A07, 11L07, 11L40, 42B20.

f is a quasi-homogeneous polynomial (if $f(x,y) = ax^j y^k$ is single monomial, then $h(f) = \max(j,k)$ and when f consists of more than one monomial, the homogeneity dilation parameters κ_1, κ_2 are uniquely determined by f; in this case $h(f)$ can be described explicitly in terms of κ_1, κ_2 and the maximum multiplicity of the real roots of f). The exponent $i(f)$ is sometimes referred to as Varchenko's exponent or the *multiplicity of oscillation* of f and takes only the values 0 or 1; it is always equal to 0 except when $h(f) \geq 2$ and the *principal face* of f in *adapted coordinates*[1] is a vertex of the Newton diagram in which case we set $i(f) = 1$. Again, in Section 2 we will give precise definitions of these notions and an explicit, intrinsic description of the exponent $i(f)$. The estimate (2) is sharp in the sense that

$$\lim_{\lambda \to +\infty} \frac{\lambda^{1/h(f)}}{\log^{i(f)}(\lambda)} \iint_{\mathbb{R}^2} e^{2\pi i \lambda f(x,y)} \phi(x,y) dxdy \;=\; c\,\phi(0,0) \tag{3}$$

for some nonzero constant c if the support of ϕ is sufficiently small and if the principal face of f in adapted coordinates is a compact set. For proofs of (2) and (3), see for example [8] where these results are established for any smooth real-valued phase f of finite-type.

It turns out that the uniform estimates in (1), discrete analogues of (2), hold for every quasi-homogeneous polynomial $f \in \mathbb{Z}[X,Y]$ *except* for a single family of degenerate f of the form

$$f(x,y) \;\;=\;\; a(by^2 + cxy + dx^2)^m$$

where $m \geq 2$ and the quadratic polynomial $by^2 + cxy + dx^2$ is irreducible over the rationals $\mathbb{Q}$. In this case (1) holds with the same decay parameter $h(f)$ but now the $0-1$ valued exponent $i(f) = i_p(f)$ depends on the prime p. For example when $f(x,y) = a(y^2 - 2x^2)^m$ and $m \geq 2$, it turns out that $i_p(f) = 1$ when $p \equiv 1$ or 7 mod 8 and $i_p(f) = 0$ when $p \equiv 3$ or 5 mod 8.

We denote by E_m the class of functions $f(x,y) = a(by^2 + cxy + dx^2)^m$ with $by^2 + cxy + dx^2$ irreducible over $\mathbb{Q}$. Hence when $m \geq 2$, E_m is an exceptional class where the direct discrete analogue of the euclidean estimate (2) does not hold. When we turn to counting solutions of polynomial congruences, E_m will be an exceptional class for all $m \geq 1$. An explanation of how the classes E_m arise is given before the statement of Theorem 1.3 below.

We also obtain a version of (3) for $\mathcal{S}(f;p^s)$ in the following theorem.

Theorem 1.1. *For any quasi-homogeneous polynomial $f \in \mathbb{Z}[X,Y]$, there is a finite collection $\mathcal{P}(f)$ of prime numbers and constants $c, C > 0$, depending only on the degree of f, so that for every prime $p \notin \mathcal{P}(f)$ and f not in any exceptional class E_m with $m \geq 2$,*

$$|\mathcal{S}(f;p^s)| \;\leq\; Cs^{i(f)} p^{-s/h(f)}$$

holds and if furthermore $f(x) \neq ax + by$,

$$cs^{i(f)} p^{-s/h(f)} \;\leq\; |\mathcal{S}(f;p^s)| \tag{4}$$

holds for infinitely many $s \geq 1$.

[1] a local coordinate system z where the supremum defining the height is achieved; that is, $h(f) = d_z$

When f belongs to some E_m, $m \geq 2$, the above estimates still hold but now $i(f) = i_p(f)$ depends on p; more precisely $i_p(f) = 1$ or 0 depending on whether the roots of f (a conjugate pair of algebraic numbers of degree 2 over $\mathbb{Q}$) lie in the p-adic field $\mathbb{Q}_p$ or not, respectively.

When $f(x) = ax + by$ is linear such that either $p^s \not| a$ or $p^s \not| b$, then $\mathcal{S}(f; p^s) = 0$ and so no lower bound as in (4) holds in this case. The finite collection $\mathcal{P}(f)$ of exceptional primes which we will work with is a specific collection which we will describe precisely in Section 2.5 below. The sequence of $s \geq 1$ where the lower bound (4) holds can be chosen to depend only on f; more precisely, if f is not a single monomial, then there is a pair $1 \leq t \leq r$ of relatively prime integers, determined by the dilation parameters $\kappa_1, \kappa_2 > 0$, such that $f(x, y) = ax^\alpha y^\beta Q(x^r, y^t)$ for some homogeneous polynomial $Q(u, v)$ of degree $n \geq 1$; see Section 2 below. Then (4) holds for example for any $s \geq 1$ satisfying $s \equiv 0 \mod NM_1M_2P$ where $N = t\alpha + r\beta + rtn$, $M_1 = \gcd(\beta, \alpha + rn)$, $M_2 = \gcd(\alpha, \beta + tn)$ and P equals to the product of the multiplicities of the roots of Q.

For quasi-homogeneous polynomials $f \in \mathbb{Z}[X_1, \ldots, X_n]$ in arbitrary number of variables, Denef and Sperber [4] and Cluckers [1], [2] have established the estimate (1) when[2] f is nondegenerate with respect to its Newton diagram which is related to certain conjectures of Igusa found in [5] (we remark that any f in an exceptional class E_m for some $m \geq 2$ is degenerate with respect to its Newton diagram). The estimates in Theorem 1.1 extend their work in the two variable setting to arbitrary quasi-homogeneous polynomials. In fact in [4], Denef and Sperber make a conjecture for general homogeneous polynomials (extended to quasi-homogeneous polynomials by Cluckers) and Theorem 1.1 verifies this conjecture in the two variable setting. The lower bound (4) shows the general sharpness of the estimate with respect to p and s. Sharp estimates for arbitrary quasi-homogeneous polynomials have been obtained previously by Cluckers [3] in the case when $s = 1$ or $s = 2$, again for polynomials in any number of variables.

We turn our attention now to polynomial congruences. Whenever a pair of integers (x, y) satisfies the congruence $f(x, y) \equiv 0 \mod n$, then so does $(x + jn, y + kn)$ for any $(j, k) \in \mathbb{Z}^2$. Therefore a solution to the congruence $f \equiv 0 \mod n$ is defined to be an element in the ring $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ and if $\#\{f \equiv 0 \bmod n\}$ denotes the total number of solutions, we will examine the normalised number of solutions

$$\mathcal{N}(f; n) \ := \ n^{-2} \#\{f \equiv 0 \bmod n\}.$$

The quantity $\mathcal{N}(f; n)$ is a multiplicative function of n and so matters are reduced to studying $\mathcal{N}(f; p^s)$ for powers of a fixed prime p. Not surprisingly we obtain similar estimates for $\mathcal{N}(f; p^s)$ which are direct analogues of ones arising in euclidean sublevel set estimates which we will not write down explicitly. In the euclidean situation the decay parameter $h(f)$ remains the same but Varchenko's exponent needs slight modification: we define $\nu(f) = 0$ in every case except when the principal

[2]there is one exceptional case here; when $f(x, y) = ax(y - \zeta x^r)$ (or the symmetric example with x and y interchanged), $h(f) = 1$ and so $i(f) = 0$ but the bisectrix passes through the vertex $(1, 1)$ and so the estimates in [4] or [2], strictly speaking, carry a linear factor of s.

face of f in adapted coordinates is a vertex of the Newton diagram in which case we set $\nu(f) = 1$. So the only difference between $i(f)$ and $\nu(f)$ occurs when $h(f) < 2$.

Theorem 1.2. *For any quasi-homogeneous polynomial $f \in \mathbb{Z}[X,Y]$, there is a finite collection of prime numbers $\mathcal{P}(f)$ and constants $C, c, c' > 0$, depending only on the degree of f, so that for any $p \notin \mathcal{P}(f)$ and $f \notin E_m$ for any $m \geq 1$,*

$$cs^{\nu(f)}p^{-s/h(f)}p^{-2} \;\leq\; \mathcal{N}(f;p^s) \;\leq\; Cs^{\nu(f)}p^{-s/h(f)} \tag{5}$$

holds and

$$c's^{\nu(f)}p^{-s/h(f)} \;\leq\; \mathcal{N}(f;p^s) \tag{6}$$

holds for infinitely many $s \geq 1$.

When f lies in some E_m with $m \geq 1$, the estimates (5) *and* (6) *still hold but the exponent $\nu(f) = \nu_p(f)$ now depends on p; more precisely $\nu_p(f) = 1$ or 0 depending on whether the roots of f (a conjugate pair of algebraic numbers of degree 2 over $\mathbb{Q}$) lie in the p-adic field $\mathbb{Q}_p$ or not, respectively.*

Simple examples show that the factor p^{-2} in the lower bound in (5) cannot be replaced by p^{-1}; for instance if $f(x,y) = y^4 - 2x^6$, then $h(f) = 12/5$, $\nu(f) = 0$ and the analysis in Section 4 shows that $\mathcal{N}(f;p^s) \leq cp^{-5s/12}p^{-19/12}$ if $s \equiv 1 \bmod 12$ and either $p \equiv 3$ or $5 \bmod 8$. See Section 4.7 for details. Nevertheless there is a natural large class of quasi-homogeneous polynomials where the factor p^{-2} can be replaced by p^{-1}; see the comments after the statement of Theorem 1.3 below. When $f(x) = ax + by$ is linear, the situation of polynomial congruences differs from the situation of exponential sums. In this case, $\mathcal{N}(f;p^s) = p^{-s}$ if either $p \nmid a$ or $p \nmid b$, $h(f) = 1$ and $\nu(f) = 0$ so that (5) and (6) hold.

As we will see the proofs of Theorems 1.1 and 1.2 are very elementary, relying on a sharp structural statement for the solution set of general polynomial congruences of a single variable found in [15]; see also [16]. This result is a nonarchimedean version of a result of Phong, Stein and Sturm [13] about polynomial sublevel sets in euclidean spaces. The result in [15] is valid in general settings and Theorems 1.1 and 1.2 generalise accordingly.

Let $\mathfrak{o}$ be any ring endowed with a nontrivial discrete valuation $|\cdot|$ so that $|x| \leq 1$ for every $x \in \mathfrak{o}$. Let us suppose that the nonzero prime ideal $\mathfrak{p} := \{x \in \mathfrak{o} : |x| < 1\}$ is maximal in $\mathfrak{o}$ such that the localisation of $\mathfrak{o}$ to $\mathfrak{p}$ is the valuation ring $\{x \in K : |x| \leq 1\}$ of the field of fractions K of $\mathfrak{o}$ induced by $|\cdot|$. The valuation ring has a unique maximal ideal generated by a prime element π which may assume lies in $\mathfrak{o}$. We make the finiteness assumption that the residue class field $\mathfrak{o}/\mathfrak{p}$ is finite, say with $q = p^f$ elements where p is prime, and we normalise the valuation so that $|\pi| = q^{-1}$.

The maximality of $\mathfrak{p}$ implies that the fields $\mathfrak{o}/\mathfrak{p} \simeq \bar{\mathfrak{o}}/\pi\bar{\mathfrak{o}}$ are isomorphic where $\bar{\mathfrak{o}}$ denotes the completion of $\mathfrak{o}$ with respect to $|\cdot|$. Furthermore the field of fractions of $\bar{\mathfrak{o}}$ is $\bar{K}$, the completion of K with respect to $|\cdot|$, and the valuation extends uniquely to $\bar{K}$. Finally $\bar{\mathfrak{o}}$ is the valuation ring of $\bar{K}$ with respect to $|\cdot|$; that is, $\bar{\mathfrak{o}} = \{x \in \bar{K} : |x| \leq 1\}$.

Our finiteness hypothesis on the residue class field implies that $\bar{K}$ is a local field. Hence $\bar{K}$ is a finite field extension of the p-adic field $\mathbb{Q}_p$ (in the characteristic 0 case) or the field $\mathbb{F}_p((\pi))$ of Laurent series with coefficients in the field $\mathbb{F}_p$ of integers modulo p (in the positive characteristic case); in the latter case we can be more explicit, namely $\bar{K} = \mathbb{F}_q((\pi))$ where $q = p^f$ is defined above as the number of elements in the residue class field. If n is the degree of $\bar{K}$ over $\mathbb{Q}_p$ or $\mathbb{F}_p((\pi))$, then $n = ef$ where f, defined above, is the residual degree and the exponent e is the ramification index of this extension. In the characteristic 0 case, viewing $\mathbb{Z}$ as a subring of $\mathfrak{o}$ or $\bar{\mathfrak{o}}$, we have $p = \pi^e u$ for some unit u in $\bar{\mathfrak{o}}$.

Elements $x \in \bar{\mathfrak{o}}$ have a unique power series representation $x = \sum_{j \geq 0} x_j \pi^j$ with the x_j lying in a fixed set of representations of the elements of the residue class field $\bar{\mathfrak{o}}/\pi\bar{\mathfrak{o}}$. Like the prime element π, the representations $\{x_j\}$ in $\bar{\mathfrak{o}}$ of the residue class field can be chosen from the ring $\mathfrak{o}$ itself. For these elementary facts about discrete valuation rings, see for example [9] or [10].

The basic example is the ring of rational integers $\mathfrak{o} = \mathbb{Z}$ endowed with the p-adic valuation $|\cdot|_p$ for some prime p. This is the setting of Theorems 1.1 and 1.2. More generally one can consider any Dedekind domain $\mathfrak{o}$ with the finiteness property (FP) that the class fields $\mathfrak{o}/\mathfrak{p}$ are finite for all nonzero prime ideals $\mathfrak{p}$. In this setting each nonzero prime ideal $\mathfrak{p}$ is maximal and gives rise to a discrete valuation $|\cdot|_{\mathfrak{p}}$; in additive notation this valuation $\mathrm{ord}_{\mathfrak{p}}$ is defined on $\mathfrak{o}$ so that $\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(x)}$ is the $\mathfrak{p}$ factor in the prime ideal decomposition of the principal ideal $x\mathfrak{o}$ generated by $x \in \mathfrak{o}$. Furthermore the valuation ring $\{x \in K : |x|_{\mathfrak{p}} \leq 1\}$ of the field of fractions K of $\mathfrak{o}$ is the localisation of $\mathfrak{o}$ to $\mathfrak{p}$ and so we are in the setting described in the previous paragraphs.

We denote by $\bar{\mathfrak{o}}_{\mathfrak{p}}$ the completion of $\mathfrak{o}$ with respect to the valuation arising from $\mathfrak{p}$ and we denote by $\pi_{\mathfrak{p}} \in \mathfrak{o}$ the prime element generating the unique maximal ideal of $\bar{\mathfrak{o}}_{\mathfrak{p}}$. When the residue class field $\mathfrak{o}/\mathfrak{p}$ is finite, say with $q_{\mathfrak{p}}$ elements, then via the isomorphism $\mathfrak{o}/\mathfrak{p} \to \bar{\mathfrak{o}}_{\mathfrak{p}}/\pi_{\mathfrak{p}}\bar{\mathfrak{o}}_{\mathfrak{p}}$, we see that the multiplicative valuation $|x|_{\mathfrak{p}} := q_{\mathfrak{p}}^{-\mathrm{ord}_{\mathfrak{p}}(x)}$, extended uniquely to $\bar{\mathfrak{o}}_{\mathfrak{p}}$, is automatically normalised with $|\pi_{\mathfrak{p}}|_{\mathfrak{p}} = q_{\mathfrak{p}}^{-1}$ or $\mathrm{ord}_{\mathfrak{p}}(\pi_{\mathfrak{p}}) = 1$.

In the setting of Dedekind domains with the finiteness property (FP) many results from elementary number theory in $\mathbb{Z}$ have analogues in this more abstract setting; see for example [11]. In a similar way there are analogous results of Theorems 1.1 and 1.2. Instead of $f \in \mathbb{Z}[X, Y]$, we consider polynomials $f \in \mathfrak{o}[X, Y]$ where $\mathfrak{o}$ is any Dedekind domain with the finiteness property (FP). As before, a solution to the polynomial congruence $f \equiv 0 \bmod \mathfrak{i}$ where $\mathfrak{i}$ is a nonzero ideal of $\mathfrak{o}$, is defined to be an element in the class ring $\mathfrak{o}/\mathfrak{i}$ and this ring is finite by the finiteness property (FP). If we denote by $\|\mathfrak{i}\|$ the number of elements of $\mathfrak{o}/\mathfrak{i}$, we study the normalised number of solutions to the polynomial congruence $f \equiv 0 \bmod \mathfrak{i}$

$$\mathcal{N}(f, \mathfrak{i}) \ := \ \|\mathfrak{i}\|^{-2} \#\{f(x, y) \equiv 0 \bmod \mathfrak{i}\}.$$

If $\mathfrak{i} = \prod \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{i})}$ is the prime ideal decomposition of the ideal $\mathfrak{i}$, then basic isomorphism theorems show

$$\mathcal{N}(f, \mathfrak{i}) \ = \ \prod_{\mathfrak{p}|\mathfrak{i}} \mathcal{N}(f, \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{i})})$$

where $\mathcal{N}(f, \mathfrak{p}^s) = q_{\mathfrak{p}}^{-2s} \# \{ f \equiv 0 \bmod \mathfrak{p}^s \}$; see for example [10]. Therefore matters are reduced to the case when the ideal $\mathfrak{i} = \mathfrak{p}^s$ is a power of a fixed prime ideal $\mathfrak{p}$.

In this more abstract setting of Dedekind domains we also introduce and study character sums which are generalisations of the exponential sums $\mathcal{S}(f; p^s)$ over the integers $\mathbb{Z}$. For a fixed nonzero prime ideal $\mathfrak{p}$, we consider a nonprincipal additive character χ of the factor ring $\mathfrak{o}/\mathfrak{p}^s$ which we will assume to be a *primitive* character in the sense that there exists an element $y \in \mathfrak{o}$ with $|y|_{\mathfrak{p}} = q_{\mathfrak{p}}^{-s+1}$ and so that $\chi(y + \mathfrak{p}^s) \neq 1$ (if no such element exists, then χ would restrict to a nonprincipal character of the factor ring $\mathfrak{o}/\mathfrak{p}^{s-1}$). For an $f \in \mathfrak{o}[X, Y]$ (which by reducing the coefficients mod $\mathfrak{p}^s$, we may view f as a polynomial with coefficients in $\mathfrak{o}/\mathfrak{p}^s$), we set

$$\mathcal{S}_{\chi}(f; \mathfrak{p}^s) \ := \ q_{\mathfrak{p}}^{-2s} \sum_{(x,y) \in [\mathfrak{o}/\mathfrak{p}^s]^2} \sum \chi(f(x, y))$$

and, as in the setting of $\mathfrak{o} = \mathbb{Z}$, our main interest will be to obtain bounds for $\mathcal{S}_{\chi}(f; \mathfrak{p}^s)$ and $\mathcal{N}(f; \mathfrak{p}^s)$ which are uniform over all nonzero prime ideals $\mathfrak{p}$ and exponents s when $f \in \mathfrak{o}[X, Y]$ is a quasi-homogeneous polynomial; that is, f satisfies $f(r^{\kappa_1} x, r^{\kappa_2} y) = r f(x, y)$ for some positive numbers $\kappa_1, \kappa_2 > 0$.

We now introduce the height $h(f)$ and Varchenko's exponents $i(f)$ and $\nu(f)$ but appeal to the explicit description of these parameters alluded to above, avoiding the original definitions in terms of local coordinates. When $f(x, y) = a x^{\alpha} y^{\beta}$ consists of a single monomial, we set as before $h(f) = \max(\alpha, \beta)$. Furthermore we set $i(f) = \nu(f) = 0$ when $\alpha \neq \beta$, $\nu(f) = 1$ when $\alpha = \beta$ and $i(f) = 1$ if $\alpha = \beta \geq 2$ but $i(f) = 0$ when $f(x, y) = axy$. When f consists of more than one monomial, then κ_1 and κ_2 are uniquely determined by f (see Lemma 2.1 below); of course there is a continuum of choices for κ_1 and κ_2 when f is a single monomial. Recall that K denotes the field of fractions of $\mathfrak{o}$ and by $\bar{K}_{\mathfrak{p}}$, we denote the field of fractions of $\bar{\mathfrak{o}}_{\mathfrak{p}}$. If $\mathfrak{o} = \mathbb{Z}$ and $\mathfrak{p} = p\mathbb{Z}$ for some prime p, then $K = \mathbb{Q}$ and $\bar{K}_{\mathfrak{p}} = \mathbb{Q}_p$.

Suppose now that f consists of more than one monomial. We will see that the zero set $\{f(x, y) = 0\}$ of f over some field extension of K is a finite union of algebraic curves or *roots of* f which can be enumerated by a certain sequence of algebraic elements $\{\zeta_j\}$ over K, each *root* ζ_j comes with an associated multiplicity or order n_j. We define $m_K(f) := \max\{n_j : \zeta_j \in K\}$, the maximal order of the roots of f over K, and following [7], we call $d(f) := (\kappa_1 + \kappa_2)^{-1}$ the *homogeneous distance* of f. Finally (as in [7]) we define the height of f as

$$h(f) \ := \ \max(m_K(f), d(f)).$$

In Section 2, we will see that when $\mathfrak{o} = \mathbb{Z}$, this definition of height coincides with the euclidean definition in terms of the supremum of Newton distances. In fact a result of Ikromov and Müller in [7] shows that in the euclidean setting, the original definition of the height $h(f)$ is equal $\max(m_{\mathbb{R}}(f), d(f))$ when $f \in \mathbb{R}[X, Y]$ is any quasi-homogeneous polynomial with real coefficients. Here $m_{\mathbb{R}}(f)$ is the maximal

order of the roots of f over $\mathbb{R}$, instead of being over $K = \mathbb{Q}$, and therefore larger than $m_{\mathbb{Q}}(f)$ when $f \in \mathbb{Z}[X, Y]$. Nevertheless taking the maximum with the homogeneous distance $d(f)$ is the same; that is $h(f)$ is unchanged, $h(f) = \max(m_{\mathbb{Q}}(f), d(f)) = \max(m_{\mathbb{R}}(f), d(f))$. See Section 2 for details.

Another result of Ikromov and Müller shows that the Varchenko exponent $\nu(f)$ is equal to 0 if $m_{\mathbb{R}}(f) \neq d(f)$ and $\nu(f) = 1$ if $m_{\mathbb{R}}(f) = d(f)$ when $f \in \mathbb{R}[X, Y]$ is quasi-homogeneous (we recall that the difference between $\nu(f)$ and $i(f)$ occurs only when $h(f) < 2$). We will see in Section 2 that in the setting of $\mathfrak{o} = \mathbb{Z}$, the dichotomy $m_{\mathbb{R}}(f) = d(f)$ or $m_{\mathbb{R}}(f) \neq d(f)$ which determines the exponents $i(f)$ and $\nu(f)$ is exactly the same as $m_{\mathbb{Q}}(f) = d(f)$ or $m_{\mathbb{Q}}(f) \neq d(f)$ for every quasi-homogeneous polynomial $f \in \mathbb{Z}[X, Y]$ except for the classes E_m. This explains how the exceptional class E_m arises and indicates why the exponent of the linear factor s in (1) depends on the prime p for these special polynomials.

In the abstract setting of Dedekind domains $\mathfrak{o}$, we define $\nu(f) = 0$ if $m_K(f) \neq d(f)$ and $\nu(f) = 1$ if $m_K(f) = d(f)$. Furthermore we set $i(f) = \nu(f)$ except when $h(f) < 2$ where we always set $i(f) = 0$. As in Theorems 1.1 and 1.2, we obtain uniform estimates for $\mathcal{N}(f; \mathfrak{p}^s)$ and $\mathcal{S}_\chi(f; \mathfrak{p}^s)$ except when $f(x, y) = a(bx^2 + cxy + dy^2)^m$ for some $m \geq 1$ and where the quadratic polynomial $bx^2 + cxy + dy^2$ is irreducible over K (the exceptional classes E_m are restricted to $m \geq 2$ for the character sum $\mathcal{S}_\chi$). We will continue to refer to these exceptional classes as E_m.

Theorem 1.3. *Let $f \in \mathfrak{o}[X, Y]$ be a quasi-homogeneous polynomial with coefficients lying in a Dedekind domain $\mathfrak{o}$ with property (FP). If the characteristic of $\mathfrak{o}$ is positive, we assume that it is larger than the degree of f. Then there is a finite collection $\mathcal{P}(f)$ of prime ideals of $\mathfrak{o}$ and constants $c', c, C > 0$, depending only on the degree of f, so that for any f not in any exceptional class E_m (and $m \geq 2$ for $\mathcal{S}_\chi$),*

$$|\mathcal{S}_\chi(f; \mathfrak{p}^s)| \ \leq \ C s^{i(f)} q_{\mathfrak{p}}^{-s/h(f)} \tag{7}$$

and

$$c\, s^{\nu(f)} q_{\mathfrak{p}}^{-s/h(f)} q_{\mathfrak{p}}^{-2} \ \leq \ \mathcal{N}(f; \mathfrak{p}^s) \ \leq \ C s^{\nu(f)} q_{\mathfrak{p}}^{-s/h(f)} \tag{8}$$

hold for every nonzero prime ideal $\mathfrak{p} \notin \mathcal{P}(f)$ and $s \geq 1$. Furthermore for $\mathfrak{p} \notin \mathcal{P}(f)$,

$$c'\, s^{\nu(f)} q_{\mathfrak{p}}^{-s/h(f)} \ \leq \ \mathcal{N}(f; \mathfrak{p}^s) \tag{9}$$

and, if also $f(x) \neq ax + by$,

$$c'\, s^{i(f)} q_{\mathfrak{p}}^{-s/h(f)} \ \leq \ |\mathcal{S}_\chi(f; \mathfrak{p}^s)| \tag{10}$$

hold for infinitely many $s \geq 1$.

When f belongs to some class E_m (and $m \geq 2$ for $\mathcal{S}_\chi$), the estimates (7), (8), (9) and (10) still hold but now the exponents $i_{\mathfrak{p}}(f), \nu_{\mathfrak{p}}(f)$ depend on the prime ideal $\mathfrak{p}$; precisely, if $m \geq 2$, then $i_{\mathfrak{p}}(f) = \nu_{\mathfrak{p}}(f) = 1$ or 0 depending on whether the two conjugate roots of f lie in $\bar{K}_{\mathfrak{p}}$ or not, respectively. If $m = 1$, then E_1 is **not** *an exceptional class for character sums (we have $i(f) = 0$ when $f \in E_1$) but it is an exceptional class for the problem of polynomial congruences; in this case $\nu_{\mathfrak{p}}(f)$ depends on the prime ideal $\mathfrak{p}$ and is defined as in the case $m \geq 2$.*

As we have already mentioned, there are simple examples which show that the factor $q_{\mathfrak{p}}^{-2}$ in the lower bound in (8) cannot be replaced by $q_{\mathfrak{p}}^{-1}$. However if $m_K(f) \geq d(f)$, then the factor $q_{\mathfrak{p}}^{-2}$ in (8) can be replaced by $q_{\mathfrak{p}}^{-1}$.

In the generality of Theorem 1.3, Cluckers [2] has proved the main estimate (7) for quasi-homogeneous polynomials in any number of variables which are non-degenerate with respect to the Newton diagram (and in [3] for general quasi-homogeneous polynomials when $s = 1$ or $s = 2$). In fact we will appeal to Cluckers' result for certain cases when $h(f) < 2$. Alternatively one can use more precise finite field character sum estimates at the appropriate places in the arguments below.

Acknowledgement: We wish to thank Tony Carbery for some motivating discussions at the beginning of these investigations. Also we would like to thank Ben Lichtin for comments leading to a more precise formulation of the main results.

2. Notation and preliminaries

For any polynomial $g \in \mathfrak{o}[X, Y]$, $g(x, y) = \sum_{j,k} c_{j,k} x^j y^k$, we call the set $S(g) := \{(j, k) \in \mathbb{N}^2 : c_{j,k} \neq 0\}$, the support of g. The *Newton polyhedron* $\Delta(g)$ of g is the convex hull of the union of all quadrants $(j, k) + \mathbb{R}^2_+$ in $\mathbb{R}^2$ with $(j, k) \in S(g)$. If we use coordinates (t_1, t_2) for points in the plane containing the Newton polyhedron, consider the point (d_*, d_*) in this plane where the bisectrix $t_1 = t_2$ intersects the boundary of $\Delta(g)$. The coordinate d_* is called the Newton distance of g in the coordinates $z = (x, y)$.

We turn our attention to quasi-homogeneous polynomials $f \in \mathfrak{o}[X, Y]$ so that $f(r^{\kappa_1} x, r^{\kappa_2} y) = r f(x, y)$ for some positive $\kappa_1, \kappa_2 > 0$ and all $r \geq 0$. When $f(x, y) = a x^\alpha y^\beta$ is a single monomial, the conclusions of Theorem 1.3 are easily verified in this case. For the convenience of the reader we give the simple analysis in an appendix, see Section 6. Therefore from now on (until the last section), we assume that f consists of more than one monomial. In this case, it turns out that the dilation parameters κ_1 and κ_2 are uniquely determined by f.

Recall that $d(f) = (\kappa_1 + \kappa_2)^{-1}$ is the homogeneous distance of f and without loss of generality we will assume $\kappa_2 \geq \kappa_1$. We record in the following lemma some elementary facts about quasi-homogeneous polynomials observed in [7].

Lemma 2.1. *Let f be a quasi-homogeneous polynomial with dilation parameters $\kappa_1, \kappa_2 > 0$ satisfying $\kappa_2 \geq \kappa_1$ and consisting of more than one monomial. Then the exponents $\kappa_1 = t/m$, $\kappa_2 = r/m$ are rational numbers, uniquely determined by f with $gcd(r, t) = gcd(r, t, m) = 1$ (the condition $\kappa_2 \geq \kappa_1$ means $r \geq t \geq 1$). Furthermore $f(x, y) = x^\alpha y^\beta Q(x^r, y^t)$ for some homogeneous polynomial $Q \in \mathfrak{o}[X, Y]$,*

$$Q(w_1, w_2) \;=\; a w_2^n + c_{n-1} w_2^{n-1} w_1 + \cdots + c_1 w_2 w_1^{n-1} + b w_1^n$$

with $a, b \neq 0$. Factoring $Q(1,w) = a\prod_{j=1}^{M}(w-\zeta_j)^{n_j}$ with respect to its distinct roots $\{\zeta_j\}$ lying in some extension field L of K, we may write

$$f(x,y) \;=\; ax^{\alpha}y^{\beta}\prod_{j=1}^{M}(y^t-\zeta_j x^r)^{n_j}. \tag{11}$$

Setting $n := \sum_{j=1}^{M} n_j$, we have

$$d(f) \;=\; \frac{1}{\kappa_1+\kappa_2} \;=\; \frac{t\alpha+r\beta+trn}{t+r}.$$

We set $m_K(f) := \max(\alpha,\beta,\max(n_j : \zeta_j \in K))$ and $h(f) := \max(m_K(f), d(f))$. If $\beta > 0$, we introduce the index $j = 0$ and set $\zeta_0 = 0$ and $n_0 = \beta$. We call the collection $\{\zeta_j\}_{j=0}^{M}$ the *roots* of f.

We have the following relationship between the multiplicities $n_j, 0 \leq j \leq M$ and the homogeneous distance $d(f)$; the analogous result when $K = \mathbb{R}$ was observed in [7], the extension to general fields K being straightforward.

Lemma 2.2. *Let f be a quasi-homogeneous polynomial with dilation parameters $\kappa_1, \kappa_2 > 0$ satisfying $\kappa_2 \geq \kappa_1$. We use the notation introduced above (our underlying assumption that f is not a monomial remains in force).*

1. *If there is a multiplicity $n_{j_*} > d(f)$ for some $0 \leq j_* \leq M$, then all the other multiplicities must be* **strictly** *less than $d(f)$; that is $n_j < d(f)$ for all $0 \leq j \neq j_* \leq M$. In particular, there is at most one multiplicity $n_j,\ 0 \leq j \leq M$ with $n_j > d(f)$.*
2. *If $\kappa_2/\kappa_1 \notin \mathbb{N}$ (that is, $t \geq 2$), then $n = \sum_{j=1}^{M} n_j < d(f)$.*
3. *If $\kappa_2/\kappa_1 \in \mathbb{N}$, then $n_j \leq d(f)$ for every $1 \leq j \leq M$ with $\zeta_j \notin K$ (these are the roots of f with degree at least two with respect to K).*

   So necessarily, if there is a multiplicity $n_j > d(f)$ (unique by (1)), it must correspond to a root $\zeta_j \in K$.
4. *Finally, if there is a multiplicity n_j corresponding to a root $\zeta_j \notin K$ such that $n_j = d(f)$, then f must lie in an exceptional class E_m for some $m \geq 1$.*

   Therefore outwith the special class of polynomials f in E_m, all multiplicities n_j corresponding to a root $\zeta_j \notin K$, necessarily satisfy $n_j < d(f)$.

Proof Suppose $n_{j_1} > n_{j_2} \geq d(f)$ for two multiplicities n_{j_1}, n_{j_2} with $0 \leq j_1 \neq j_2 \leq M$. Then

$$d(f) \;\geq\; \frac{r(\beta+tn)}{r+t} \;>\; \frac{rd(f)+rtd(f)}{r+1} \;=\; d(f)\frac{r(1+t)}{r+t} \;\geq\; d(f) \tag{12}$$

which is a contradiction. This proves (1).

If $t \geq 2$, then $r > t \geq 2$ so that $\frac{1}{r} + \frac{1}{t} < 1$ and hence

$$d(f) \;\geq\; \frac{rtn}{r+t} > n$$

which proves (2).

To prove (3) we must show that $n_j \leq d(f)$ for every $1 \leq j \leq M$ with $\zeta_j \notin K$. This simply follows from the fact that the conjugates of any ζ_{j_0} over K lie among the roots $\{\zeta_j\}_{j=1}^M$ and any conjugate ζ_j of ζ_{j_0} must have the same multiplicity; that is, $n_j = n_{j_0}$. Finally if the degree of ζ_{j_0} is at least two, then there exists a conjugate of ζ_{j_0} distinct from itself and so if $n_{j_0} > d(f)$, one arrives at a contradiction as in (12).

Finally to prove (4), we first observe by (2) that necessarily $\kappa_2/\kappa_1 \in \mathbb{N}$ and so $t = 1$. If $n_j = d(f)$ is a multiplicity corresponding to a root $\zeta_j \notin K$, then the degree of ζ_j over K is at least two and so there is a conjugate $\zeta_{j'}$ of ζ_j with $j \neq j'$ and $n_j = n_{j'}$. Therefore

$$\frac{2rd(f)}{r+1} \;=\; \frac{r(n_j + n_{j'})}{r+1} \;\leq\; d(f)$$

which implies that $r = 1$. Now running the same argument again with $r = 1$, we obtain

$$d(f) \;=\; \frac{(n_j + n_{j'})}{2} \;\leq\; \frac{\alpha + \beta + (n_j + n_{j'} + n')}{2} \;=\; d(f)$$

where $n' = n - n_j - n_{j'}$. This gives a contradiction if there is a strict inequality above and so we conclude that necessarily $\alpha = \beta = n' = 0$ which implies that f is of the form E_m for some $m \geq 1$.

■

2.3. **The height $h(f)$.** For real quasi-homogeneous polynomials $f \in \mathbb{R}[X, Y]$, it was shown in [8] that $m_{\mathbb{R}}(f) := \max(\alpha, \beta, \max(n_j : \zeta_j \in \mathbb{R})) = \sup_z d_z$ where $\sup_z d_z$ is the supremum of the Newton distances of f over all smooth local coordinate systems z and was introduced in the previous section as the definition of the *height* for real-valued functions f. Now when $\mathfrak{o} = \mathbb{Z}$, $K = \mathbb{Q}$ and $f \in \mathbb{Z}[X, Y]$ is quasi-homogeneous, we see from Lemma 2.2 that $\max(m_{\mathbb{Q}}(f), d(f)) = \max(m_{\mathbb{R}}(f), d(f))$. In fact if $m_{\mathbb{R}}(f) > d(f)$, then by part (3) of Lemma 2.2, the unique multiplicity $n_j > d(f)$ must correspond to a root $\zeta_j \in \mathbb{Q}$. Hence our definition of height as $\max(m_{\mathbb{Q}}(f), d(f))$ agrees with usual definition $\sup_z d_z$ when $f \in \mathbb{Z}[X, Y]$ is quasi-homogeneous.

2.4. **The Varchenko exponents $i(f)$ and $\nu(f)$.** In the introduction we defined the Varchenko exponent $\nu(f)$ as 1 when $m_K(f) = d(f)$ and zero otherwise. Furthermore the exponent $i(f) = \nu(f)$ whenever $h(f) \geq 2$ and we set $i(f) = 0$ when $h(f) < 2$.

As we mentioned in the introduction, Ikromov and Müller [8] showed that the above definition of $\nu(f)$ in the setting $K = \mathbb{R}$ is equivalent to the original definition in terms of when the principal face of f in adapted coordinates is a vertex of the Newton diagram. Now when $\mathfrak{o} = \mathbb{Z}$ and $f \in \mathbb{Z}[X, Y]$ is quasi-homogeneous, we have already noted that the implication $m_{\mathbb{R}}(f) \neq d(f) \Rightarrow m_{\mathbb{Q}}(f) \neq d(f)$ follows from Lemma 2.2 part (c). Furthermore Lemma 2.2 part (d) shows that the implication $m_{\mathbb{R}}(f) = d(f) \Rightarrow m_{\mathbb{Q}}(f) = d(f)$ holds when f does not belong to the exceptional class E_m. Therefore outwith these exceptional classes E_m, the dichotomy $m_{\mathbb{R}}(f) =$

$d(f)$ or $m_{\mathbb{R}}(f) \neq d(f)$ is the same as $m_{\mathbb{Q}}(f) = d(f)$ or $m_{\mathbb{Q}}(f) \neq d(f)$ and so in the setting of $\mathfrak{o} = \mathbb{Z}$, the definition of the Varchenko exponents agrees with the usual definition.

2.5. **The exceptional set $\mathcal{P}(f)$ of primes ideals in Theorem 1.3.** For a fixed nonzero prime ideal $\mathfrak{p}$ of $\mathfrak{o}$, we will analyse $\mathcal{S}_\chi(f;\mathfrak{p}^s)$ and $\mathcal{N}(f;\mathfrak{p}^s)$ via the $\mathfrak{p}$-adic valuation $|\cdot|_\mathfrak{p}$ on the field K, defined in the introduction. In our analysis a finite collection $\mathcal{A}$ of algebraic elements over K depending only on f arise naturally in our estimates. At present we will not attempt to write the complete list $\mathcal{A}$ except to note that it includes the roots $\{\zeta_j\}_{j\geq 1}$ of f, differences of the roots $\{\zeta_j - \zeta_k\}_{j\neq k}$ and the leading coefficient a in Q defining f, introduced above. From time to time we will add to it but in the end $\mathcal{A}$ will consist of finitely many algebraic elements over K, depending only on f. The algebraic elements in $\mathcal{A}$ all live in some algebraic closure K^{alg} of K and for each valuation $|\cdot|_\mathfrak{p}$ on K there are many ways to extend it to a valuation on K^{alg}. For each prime ideal $\mathfrak{p}$ and element $\xi \in K^{alg}$, we make the following canonical choice for $|\xi|_\mathfrak{p}$: embed K^{alg} into an algebraic closure $\bar{K}_\mathfrak{p}^{alg}$ of $\bar{K}_\mathfrak{p}$ via an isomorphism over K. There is a unique way of extending the valuation $|\cdot|_\mathfrak{p}$ on K to $\bar{K}_\mathfrak{p}^{alg}$ via $\bar{K}_\mathfrak{p}$ and for $\xi \in K^{alg}$, we set $|\xi|_\mathfrak{p}$ to be the value of this extended valuation on the image ξ' of ξ under this embedding. For notational convenience, we will identify K^{alg} with its embedded image over K in $\bar{K}_\mathfrak{p}^{alg}$ from now on.

More precisely it is the $\mathfrak{p}$-adic valuations $|\cdot|_\mathfrak{p}$ of the elements in $\mathcal{A}$ which appear in our estimates. The important observation here is that there are only finitely many prime ideals $\mathcal{P}(f)$ of $\mathfrak{o}$, depending only on these algebraic elements over K (and hence depends only on f), so that $|\xi|_\mathfrak{p} = 1$ for all $\mathfrak{p} \notin \mathcal{P}(f)$ and every $\xi \in \mathcal{A}$. To see this consider an algebraic element $\xi \in \mathcal{A}$ and its minimal polynomial $x^d + a_{d-1}x^{d-1} + \cdots + a_0$ over K so that each $a_j \in K$. Let $\mathcal{F}(\xi)$ denote all the prime ideals which arise in the prime ideal factorisation of one of the (fractional) principal ideals $a_j\mathfrak{o}$. If $\mathfrak{p} \notin \mathcal{F}(\xi)$, then $|a_j|_\mathfrak{p} = 1$ for every $0 \leq j \leq d-1$ with $a_j \neq 0$. Fix a $\mathfrak{p} \notin \mathcal{F}(\xi)$ and consider the conjugates $\xi_1, \xi_2, \ldots, \xi_r$ of ξ over K lying in K^{alg}. In the characteristic 0 case, $r = d$ and for each $s \geq 1$,

$$a_{d-s} \;=\; \pm \sum_{1\leq j_1<\cdots<j_s\leq d} \xi_{j_1}\xi_{j_2}\cdots\xi_{j_s}.$$

In the positive characteristic case, $d = rp^\mu$ for some $\mu \geq 0$ where p is the characteristic of K. Then for each $s \geq 1$,

$$a_{d-sp^\mu} \;=\; \pm\Big[\sum_{1\leq j_1<\cdots<j_s\leq r} \xi_{j_1}\xi_{j_2}\cdots\xi_{j_s}\Big]^{p^\mu}. \tag{13}$$

We combine the two cases below and use (13) in both cases, taking $\mu = 0$ in (13) for the characteristic 0 case.

We claim that $|\xi|_\mathfrak{p} = 1$. In fact if $|\xi_1|_\mathfrak{p} \geq |\xi_2|_\mathfrak{p} \geq \cdots \geq |\xi_r|_\mathfrak{p}$, then we must have equality $|\xi_1|_\mathfrak{p} = \cdots = |\xi_r|_\mathfrak{p}$ and hence $|\xi|_\mathfrak{p} = 1$ since $a_0 = \pm[\xi_1\cdots\xi_r]^{p^\mu}$. Suppose equality does not hold. Then $|\xi_1|_\mathfrak{p} = \cdots = |\xi_s|_\mathfrak{p} > |\xi_{s+1}|_\mathfrak{p} \geq \cdots \geq |\xi_r|_\mathfrak{p}$ for some $1 \leq s < r$ and hence $1 = |a_{d-sp^\mu}| = |\xi_1\cdots\xi_s|_\mathfrak{p}^{p^\mu}$ by the nonarchimedean nature of $|\cdot|_\mathfrak{p}$. In fact $|\xi_{j_1}\cdots\xi_{j_s}|_\mathfrak{p} < |\xi_1\cdots\xi_s|_\mathfrak{p}$ for every term $\xi_{j_1}\cdots\xi_{j_s}$ in the sum (13)

not equal to $\xi_1 \cdots \xi_s$. This implies $1 = |\xi_1|_{\mathfrak{p}} = \cdots = |\xi_s|_{\mathfrak{p}}$ which leads to the contradiction $1 = |a_0| = |\xi_1 \cdots \xi_r|_{\mathfrak{p}}^{p^\mu} < 1$.

We will also need to guarantee that $q_{\mathfrak{p}}$, the number of elements of the residue class field $\mathfrak{o}/\mathfrak{p}$, is not too small; more precisely, we will need that $q_{\mathfrak{p}} \geq C_f$ where C_f is a fixed positive constant, depending only on the degree of our quasi-homogeneous polynomial f. The precise value of C_f will be determined later. In the setting of Dedekind domains $\mathfrak{o}$ with the finiteness property (FP) the collection $\mathcal{B}_C$ of prime ideals $\mathfrak{p}$ with absolute norm $q_{\mathfrak{p}} \leq C$ is finite in number; see for example, [11].

The exceptional set $\mathcal{P}(f)$ of prime ideals in the statement of Theorem 1.3 is the union of $\mathcal{F}(\xi)$ over all algebraic elements $\xi \in \mathcal{A}$, together with the collection $\mathcal{B}_{C_f}$.

2.6. **Passing to the completion $\bar{\mathfrak{o}}_{\mathfrak{p}}$.** It will be convenient for us to pass to the completion $\bar{\mathfrak{o}}_{\mathfrak{p}}$. This will enable us to write our character sum as an "oscillatory integral" over a local field and to write the number of solutions to a polynomial congruence as the measure of a sublevel set. Since the residue class field $\bar{\mathfrak{o}}_{\mathfrak{p}}/\pi_{\mathfrak{p}}\bar{\mathfrak{o}}_{\mathfrak{p}}$ is finite, the ring $\bar{\mathfrak{o}}_{\mathfrak{p}}$ is then the compact ring of integers of the local field $\bar{K}_{\mathfrak{p}}$, the quotient field of $\bar{\mathfrak{o}}_{\mathfrak{p}}$. We then have at our disposal a Haar measure $d\mu_{\mathfrak{p}}$ on $\bar{K}_{\mathfrak{p}}$ which we normalise so that $\mu_{\mathfrak{p}}(\bar{\mathfrak{o}}_{\mathfrak{p}}) = 1$. The discrete valuation $|\cdot|_{\mathfrak{p}}$, initially defined on $\mathfrak{o}$, extends uniquely to a valuation on $\bar{K}_{\mathfrak{p}}$ which we continue to denote by $|\cdot|_{\mathfrak{p}}$.

Since the prime ideal $\mathfrak{p}$ is fixed (although we keep in mind estimates which are uniform in $\mathfrak{p}$), we will suppress from now on the subscript $\mathfrak{p}$ in the various quantities $\bar{\mathfrak{o}}_{\mathfrak{p}}, \bar{K}_{\mathfrak{p}}, \pi_{\mathfrak{p}}, q_{\mathfrak{p}}, d\mu_{\mathfrak{p}}, |\cdot|_{\mathfrak{p}}$, etc... for notational convenience.

From the isomorphisms $\mathfrak{o}/\mathfrak{p}^s \to \bar{\mathfrak{o}}/\pi^s\bar{\mathfrak{o}}$, we see that the number of solutions to $f \equiv 0 \mod \mathfrak{p}^s$ is the same as the number of solutions to $f \equiv 0 \mod \pi^s\bar{\mathfrak{o}}$; that is

$$\mathcal{N}(f; \mathfrak{p}^s) \;=\; q^{-2s}\#\{f \equiv 0 \bmod \pi^s\bar{\mathfrak{o}}\} \;=\; \mathcal{N}(f; \pi^s\bar{\mathfrak{o}}).$$

If $d\mu_2 = d\mu \times d\mu$ denotes the product measure on $\bar{\mathfrak{o}} \times \bar{\mathfrak{o}}$, we have

$$\mathcal{N}(f; \pi^s\bar{\mathfrak{o}}) \;=\; \mu_2\big(\{z \in \bar{\mathfrak{o}} \times \bar{\mathfrak{o}} : \; |f(z)| \;\leq\; q^{-s}\}\big). \tag{14}$$

In fact the right hand side of (14) is equal to

$$\iint_{\bar{\mathfrak{o}}\times\bar{\mathfrak{o}}} \mathbf{1}_{\{|f(w)|\leq q^{-s}\}}(y)\, d\mu_2(y) \;=\; \sum_{z' \leq \pi^s\bar{\mathfrak{o}}} \iint_{B_{q^{-s}}(z')} \mathbf{1}_{\{|f(w)|\leq q^{-s}\}}(y)\, d\mu_2(y)$$

$$=\; q^{-2s}\#\{z' \leq \pi^s\bar{\mathfrak{o}} : \; |f(x',y')| \;\leq\; q^{-s}\} \;=\; \mathcal{N}(f; \pi^s\bar{\mathfrak{o}}).$$

Here we are using the nonstandard notation $z' \leq \pi^s\bar{\mathfrak{o}}$ to denote elements $z' = (x', y')$ in $\bar{\mathfrak{o}} \times \bar{\mathfrak{o}}$ of the form $x' = x_0 + x_1\pi + \cdots + x_{s-1}\pi^{s-1}, y' = y_0 + y_1\pi + \cdots + y_{s-1}\pi^{s-1}$ where each x_j and y_j varies over the q representations in $\mathfrak{o}$ of the elements in the residue class field. Also $B_r(z) = \{w \in \bar{K} \times \bar{K} : \|w - z\| \leq r\}$ denote balls in $\bar{K} \times \bar{K}$ where $\|z\| := \max(|x|, |y|)$ if $z = (x, y)$. The second equality above follows since $|f(x, y)| \leq q^{-s}$ if and only if $|f(x', y')| \leq q^{-s}$ for elements $z = (x, y) \in B_{q^{-s}}(x', y')$.

A similar identity holds for character sums. We claim we can find a non-principal additive character ψ on $\bar{K}$ with $\psi \equiv 1$ on $\bar{\mathfrak{o}}$ so that

$$\mathcal{S}_\chi(f;\mathfrak{p}^s) \;=\; \iint_{\bar{\mathfrak{o}}\times\bar{\mathfrak{o}}} \psi(\pi^{-s}f(x,y))\,d\mu(x)d\mu(y). \tag{15}$$

Furthermore ψ will be non-trivial on $\{z \in \bar{K} : |z| \le q\}$ since χ is primitive.

In fact, starting with our non-principal, primitive additive character χ on $\mathfrak{o}/\mathfrak{p}^s$, we pass to a character χ' on $\bar{\mathfrak{o}}/\pi^s\bar{\mathfrak{o}}$ via the isomorphism $\mathfrak{o}/\mathfrak{p}^s \simeq \bar{\mathfrak{o}}/\pi^s\bar{\mathfrak{o}}$ so that

$$\mathcal{S}_\chi(f;\mathfrak{p}^s) \;=\; q^{-2s}\sum_{(x,y)\in[\mathfrak{o}/\mathfrak{p}^s]^2}\chi(f(x,y)) \;=\; q^{-2s}\sum_{(x,y)\in[\bar{\mathfrak{o}}/\pi^s\bar{\mathfrak{o}}]^2}\chi'(f(x,y)).$$

Next, χ' restricts to a non-principal character $\bar{\chi}$ on $\bar{\mathfrak{o}}$ via $\bar{\chi}(x) = \chi'(x+\pi^s\bar{\mathfrak{o}})$ which is equal to 1 on $\pi^s\bar{\mathfrak{o}}$. The characters of $\bar{\mathfrak{o}}$ arise as $x \to \psi_0(yx)$ for some $y = \sum_{j=-m}^{-1} x_j\pi^j$ and some fixed non-principal character ψ_0 on $\bar{K}$ which is 1 on $\bar{\mathfrak{o}}$ and non-trivial on $\{z \in \bar{K} : |z| \le q\}$. Hence $\bar{\chi}(x) = \psi_0(y'x)$ for some y' satisfying $|y'| = q^s$. In fact since ψ_0 is non-trivial on $B_q(0)$ we can find an x with $|y'x| = q$ so that $\bar{\chi}(x) \neq 1$ and hence $|x| \ge q^{-s+1}$ implying $|y'| \le q^s$. On the other hand since χ is a primitive character, we can find a v with $|v| = q^{-s+1}$ so that $\psi_0(y'v) = \bar{\chi}(v) \neq 1$. This implies that $|y'|q^{-s+1} = |y'v| \ge q$ and so $|y'| \ge q^s$.

Therefore the character $\psi(z) := \psi_0(y'\pi^s z)$ on $\bar{K}$ has the properties $\psi(\pi^{-s}x) = \bar{\chi}(x)$ on $\bar{\mathfrak{o}}$, $\psi \equiv 1$ on $\bar{\mathfrak{o}}$ and ψ is non-trivial on $B_q(0)$. Furthermore, using the nonstandard notation $z' \le \pi^s\bar{\mathfrak{o}}$ introduced above,

$$\iint_{\bar{\mathfrak{o}}\times\bar{\mathfrak{o}}}\psi(\pi^{-s}f(z))d\mu_2(z) = \sum_{w'\le\pi^s\bar{\mathfrak{o}}}\iint_{B_{q^{-s}}(w')}\psi(\pi^{-s}f(z))d\mu_2(z) \;=$$

$$q^{-2s}\sum_{w'\le\pi^s\bar{\mathfrak{o}}}\psi(\pi^{-s}f(w')) = q^{-2s}\sum_{x'\le\pi^s\bar{\mathfrak{o}}}\bar{\chi}(f(x')) = q^{-2s}\sum_{(x,y)\in[\bar{\mathfrak{o}}/\pi^s\bar{\mathfrak{o}}]^2}\chi'(f(x,y))$$

which establishes (15) since the last sum is equal to $\mathcal{S}_\chi(f;\mathfrak{p}^s)$.

2.7. **Lower bounds on the distance from roots of f to $\bar{\mathfrak{o}}$.** In our analysis we will need to understand sets of the form $B_\rho(\zeta)\cap\bar{\mathfrak{o}}$ where ζ is one of the nonzero roots of f appearing in (11),

$$B_\rho(\zeta) \;=\; \{y \in \bar{K}^{alg} : |y-\zeta| \le \rho\}$$

is a ball lying in $\bar{K}^{alg}$ and $|\cdot|$ is the unique extension to $\bar{K}^{alg}$ of our original valuation on $\bar{K}$. For $\mathfrak{p} \notin \mathcal{P}(f)$, ζ has the property that $|\zeta| = |\zeta|_{\mathfrak{p}} = 1$ as well as $|\zeta_1| = \cdots = |\zeta_r| = 1$ where $\zeta_1,\ldots,\zeta_r$ denote the conjugates of ζ over K. Since these conjugates are among the roots of f, they lie in $\mathcal{A}$ as well as their differences and so $|\zeta_s - \zeta_t| = |\zeta_s-\zeta_t|_{\mathfrak{p}} = 1$ also holds for $1 \le s \neq t \le r$ and $\mathfrak{p} \notin \mathcal{P}(f)$.

It will be useful to have a good bound from below on the quantity $\inf_{x\in\bar{\mathfrak{o}}}|x-\zeta|$ whenever $\zeta \notin \bar{K}$. This will be easily achieved by Krasner's lemma when ζ is separable over K. In this case we will see that $\inf_{x\in\bar{\mathfrak{o}}}|x-\zeta| = 1$. In fact we will show that $|x-\zeta| = 1$ for every $x \in \bar{\mathfrak{o}}$. When ζ is not separable over K (and so K must have positive characteristic, say equal to p), then there is a $\mu \ge 1$ such that ζ^{p^μ} is separable over K. We claim that $\zeta^{p^\mu} \notin \bar{K}$ and so one can argue again by

Krasner's lemma to deduce that $\inf_{x\in\bar{\mathfrak{o}}}|x-\zeta|=1$. In fact the supposition $\zeta^{p^\mu}\in\bar{K}$ implies that $\zeta\in\bar{K}$, contrary to our assumption $\zeta\notin\bar{K}$. To see this, note that in the positive characteristic case, $\bar{K}=\mathbb{F}_q((\pi))$ is the field of Laurent series with coefficients in the finite field $\mathbb{F}_q$ with $q=p^f$ elements. Since ζ is algebraic over K it is algebraic over $\bar{K}$ and so lies in $\mathbb{F}_{q^d}((\pi))$ for some $d\geq 2$ since $\zeta\notin\mathbb{F}_q((\pi))$. Hence

$$\zeta \;=\; \xi_0+\xi_1\pi+\xi_2\pi^2+\xi_3\pi^3+\cdots$$

where each ξ_j lies in $\mathbb{F}_{q^d}$ (recall that $|\zeta|=|\zeta|_{\mathfrak{p}}=1$) and so

$$\zeta^{p^\mu} \;=\; [\xi_0]^{p^\mu}+[\xi_1]^{p^\mu}\pi^{p^\mu}+[\xi_2]^{p^\mu}\pi^{2p^\mu}+\cdots\;\in\;\bar{K}\;=\;\mathbb{F}_q((\pi)).$$

Therefore $\xi_j^{p^\mu}\in\mathbb{F}_q$ for each $j\geq 0$. The map $\phi(x)=x^{p^\mu}$ is automorphism for both fields $\mathbb{F}_{q^d}$ and $\mathbb{F}_q$. As an automorphism of $\mathbb{F}_q$, we can find an $\eta_j\in\mathbb{F}_q$ such that $\eta_j^{p^\mu}=\xi_j^{p^\mu}$ for each $j\geq 0$. As an automorphism of $\mathbb{F}_{q^d}$, we deduce $\xi_j=\eta_j\in\mathbb{F}_q$ for every $j\geq 0$, implying that $\zeta\in\mathbb{F}_q((\pi))=\bar{K}$, contradicting our underlying assumption $\zeta\notin\bar{K}$.

We have the following lemma.

Lemma 2.8. *In the setting above, suppose $\zeta\notin\bar{K}$. Then for every $x\in\bar{\mathfrak{o}}$, $|x-\zeta|=1$.*

Proof We split the proof into two cases. First suppose that ζ is separable over K. Then ζ is separable over $\bar{K}$. Suppose that there is an $x\in\bar{\mathfrak{o}}$ such that $|x-\zeta|<1$. Then $|\zeta-x|<|\zeta-\zeta'|$ for all conjugates ζ' of ζ over $\bar{K}$ different from ζ since $|\zeta-\zeta'|=1$. Hence by Krasner' lemma (see for example [10]), $\bar{K}[\zeta]\subset\bar{K}[x]=\bar{K}$ implying $\zeta\in\bar{K}$ which contradicts our underlying assumption $\zeta\notin\bar{K}$. Hence $|x-\zeta|\geq 1$ but clearly $|x-\zeta|\leq 1$ since $|\zeta|=1$.

Now let us consider the case when ζ is not separable over K. As discussed above, there is a $\mu\geq 1$ so that ζ^{p^μ} is separable over K yet does not belong to $\bar{K}$. Hence we can apply Krasner's lemma to ζ^{p^μ} to deduce $|y-\zeta^{p^\mu}|\geq 1$ for every $y\in\bar{\mathfrak{o}}$. Therefore for every $x\in\bar{\mathfrak{o}}$,

$$|x-\zeta|^{p^\mu} \;=\; |(x-\zeta)^{p^\mu}| \;=\; |x^{p^\mu}-\zeta^{p^\mu}| \;\geq\; 1$$

and so we have $|x-\zeta|=1$.

■

2.9. **Notation and constants.** All constants $C,c,c'>0$ throughout this paper will depend only on the degree of our quasi-homogeneous polynomial $f(x,y)$, although the values of these constants may change from line to line. Often it will be convenient to suppress explicitly mentioning the constants C or c in these inequalities and we will use the notation $A\lesssim B$ between positive quantities A and B to denote the inequality $A\leq CB$ or $cA\leq B$. Finally we use the notation $A\sim B$ to denote that both inequalities $A\lesssim B$ and $B\lesssim A$ hold.

3. Polynomial congruences in one variable

The proof of Theorem 1.3 relies on a precise structural statement for sublevel sets of polynomials $P \in \bar{K}[X]$ in one variable with coefficients lying in our local field $\bar{K}$ which carries the nontrivial valuation $|\cdot|$. Suppose our polynomial $P(x) = a\prod(x-\xi_j)^{e_j}$ has distinct roots $\xi_1, \ldots, \xi_m$ lying in $\bar{K}^{alg}$. As remarked earlier our valuation on $\bar{K}$ extends uniquely to a valuation on $\bar{K}^{alg}$ which we will continue to denote by $|\cdot|$. The structural statement of a sublevel set $\{x \in S : |P(x)| \le \delta\}$ where $S \subset \bar{K}$ will be given in terms of *balls* $B_r(\xi) := \{y \in \bar{K}^{alg} : |y-\xi| \le r\}$ in $\bar{K}^{alg}$, centred at the roots $\{\xi_j\}$ of P with radii r described by *root clusters* $\mathcal{C}$ of $\{\xi_1, \ldots, \xi_m\}$; a root cluster $\mathcal{C}$ being defined simply as some subset $\mathcal{C} \subset \{\xi_1, \ldots, \xi_m\}$ of the roots of P. We associate a size $S(\mathcal{C}) := \sum_{\xi_j \in \mathcal{C}} e_j$ to a cluster by counting the number of roots in the cluster with multiplicities. The following proposition is the non-archimedean version of a basic sublevel set estimate due to Phong, Stein and Sturm [13] and its simple proof can be found in [15] or [16].

Proposition 3.1. *With the notation as above, we have*

$$\big\{x \in S : \ |P(x)| \le \delta\big\} \ = \ \bigcup_{j=1}^{m} [B_{r_j}(\xi_j) \cap S]. \tag{16}$$

Here

$$r_j \ = \ \min_{\mathcal{C} \ni \xi_j} r_{\mathcal{C},j}(\delta) \ := \ \min_{\mathcal{C} \ni \xi_j} \Big[\frac{\delta}{|a\prod_{\xi_k \notin \mathcal{C}}(\xi_j - \xi_k)^{e_k}|}\Big]^{1/S(\mathcal{C})}$$

where the minimum is taken over all root clusters $\mathcal{C}$ containing ξ_j and the product is taken over all k such that $\xi_k \notin \mathcal{C}$.

In our application of Proposition 3.1 the roots ξ_j and the coefficient $a \in \bar{K}$ have the property that $|a| = |\xi_j| = 1$. Furthermore $|\xi_j - \xi_k| = 1$ for all $j \ne k$. In this case the minimum over all root clusters $\mathcal{C}$ containing a root ξ_j in the definition of r_j is attained when $\mathcal{C} = \{\xi_j\}$ is the singleton root cluster (here we are assuming $\delta \le 1$). Therefore

$$r_j \ = \ r_j(\delta) \ = \ \delta^{1/e_j}. \tag{17}$$

4. The main estimates in Theorem 1.3

We will give a direct proof which treats simultaneously our character sums

$$S_\chi(f; \mathfrak{p}^s) \ = \ \iint_{\bar{\mathfrak{o}} \times \bar{\mathfrak{o}}} \psi(\pi^{-s} f(x,y))\, d\mu(x) d\mu(y)$$

and the number of solutions to our polynomial congruences

$$\mathcal{N}(f; \mathfrak{p}^s) = \mu_2\big(\{z \in \bar{\mathfrak{o}} \times \bar{\mathfrak{o}} : \ |f(z)| \ \le \ q^{-s}\}\big) = \iint_{\bar{\mathfrak{o}} \times \bar{\mathfrak{o}}} \mathbf{1}_{\bar{\mathfrak{o}}}(\pi^{-s} f(x,y))\, d\mu(x) d\mu(y);$$

that is one proof works to establish the estimates (7), (8), (9) and (10) in Theorem 1.3. We make the ongoing assumption that f consists of more than one monomial; for the simple case when f is a monomial, see Section 6. When treating $\mathcal{S}_\chi(f; \mathfrak{p}^s)$, we assume $2 \le d(f)$ (for the case $d(f) < 2$, see Section 5). Recall that the Varchenko

exponents $i(f) = \nu(f)$ agree when $h(f) \geq 2$ and in this case, we will denote the common value as $\nu(f)$.

In the case when the ratio κ_2/κ_1 of the dilation parameters is an integer (this includes the case when f is a a homogeneous polynomial), the argument below works if we replace the additive character ψ or the indicator function $\mathbf{1}_{\bar{\mathfrak{o}}}$ by any general complex-valued function $\mathcal{C} : \bar{K} \to \mathbb{C}$ with the following properties:

$(C1)$ $\quad \mathcal{C} \equiv 1$ on $\bar{\mathfrak{o}}$;

$(C2)$ $\displaystyle\int_{|x|=1} \mathcal{C}(\pi^{-j} g(x))\, d\mu(x) = 0$ for all $j \geq 2$ and $g(x) = b_k x^k + \cdots + b_1 x + b_0$ in $\mathfrak{o}[X]$ with the property $\pi | b_r$ for $r \leq k-1$ and $|k b_k| = 1$; and

$(C3)$ $\quad \Big| \displaystyle\int_{|x|=1} \mathcal{C}(\pi^{-1} b x^k)\, d\mu(x) \Big| \leq A_k q^{-1/2}$ for all $k \geq 1$ and $|b| = 1$.

When $\mathcal{C} = \mathbf{1}_{\bar{\mathfrak{o}}}$, properties (C2) and (C3) are trivial to verify since $\pi^{-j} g(x) \notin \bar{\mathfrak{o}}$ for all $j \geq 1$ and $|g(x)| = 1$ whenever $|x| = 1$; in particular the integral in (C3) in fact vanishes in this case.

If we have this extra cancellation we can replace (C3) with the stronger property

$(C3)'$ $\displaystyle\int_{|x|=1} \mathcal{C}(\pi^{-1} b x^k)\, d\mu(x) = 0$ for all $k \geq 1$ and $|b| = 1$.

For the general case, when κ_2/κ_1 is not necessarily an integer, we will need a slight strengthening of property (C2); namely the vanishing $\int_{|x|=1} \mathcal{C}(\pi^{-j} g(x)) d\mu(x) = 0$ still holds if the region of integration $\{|x| = 1\}$ is replaced by any finite union of disjoint balls $B_{q^{-1}}$ in $\bar{\mathfrak{o}}$ with radius q^{-1}. Furthermore there will be one instance where we will need to appeal to a stronger form of property (C3); namely when the monomial x^k is replaced by a general monic $x^k + c_{k-1} x^{k-1} + \cdots + c_1 x$ polynomial. Such square root $q^{-1/2}$ estimates for character sums follow from the work of A. Weil but there is no need to appeal to such deep results in the monomial case x^k.

The verification of (C2) and (C3) for the additive character $\mathcal{C} = \psi$ is straightforward. In fact to see (C2), we write our oscillatory integral

$$\int_{|x|=1} \psi(\pi^{-j} g(x))\, d\mu(x) = q^{-j} \sum_{\substack{x \leq \pi^j \bar{\mathfrak{o}} \\ \pi \not| x}} \chi'(\pi^{-j} g(x))$$

back in terms of a character sum over $\bar{\mathfrak{o}}/\pi^j \bar{\mathfrak{o}}$ (using the nonstandard notation $x \leq \pi^j \bar{\mathfrak{o}}$ introduced in Section 2) and decompose the sum via $x = z + \pi^{j-1} y$ so that

$$\int_{|x|=1} \psi(\pi^{-j} g(x))\, d\mu(x) = q^{-j} \sum_{\substack{z \leq \pi^{j-1} \bar{\mathfrak{o}} \\ \pi \not| z}} \chi'(\pi^{-j} g(z)) \sum_{y \leq \pi \bar{\mathfrak{o}}} \chi'(\pi^{-1} g'(z) y);$$

in fact for $x = z + \pi^{j-1}y$, we have $g(x) \equiv g(z) + g'(z)\pi^{j-1}y \bmod \pi^j\mathfrak{o}$ since $j \geq 2$. Furthermore $g'(z) \equiv kb_kz^{k-1} \bmod \pi\bar{\mathfrak{o}}$ and so for each z arising in the first sum above, the inner sum can written as

$$\sum_{y \leq \pi\bar{\mathfrak{o}}} \chi'(\pi^{-1}kb_kz^{k-1}y)$$

and this sum vanishes by the basic orthogonality property of the nonprincipal character χ' since $\pi \not| \, kb_kz^{k-1}$ when $|kb_k| = 1$. Note that the proof works if the region of integration $\{|x| = 1\}$ in the original integral is replaced by any union of disjoint balls $B_{q^{-1}}$ with radius q^{-1}.

As mentioned above, property (C3) for character sums follows from the work of A. Weil but in this case there is a simple well-known proof which we reproduce for the convenience of the reader. Writing again the oscillatory integral

$$\int_{|x|=1} \psi(\pi^{-1}bx^k)\ d\mu(x) \ = \ q^{-1} \sum_{x \leq \pi:\ x \neq 0} \chi(\pi^{-1}bx^k)$$

as a character sum over the finite field $\mathfrak{o}/\pi\mathfrak{o}$, we rewrite the right-hand side as

$$q^{-1} \sum_{z \leq \pi:\ z \neq 0} \chi(\pi^{-1}bz) \sum_{x:\ x^k = z} 1.$$

Let g generate the multiplicative group $[\mathfrak{o}/\pi\mathfrak{o}] \setminus \{0\}$ and write $\log(z)$ as the integer ℓ, $0 \leq \ell \leq q-2$ such that $z = g^\ell$. For a given z, the equation $x^k = z$ is solvable if and only if $gcd(k, q-1) \,|\, \log(z)$ and when this happens there are precisely $d := gcd(k, q-1)$ solutions. Therefore we can write the inner sum above as $\sum_{m=0}^{d-1} \exp(2\pi im \log(z)/d)$ and hence

$$q^{-1} \sum_{x \leq \pi:\ x \neq 0} \chi(\pi^{-1}bx^k) \ = \ q^{-1} \sum_{m=0}^{d-1} \sum_{z \leq \pi:\ z \neq 0} \exp(2\pi im \log(z)/d)\ \chi(\pi^{-1}bz).$$

For $m = 0$, the character sum in z gives -1 and for $m \geq 1$, the quantity

$$U_m \ = \ \sum_{z \leq \pi:\ z \neq 0} \exp(2\pi im \log(z)/d)\ \chi(\pi^{-1}bz)$$

has modulus equal to $\sqrt{q}$. In fact

$$|U_m|^2 \ = \ \sum_{x \neq 0} \sum_{y \neq 0} \exp(2\pi im \log(x)/d) \chi(\pi^{-1}by(x-1))$$

and the double sum is equal to

$$q-1+\sum_{x \neq 0,1} \exp(2\pi im \log(x)/d) \sum_{y \neq 0} \chi(\pi^{-1}b(x-1)y) = q-1-\sum_{x \neq 0,1} \exp(2\pi im \log(x)/d) = q.$$

This shows that property (C3)

$$\Big| \int_{|x|=1} \psi(\pi^{-1}bx^k)\ d\mu(x) \Big| \ \leq \ \sqrt{gcd(k, q-1)}\ q^{-1/2}$$

holds when $\mathcal{C} = \psi$.

4.1. **The basic decomposition.** Recall that

$$f(x,y) \;=\; ax^\alpha y^\beta \prod_{j=1}^{M} (y^t - \zeta_j x^r)^{n_j}$$

and $d(f) = (\alpha t+\beta r+nr)/(r+t)$ where $n = \sum_{j=1}^M n_j$. Following Denef and Sperber [4] we decompose the integral

$$\iint_{\bar{\mathfrak{o}}\times\bar{\mathfrak{o}}} \mathcal{C}(\pi^{-s} f(x,y))\, d\mu(x) d\mu(y) \;=\; \sum_{k_1,k_2\geq 0} \iint_{|x|=q^{-k_1},|y|=q^{-k_2}} \mathcal{C}(\pi^{-s} f(x,y))\, d\mu(x) d\mu(y)$$

into three parts $I + II + III$ where

$$\begin{aligned} I \;&=\; \sum_{\substack{k_1,k_2\geq 0\\ tk_2 = rk_1}} \iint_{|x|=q^{-k_1},|y|=q^{-k_2}} \mathcal{C}(\pi^{-s} f(x,y))\, d\mu(x) d\mu(y) \\ &=\; \sum_{m\geq 0} q^{-(t+r)m} \iint_{|x|=1,|y|=1} \mathcal{C}(\pi^{-s+mN} f(x,y))\, d\mu(x) d\mu(y) \end{aligned}$$

and $N := \alpha t + \beta r + ntr$. Here we used the fact that t and r are relatively prime so that if $tk_2 = rk_1$, then $t|\, k_1$ and so we are writing $k_1 = mt$ in the above sum. Furthermore II and III are defined as

$$\begin{aligned} II \;&=\; \sum_{\substack{k_1,k_2\geq 0\\ tk_2 < rk_1}} \iint_{|x|=q^{-k_1},|y|=q^{-k_2}} \mathcal{C}(\pi^{-s} f(x,y))\, d\mu(x) d\mu(y), \\ III \;&=\; \sum_{\substack{k_1,k_2\geq 0\\ tk_2 > rk_1}} \iint_{|x|=q^{-k_1},|y|=q^{-k_2}} \mathcal{C}(\pi^{-s} f(x,y))\, d\mu(x) d\mu(y). \end{aligned}$$

4.2. **Estimates for I.** We turn our attention first to I which is the main term. We split $I = I_1 + I_2$ into two parts where

$$I_1 \;=\; \sum_{mN\geq s} q^{-(t+r)m} \int_{|x|=1} \int_{|y|=1} \mathcal{C}(\pi^{-s+mN} f(x,y))\, d\mu(x) d\mu(y)$$

and

$$I_2 \;=\; \sum_{mN\leq s-1} q^{-(t+r)m} \int_{|x|=1} \int_{|y|=1} \mathcal{C}(\pi^{-s+mN} f(x,y))\, d\mu(y) d\mu(x).$$

From property (C1) we see that

$$I_1 \;=\; (1-q^{-1})^2 \sum_{mN\geq s} q^{-(t+r)m} \;\leq\; (1-q^{-1}) q^{-s/d(f)} \tag{18}$$

and when $s \equiv 0 \bmod N$,

$$(1-q^{-1})^2 q^{-s/d(f)} \;\leq\; I_1. \tag{19}$$

For I_2 we would like to make a change of variables $u = \phi(x)$ in x so that $u^t = x$. This will require some care if $t \geq 2$ but if we can do this, then the idea is to make the change of variables $y = u^r z$ in the y integral which will successfully separate

the variables by the quasi-homogeneity of f. Of course this can be done easily if $t = 1$ (that is, when the ratio κ_2/κ_1 of the dilation parameters is an integer) which includes the homogeneous case. Some care needs to be taken then $\kappa_2/\kappa_1 \notin \mathbb{N}$ or $t \geq 2$.

4.2.1. *Estimates for I_2: the case when $\kappa_2/\kappa_1 \in \mathbb{N}$.* To get an idea of where we are heading, let us consider the treatment of I_2 when $t = 1$ (or equivalently, when $\kappa_2/\kappa_1 \in \mathbb{N}$); here $\phi(x) = x$ above so there is no initial change of variables in x. We will then discuss the modifications needed to treat the general case. When $t = 1$, we proceed directly to the second change of variables $y = x^r z$ in the inner y integral and write $I_2 =$

$$\sum_{mN \leq s-1} q^{-(1+r)m} \int_{|x|=1} \left[\int_{|z|=1} \mathcal{C}(\pi^{-s+mN} x^N h(z))\, d\mu(z) \right] d\mu(x) \tag{20}$$

where $h(z) = az^\beta \prod_{j\geq 1}(z-\zeta_j)^{n_j}$. We now interchange the order of integration and decompose the z integral depending on the size of $h(z)$;

$$I_2 = \sum_{mN\leq s-1} q^{-(1+r)m} \sum_{\ell \geq 0} \int\limits_{\left\{|z|=1:|h(z)|=q^{-\ell}\right\}} d\mu(z) \int\limits_{|x|=1} \mathcal{C}(\pi^{-s+mN+\ell}[\pi^{-\ell}h(z)]x^N) d\mu(x).$$

By property (C2) the ℓ sum vanishes for $\ell \leq s - mN - 2$ and by property (C1) the inner x integral equals to $(1 - q^{-1})$ for $\ell \geq s - mN$. Hence we split $I_2 = I_{2,1} + I_{2,2}$ where

$$I_{2,1} \;=\; (1-q^{-1}) \sum_{mN\leq s-1} q^{-(1+r)m} \sum_{\ell \geq s-mN} \mu\big(\{|z| = 1 : |h(z)| = q^{-\ell}\}\big) \tag{21}$$

and

$$I_{2,2} = \sum_{mN\leq s-1} q^{-(1+r)m} \int_{\left\{|z|=1:|h(z)|=q^{-\ell_{m,s}}\right\}} F_{m,s}(z) d\mu(z)$$

where $\ell_{m,s} = s - mN - 1$ and $F_{m,s}(z) = \int_{|x|=1} \mathcal{C}(\pi^{-1}[\pi^{-\ell_{m,s}}h(z)]x^N) d\mu(x)$. If $\mathcal{C}$ satisfies the extra cancellation condition (C3)' (which is the case for the problem of polynomial congruences), then $I_{2,2} = 0$. Property (C3) implies $|F_{m,s}(z)| \leq Cq^{-1/2}$ for z satisfying $|h(z)| = q^{-\ell_{m,s}}$ and so

$$|I_{2,2}| \;\leq\; Cq^{-1/2} \sum_{mN\leq s-1} q^{-(1+r)m} \mu\big(\{|z| = 1 : |h(z)| = q^{-\ell_{m,s}}\}\big). \tag{22}$$

From (21) and (22) we see that we need to understand the sets $\{|z| = 1 : |h(z)| = q^{-\ell}\}$ and here is where Proposition 3.1 comes into play.

Set $\mathcal{I}_{\mathfrak{p}} = \{j \geq 1 : \zeta_j \in \bar{K}\}$. Recall that $\bar{K} = \bar{K}_{\mathfrak{p}}$ is the completion of K with respect to the valuation $|\cdot|_{\mathfrak{p}}$. The set $\mathcal{I}_{\mathfrak{p}}$ may be empty. From Proposition 3.1 and the subsequent remarks, we see that for any $\ell \geq 1$,

$$\big\{|z| = 1 : |h(z)| = q^{-\ell}\big\} \;=\; \bigcup_{j\in\mathcal{I}_{\mathfrak{p},\ell}} \big\{|z| = 1 : |z-\zeta_j| = q^{-\ell/n_j}\big\} \tag{23}$$

where $\mathcal{I}_{\mathfrak{p},\ell} = \{j \in \mathcal{I}_{\mathfrak{p}} : n_j \mid \ell\}$. Since the union above is disjoint (recall that $|\zeta_j - \zeta_k| = 1$ for all $j \neq k$ when $\mathfrak{p} \notin \mathcal{P}(f)$), we have

$$I_{2,1} = (1-q^{-1})^2 \sum_{j\in\mathcal{I}_{\mathfrak{p}}} \sum_{mN\le s-1} q^{-(1+r)m} \sum_{n\ge (s-mN)/n_j} q^{-n} := (1-q^{-1})^2 \sum_{j\in\mathcal{I}_{\mathfrak{p}}} I_{2,1}^j.$$

If $\mathcal{I}_{\mathfrak{p}} = \emptyset$, then $I_{2,1} = 0$ but if $\mathcal{I}_{\mathfrak{p}} \neq \emptyset$, the following estimates hold. Since

$$q^{-(1+r)m} \sum_{n\ge (s-mN)/n_j} q^{-n} \;\le\; C\, q^{-s/n_j} q^{m(1+r)(d(f)-n_j)/n_j}$$

for each $j \in \mathcal{I}_{\mathfrak{p}}$ and some absolute constant C, we have

$$I_{2,1}^j \;\le\; C\, q^{-s/n_j} \quad I_{2,1}^j \;\le\; C\, sq^{-s/d(f)} \quad \text{or} \quad I_{2,1}^j \;\le\; C\, q^{-s/d(f)} \tag{24}$$

whenever $d(f) < n_j$, $d(f) = n_j$ or $n_j < d(f)$, respectively. Furthermore

$$q^{-s/n_j} q^{-1} \;\le\; I_{2,1}^j \quad \text{or} \quad c\, sq^{-s/d(f)} q^{-1} \;\le\; I_{2,1}^j \tag{25}$$

for all $s \ge 1$ whenever $d(f) < n_j$ or $d(f) = n_j$, respectively; however when $s \equiv 0 \mod n_j$, (25) improves to

$$q^{-s/n_j} \;\le\; I_{2,1}^j \quad \text{or} \quad c\, sq^{-s/d(f)} \;\le\; I_{2,1}^j \tag{26}$$

whenever $d(f) < n_j$ or $d(f) = n_j$, respectively.

We turn now to bounding $I_{2,2}$ and here $\ell_{m,s} \ge 1$ unless $mN = s-1$ (which can happen only if $N \mid s-1$) in which case $\ell_{m,s} = 0$. The complimentary case $\ell = 0$ to (23) is

$$\big\{|z| = 1 : |h(z)| = 1\big\} \;=\; \big\{|z| = 1 : |z-\zeta_j| = 1 \;\text{ for all } j\big\}.$$

In fact, Lemma 2.8 implies that $|z - \zeta_j| = 1$ automatically holds for all $z \in \bar{\mathfrak{o}}$ whenever $\zeta_j \notin \bar{K}$. The right hand side is $\{z : |z| = 1\}$ when $\mathcal{I}_{\mathfrak{p}} = \emptyset$. Therefore

$$I_{2,2} \;=\; \sum_{mN\le s-2} \sum_{j\in\mathcal{I}_{\mathfrak{p}}^{m,s}} I_{2,2}^{m,j} \;+\; I_{2,2}^* \;:=\; \sum_{j\in\mathcal{I}_{\mathfrak{p}}} I_{2,2}^j \;+\; I_{2,2}^*$$

where $\mathcal{I}_{\mathfrak{p}}^{m,s} := \{j \in \mathcal{I}_{\mathfrak{p}} : n_j \mid \ell_{m,s}\}$,

$$I_{2,2}^{m,j} = q^{-(1+r)m} \int_{\left\{|z|=1\,:\,|z-\zeta_j|=q^{-\ell_{m,s}/n_j}\right\}} F_{m,s}(z)\, d\mu(z), \qquad I_{2,2}^j = \sum_{\substack{mN\le s-2 \\ n_j \mid \ell_{m,s}}} I_{2,2}^{m,j}$$

and

$$I_{2,2}^* \;=\; q^{-(1+r)(s-1)/N} \int_{\{|z|=1\,:\,|z-\zeta_j|=1,\,\forall j\}} F_{(s-1)/N,s}(z)\, d\mu(z).$$

The term $I_{2,2}^*$ appears only if $s \equiv 1 \mod N$ and if this is the case, then property (C3) implies that

$$|I_{2,2}^*| \;\le\; Cq^{-1/2} q^{-(1+r)(s-1)/N} \;=\; Cq^{-[\frac{1}{2}-\frac{1}{d(f)}]} q^{-s/d(f)}. \tag{27}$$

We note $j \in \mathcal{I}_{\mathfrak{p}}^{m,s}$ implies $n_j \mid s-1-mN$ which in turn implies $\gcd(n_j, N) \mid (s-1)$. Therefore if $\gcd(n_j, N) \ge 2$ and $s \equiv 0 \mod \gcd(n_j, N)$, then $j \notin \mathcal{I}_{\mathfrak{p}}^{m,s}$ for any $m \ge 0$.

Again, using property (C3) to estimate $I_{2,2}^{m,j}$, we see that

$$|I_{2,2}^{m,j}| \;\le\; Cq^{-[\frac{1}{2}-\frac{1}{n_j}]} q^{-\frac{s}{n_j}} q^{-m\frac{1+r}{n_j}[n_j - d(f)]}$$

and so $|I_{2,2}^j| \ \leq$

$$Cq^{-[\frac{1}{2}-\frac{1}{n_j}]}q^{-s/n_j}, \ \ Csq^{-[\frac{1}{2}-\frac{1}{d(f)}]}q^{-s/d(f)}, \ \text{ or } Cq^{-[\frac{1}{2}+\frac{1}{n_j}-\frac{2}{d(f)}]}q^{-s/d(f)} \tag{28}$$

depending on whether $d(f) < n_j$, $d(f) = n_j$ or $n_j < d(f)$, respectively. Recall that $I_{2,2} = 0$ for polynomial congruences and so it is only when treating the character sums $\mathcal{S}_\chi$ that $I_{2,2}$ arises and in this case we are assuming $d(f) \geq 2$ in this section. In particular we have $|I_{2,2}| \leq Cq^{-s/d(f)}$ when $\mathcal{I}_\mathfrak{p} = \emptyset$ by (27) and the estimates

$$|I_{2,2}^j| \leq Cq^{-s/n_j}, \ \ |I_{2,2}^j| \leq Csq^{-s/d(f)} \ \text{ or } \ |I_{2,2}^j| \leq Cq^{-s/d(f)} \tag{29}$$

for $j \in \mathcal{I}_\mathfrak{p}$ if $d(f) < n_j$, $d(f) = n_j$ or $n_j < d(f)$, respectively.

4.2.2. *Estimates for I_2: the general case.* Here we describe the modifications needed when $\kappa_2/\kappa_1 \notin \mathbb{N}$ or $t \geq 2$. In the end we will arrive at the same estimates (24), (25) and (26) for $I_{2,1}$ and (29) for $I_{2,2}$ for general $t \geq 1$. Once we have succeeded in the initial change of variables indicated at the outset of Section 4.2.3, the argument for the estimates for $I_{2,1}$ are the same as in the case $t = 1$. However the argument to establish estimate (29) for general $t \geq 1$ will differ slightly from the case $t = 1$ described above.

We write

$$I_2 \ = \ \sum_{mN \leq s-1} q^{-(t+r)m} \int_{|x|=1} F(x)\, d\mu(x)$$

where

$$F(x) \ := \ \int_{|y|=1} \mathcal{C}(\pi^{-s+mN} f(x,y))\, d\mu(y).$$

We would like to make a change of variables $u = \phi(x)$ so that $u^t = x$. In order to carry this out, we fix a generator g of the multiplicative cyclic group $G := \mathbb{F}_q \setminus \{0\}$ of nonzero elements of our underlying finite field $\mathbb{F}_q = \bar{\mathfrak{o}}/\pi\bar{\mathfrak{o}}$ with $q = p^f$ elements. Set $d := \gcd(t, q-1)$ and recall that the tth powers of G are given by $G^t = \{g^d, g^{2d}, \dots, g^{(q-1)/d \cdot d} = g^{q-1} = 1\}$. Furthermore set

$$D \ := \ \{|x| = 1 : x = x_0 + x_1\pi + x_2\pi^2 + \cdots, \quad x_0 \in G^t\}$$

so that $\{|x| = 1\}$ has the decomposition

$$\{x \in \bar{\mathfrak{o}} : |x| = 1\} \ = \ D \cup gD \cup g^2D \cdots\cdots \cup g^{d-1}D \ = \ \bigcup_{e=0}^{d-1} g^e D$$

into d disjoint open sets. Therefore we can write

$$\int_{|x|=1} F(x)\, d\mu(x) \ = \ \sum_{e=0}^{d-1} \int_{g^eD} F(x)\, d\mu(x) \ = \ \sum_{e=0}^{d-1} \int_D F(g^e x) d\mu(x).$$

For each $x = x_0 + x_1\pi + \cdots \in D$, there are precisely d solutions $u_0 \in \mathbb{F}_q \setminus \{0\}$ to $u_0^t = x_0$, and by Hensel's lemma (note that if the characteristic of $\mathbb{F}_q$ is positive, it is larger than t by hypothesis) each such solution lifts uniquely to a solution $u \in \bar{\mathfrak{o}}$ of $u^t = x$. We single out the solution corresponding to $u_0 = g^\theta$ with $0 \leq \theta \leq (q-1)/d - 1$. This defines an analytic isomorphism $\phi : D \to \phi(D)$ so that if $u = \phi(x)$, then $u^t = x$. Therefore we can make the change of variables $u = \phi(x)$

(see [6] for a general change of variables formula in our setting) in each of the d integrals above,

$$\int_{|x|=1} F(x)\,d\mu(x) = \sum_{e=0}^{d-1} |t\cdot\mathbf{1}| \int_{\phi(D)} F(g^e u^t)\,d\mu(u)$$

so that (we throw in $t\cdot\mathbf{1}$ into our collection $\mathcal{A}$ in Section 2.5 to ensure that $|t\cdot\mathbf{1}| = |t\cdot\mathbf{1}|_{\mathfrak{p}} = 1$ for all $\mathfrak{p}\notin\mathcal{P}(f)$)

$$I_2 \;=\; \sum_{e=0}^{d-1} \sum_{mN\le s-1} q^{-(t+r)m} \int_{\phi(D)} F(g^e u^t)\,d\mu(u).$$

The function $F(x)$ is an integral in y and as before we make the change of variables $z = u^r y$ in the y integral which brings us to the analogue of (20) for general t:

$$I_2 \;=\; \sum_{e=0}^{d-1} \sum_{mN\le s-1} q^{-(1+r)m} \int_{\phi(D)} \left[\int_{|z|=1} \mathcal{C}(\pi^{-s+mN} h_e(z) u^N)\,d\mu(z)\right] d\mu(u)$$

where $h_e(z) = az^\beta \prod_{j=1}^M (z-\zeta_j g^{er})^{n_j}$. We now proceed exactly as in the case $t=1$, interchanging the order of integration and decomposing the z integral according to the size of $h_e(z)$, etc... The main difference is that the x integral over the set $\{|x|=1\}$ has now been replaced by a u integral over the set $\phi(D)$. From the definition of ϕ and D we see that

$$\phi(D) \;=\; \bigcup_{\theta=0}^{\frac{q-1}{d}-1} B_{q^{-1}}(u_\theta) \;=\; \bigcup_{\theta=0}^{\frac{q-1}{d}-1} \{u\in\bar{\mathfrak{o}} : |u-u_\theta|\le q^{-1}\}$$

is a disjoint union of $(q-1)/d$ balls where $u_\theta = g^\theta$. Hence $\mu(\phi(D)) = (1-q^{-1})/d$. For a fixed $0\le e\le d-1$ and $mN\le s-1$, we need to understand $\sum_{\ell\ge 0} H^\ell_{m,e}$ where

$$H^\ell_{m,e} \;:=\; \int_{\{|z|=1:|h_e(z)|=q^{-\ell}\}} d\mu(z) \int_{\phi(D)} \mathcal{C}(\pi^{-s+mN+\ell}[\pi^{-\ell}h_e(z)]u^N)\,d\mu(u)$$

so that

$$I_2 \;=\; \sum_{e=0}^{d-1} \sum_{mN\le s-1} q^{-(r+t)m} \sum_{\ell\ge 0} H^\ell_{m,e}.$$

As mentioned earlier there is a slight strengthening of property (C2), namely that integration over $\{|x|=1\}$ can be replaced by any finite union of disjoint balls $B_{q^{-1}}$ with radius q^{-1}, which holds for our $\mathcal{C}=\psi$ and $\mathcal{C}=\mathbf{1}_{\bar{\mathfrak{o}}}$. Therefore as before, the ℓ sum above vanishes when $\ell+mN-s\le -2$. By property (C1) the inner u integral in equals to $(1-q^{-1})/d$ for $\ell\ge s-mN$. Hence, proceeding exactly as in the $t=1$ case, we split $I_2 = I_{2,1}+I_{2,2}$ where

$$I_{2,1} = (1-q^{-1})/d \sum_{e=0}^{d-1} \sum_{mN\le s-1} q^{-(r+t)m} \sum_{\ell\ge s-mN} \mu\big(\{|z|=1 : |h_e(z)| = q^{-\ell}\}\big)$$

and $I_{2,2} =$

$$\sum_{e=0}^{d-1} \sum_{mN\le s-1} q^{-(r+t)m} \int_{\{|z|=1:|h_e(z)|=q^{-\ell_{m,s}}\}} \Big[\int_{\phi(D)} \mathcal{C}(\pi^{-1}[\pi^{-\ell_{m,s}}h_e(z)]u^N) d\mu(u)\Big] d\mu(z)$$

where as before $\ell_{m,s} = s - mN - 1$. If $\mathcal{C} = \mathbf{1}_{\bar{\mathfrak{o}}}$, the case for the problem of polynomial congruences, then $I_{2,2} = 0$.

As in the case $t = 1$, we see that the estimates (24), (25) and (26) for $I_{2,1}$ hold in the general case. The estimates (27), (28) and (29) for $I_{2,2}$, although true, require a modified argument. We write $I_{2,2} = \sum_{e=0}^{d-1} \sum_{mN \le s-1} q^{-(r+t)m} S_{e,m}$ where

$$S_{e,m} \;=\; \int_{\left\{|z|=1:|h_e(z)|=q^{-\ell_{m,s}}\right\}} \Big[\int_{\phi(D)} \mathcal{C}(\pi^{-1}[\pi^{-\ell_{m,s}} h_e(z)]u^N) d\mu(u)\Big] d\mu(z).$$

Suppose first that $\ell_{s,m} = s - mN - 1 \ge 1$. Then from (23), we have

$$S_{e,m} = \sum_{j \in \mathcal{I}_{\mathfrak{p}}^{m,s}} \int_{\{|z|=1:|z-g^{er}\zeta_j|=q^{-\ell_{m,s}/n_j}\}} \Big[\int_{\phi(D)} \mathcal{C}(\pi^{-1}[\pi^{-\ell_{m,s}} h_e(z)]u^N) d\mu(u)\Big] d\mu(z)$$

where as before $\mathcal{I}_{\mathfrak{p}}^{m,s} = \{j \in \mathcal{I}_{\mathfrak{p}} : n_j \mid \ell_{m,s}\}$. For each $j \in \mathcal{I}_{\mathfrak{p}}^{m,s}$, we make the change of variables $w = \pi^{-\ell_{m,s}/n_j}(z - g^{er}\zeta_j)$ so that

$$S_{e,m} = \sum_{j \in \mathcal{I}_{\mathfrak{p},m}} q^{-\ell_{m,s}/n_j} \int_{|w|=1} \Big[\int_{\phi(D)} \mathcal{C}(\pi^{-1} K_e w^{n_j} u^N) d\mu(u)\Big] d\mu(z)$$

where $K_e = a[g^{er}\zeta_j]^\beta \prod_{k \ne j} g^{ern_k}(\zeta_j - \zeta_k)^{n_k}$; in particular $|K_e| = |K_e|_{\mathfrak{p}} = 1$ for all $\mathfrak{p} \notin \mathcal{P}(f)$. The assumption $\ell_{m,s} \ge 1$ was used here.

Therefore we can write

$$I_{2,2} \;=\; \sum_{e=0}^{d-1} \sum_{mN \le s-2} \sum_{j \in \mathcal{I}_{\mathfrak{p}}^{m,s}} I_e^{m,j} \;+\; I_{2,2}^* \;:=\; \sum_{j \in \mathcal{I}_{\mathfrak{p}}} I_{2,2}^j \;+\; I_{2,2}^*$$

where

$$I_e^{m,j} = q^{-(r+t)m - \ell_{m,s}/n_j} \int_{\phi(D)} \Big[\int_{|w|=1} \mathcal{C}(\pi^{-1} K_e w^{n_j} u^N) d\mu(w)\Big] d\mu(w)$$

and

$$I_{2,2}^* \;=\; q^{-(t+r)(s-1)/N} \int_{\{|z|=1:|h_e(z)|=1\}} \Big[\int_{\phi(D)} \mathcal{C}(\pi^{-1}[h_e(z)]u^N) d\mu(u)\Big] d\mu(z).$$

The term $I_{2,2}^*$ appears only if $s \equiv 1 \bmod N$. If $\mathcal{I}_{\mathfrak{p}} = \emptyset$, then $\{|z| = 1 : |h_e(z)| = 1\} = \{|z| = 1\}$ and if $\mathcal{I}_{\mathfrak{p}} \ne \emptyset$,

$$\{|z| = 1 : |h_e(z)| = 1\} \;=\; \big\{z \in \bar{\mathfrak{o}} : |z| = 1\big\} \setminus \bigcup_{j \in \mathcal{I}_{\mathfrak{p}}} B_{q^{-1}}(z_{0,j})$$

where $g^{er}\zeta_j = z_{0,j} + z_{1,j}\pi + \cdots$ (of course for each $j \in \mathcal{I}_{\mathfrak{p}}$, $g^{er}\zeta_j \in \bar{\mathfrak{o}}$). Whether $\mathcal{I}_{\mathfrak{p}}$ is or is not empty, we interchange the order of integration so that

$$I_{2,2}^* = q^{-(t+r)(s-1)/N} \Big[\int_{\phi(D)} \Big[\int_{|z|\le 1} \mathcal{C}(\pi^{-1} u^N h_e(z)) d\mu(z)\Big] d\mu(u) \;+\; E\Big]$$

where $|E| \le Cq^{-1}$. When $\mathcal{C} = \psi$, the integral $\int_{|z|\le 1} \psi(\pi^{-1}u^N h_e(z)) d\mu(z)$ is a character sum over a finite field for each fixed u with $|u| = 1$ and therefore we can appeal to A. Weil's work to obtain the bound

$$|I_{2,2}^*| \;\le\; Cq^{-[\frac{1}{2} - \frac{1}{d(f)}]} q^{-s/d(f)} \tag{30}$$

in this case.

Using property (C3) to estimate $I_e^{m,j}$, we see that

$$|I_e^{m,j}| \ \le \ Cq^{-[\frac{1}{2}-\frac{1}{n_j}]}q^{-\frac{s}{n_j}}q^{-m\frac{t+r}{n_j}[n_j-d(f)]}$$

and so $|I_{2,2}^j| \ \le$

$$Cq^{-[\frac{1}{2}-\frac{1}{n_j}]}q^{-s/n_j}, \ \ Csq^{-[\frac{1}{2}-\frac{1}{d(f)}]}q^{-s/d(f)}, \ \text{ or } Cq^{-[\frac{1}{2}+\frac{1}{n_j}-\frac{2}{d(f)}]}q^{-s/d(f)} \tag{31}$$

depending on whether $d(f) < n_j$, $d(f) = n_j$ or $n_j < d(f)$, respectively. Recall that $I_{2,2} = 0$ for polynomial congruences and so it is only when treating the character sums $\mathcal{S}_\chi$ that $I_{2,2}$ arises and in this case we are assuming $d(f) \ge 2$ in this section. In particular we have $|I_{2,2}^*| \le Cq^{-s/d(f)}$ by (30) and the estimates

$$|I_{2,2}^j| \le Cq^{-s/n_j}, \ \ |I_{2,2}^j| \le Csq^{-s/d(f)} \ \text{ or } \ |I_{2,2}^j| \le Cq^{-s/d(f)} \tag{32}$$

for $j \in \mathcal{I}_\mathfrak{p}$ if $d(f) < n_j$, $d(f) = n_j$ or $n_j < d(f)$, respectively.

Finally we observe that if $j \in \mathcal{I}_\mathfrak{p}^{m,s}$, then $n_j \mid \ell_{m,s}$ and this implies that $\gcd(N, n_j) \mid s-1$. Therefore if $\gcd(n_j, N) \ge 2$ and $s \equiv 0 \bmod \gcd(N, n_j)$, then $j \notin \mathcal{I}_\mathfrak{p}^{m,s}$ for any $m \ge 0$. This will be important when we turn our attention to the lower bound (10) in Theorem 1.3.

4.2.3. *Putting the estimates together for I.* We combine the estimates derived above to give bounds for

$$I \ = \ I_1 + I_2 \ = \ I_1 \ + \ \sum_{j \in \mathcal{I}_\mathfrak{p}} I_{2,1}^j \ + \ I_{2,2}.$$

First we consider upper bounds for I and we begin by treating those f not in any E_m, $m \ge 1$. Then by Lemma 2.2 we see that $m_K(f) \ge d(f)$ if and only if there is some multiplicity $n_j \ge d(f)$ (and so necessarily the multiplicity n_j is associated to a root $\zeta_j \in K$). Therefore the estimates (18), (24) (valid for general $t \ge 1$), (30) and (32) give the desired bound for I from above; when $\mathfrak{p} \notin \mathcal{P}(f)$,

$$|I| \ \le \ Cs^{\nu(f)}q^{-s/h(f)} \tag{33}$$

where $C = C_{deg(f)}$. This holds for general f if $\mathcal{C} = \mathbf{1}_{\bar{\mathfrak{o}}}$ and for f with $d(f) \ge 2$ if $\mathcal{C} = \psi$; recall that in this section, when $\mathcal{C} = \psi$, we are assuming that $2 \le d(f)$ in which case $i(f) = \nu(f)$ (see Section 5 for the case of character sums when $d(f) < 2$).

When $f \in E_m$, $m \ge 2$, there are two conjugate roots ζ, ζ^* of degree 2 over K, $m_K(f) = 0$, $m = d(f) = h(f)$ and $n_1 = n_2 = m$. If $\zeta, \zeta^* \in \bar{K}$, then $i_\mathfrak{p}(f) = \nu_\mathfrak{p}(f) = 1$ and $\mathcal{I}_\mathfrak{p} = \{1, 2\}$. On the other hand if $\zeta, \zeta^* \notin \bar{K}$, then $i_\mathfrak{p}(f) = \nu_\mathfrak{p}(f) = 0$, $\mathcal{I}_\mathfrak{p} = \emptyset$ and so $I_{2,1} = 0$. Hence (18), (24), (30) and (32) show that

$$|I| \ \le \ Cs^{\nu_\mathfrak{p}(f)}q^{-s/h(f)} \tag{34}$$

when $\mathfrak{p} \notin \mathcal{P}(f)$. When $f \in E_1$, $m_K(f) = 0$ and $d(f) = 1$. The estimates for the character sum S_χ are treated in Section 4.8; note that for the character sum, $f \in E_1$ is not an exceptional case and we obtain uniform bounds for all $s \ge 1$ and $\mathfrak{p} \notin \mathcal{P}(f)$. This leaves establishing (34) for polynomial congruences when $f \in E_1$. Recall that $I_{2,2} = 0$ for polynomial congruences. If $\zeta, \zeta^* \in \bar{K}$, then $\nu_\mathfrak{p}(f) = 1$ and $\mathcal{I}_\mathfrak{p} = \{1, 2\}$. Therefore (18) and (24) give the desired estimate. On the other hand

if $\zeta, \zeta^* \notin \bar{K}$, then $\nu_{\mathfrak{p}}(f) = 0$, $\mathcal{I}_{\mathfrak{p}} = \emptyset$ and so $I_{2,1} = 0$ implying $I_2 = 0$. Hence $I = I_1$ and so (18) alone gives the desired estimate.

Next we will show that for polynomial congruences $\mathcal{C} = \mathbf{1}_{\bar{\mathfrak{o}}}$, the lower bound

$$cs^{\nu(f)}q^{-s/h(f)} \ \leq \ I \tag{35}$$

holds for infinitely many $s \geq 1$, for some $c = c_{deg(f)} > 0$ and $\mathfrak{p} \notin \mathcal{P}(f)$ when f does not lie in any E_m, $m \geq 1$. Since $\mathcal{N}(f; \pi^s) \geq I$, the bound (35) establishes the lower bound (9) in Theorem 1.3. To prove (35) we will restrict to $s \equiv 0 \bmod N \prod_{j \in \mathcal{I}_{\mathfrak{p}}} n_j$ and in particular $s \equiv 0 \bmod N$ so (19) implies $I \geq I_1 \geq cq^{-s/d(f)}$ for these values of s. This proves (35) when $m_K(f) < d(f)$ in which case $\nu(f) = 0$ and $d(f) = h(f)$. When $m_K(f) \geq d(f)$, Lemma 2.2 implies that there is a unique root $\zeta_{j_*} \in K$ such that $n_{j_*} \geq d(f)$. and so (26) implies $I \geq I_{2,1}^{j_*} \geq cs^{\nu(f)}q^{-s/h(f)}$ whenever $s \equiv 0 \bmod n_{j_*}$. This establishes (35) and therefore (9) when $f \notin E_m$ for any $m \geq 1$. When $f \in E_m$ for some $m \geq 1$, then $h(f) = d(f) = m = n_1 = n_2$. If the conjugate roots ζ, ζ_* do not belong to $\bar{K}$, then $\nu_{\mathfrak{p}}(f) = 0$ and (19) implies $I \geq I_1 \geq cq^{-s/d(f)}$ if $s \equiv 0 \bmod N$. If the conjugate roots belong to $\bar{K}$, then $\nu_{\mathfrak{p}}(f) = 1$, $\mathcal{I}_{\mathfrak{p}} = \{1, 2\}$ and (26) implies $I \geq I_{2,1}^1 \geq csq^{-s/d(f)}$ if $s \equiv 0 \bmod m$. Hence (35) (and hence (9)) holds for $f \in E_m$ with $\nu(f)$ replaced by $\nu_{\mathfrak{p}}(f)$.

We now show that when $\mathcal{C} = \psi$ (that is for character sums), f is not linear and $f \notin E_m$ for any $m \geq 2$,

$$cs^{i(f)}q^{-s/h(f)} \ \leq \ |I| \tag{36}$$

holds for infinitely many $s \geq 1$, for some $c = c_{deg(f)} > 0$ and $\mathfrak{p} \notin \mathcal{P}(f)$. Recall that in this section, we are assuming that $d(f) \geq 2$ when treating character sums; the case when $d(f) < 2$ is treated in Section 5. Nevertheless the analysis we give here will handle certain situations when $d(f) < 2$; more precisely, the analysis will cover those f with $m_K(f) < d(f)$ (except for the case when $f \in E_1$ which we treat separately in Section 4.8) and also those f with $d(f) \leq m_K(f)$ but either $2 < m_K(f)$ or $2 = d(f) = m_K(f)$. This will help alleviate the analysis in Section 5.

Note that $f(x, y) = ay + bx$ is linear if and only if $N = t\alpha + r\beta + trn = 1$ and so we may assume without loss of generality that $N \geq 2$. Furthermore we will restrict ourselves to $s \equiv 0 \bmod N \prod_{j \in \mathcal{I}_{\mathfrak{p}}} n_j$ when establishing (36) and so in particular $s \not\equiv 1 \bmod N$ since $N \geq 2$ which implies that $I_{2,2}^* = 0$ for these values of s. We consider first the case $m_K(f) \geq d(f)$ (then $h(f) = m_K(f) \geq d(f)$) and so by Lemma 2.2, there is a unique root $\zeta_{j_*} \in K$ with multiplicity $n_{j_*} = h(f) \geq d(f)$. Suppose first $n_{j_*} > 2$ in which case we will use the improved bound (31) for $I_{2,2}^{j_*}$ so that for any $\epsilon > 0$, $|I_{2,2}^{j_*}| \leq \epsilon s^{\nu(f)}q^{-s/h(f)}$ if q is large enough and this is the case when $\mathfrak{p} \notin \mathcal{P}(f)$. For other $j \in \mathcal{I}_{\mathfrak{p}}$ with $j \neq j_*$, we have $n_j < d(f)$ and we will use the bound in (31)

$$|I_{2,2}^j| \ \leq \ Cq^{-[\frac{1}{2} + \frac{1}{n_j} - \frac{2}{d(f)}]}q^{-s/d(f)},$$

noting that the exponent $\frac{1}{2} + \frac{1}{n_j} - \frac{2}{d(f)}$ is always strictly positive. This is certainly the case if $d(f) \geq 2$ and if $d(f) < 2$, then $n_j = 1$ and so the exponent still remains

strictly positive as long as $d \geq 4/3$. We claim that the existence of two multiplicities, $n_j = 1 < d(f) \leq n_{j_*}$ rules out the possibility that $d(f) \leq 4/3$. If $d(f) \leq 4/3$, then

$$3rt \leq tr(1 + n_{j_*}) \leq trn \leq N = d(f)(r + t) \leq (4/3)(r + t)$$

which implies that $9rt \leq 4t + 4r$ and this is easily seen to be impossible. Therefore for any $\epsilon > 0$ and for any $j \in \mathcal{I}_{\mathfrak{p}}$ with $j \neq j_*$, we have the same estimate as for $I^{j_*}_{2,2}$; namely, $|I^j_{2,2}| \leq \epsilon s^{i(f)} q^{-s/h(f)}$ for q large enough. Finally since $s \equiv 0 \bmod n_{j_*}$, (26) implies $I_{2,1} \geq c s^{i(f)} q^{-s/h(f)}$ and so for q large enough,

$$|I| = |I_1 + I_{2,1} + I_{2,2}| \geq I_1 + I_{2,1} - \epsilon s^{i(f)} q^{-s/h(f)} \geq (c/2) s^{i(f)} q^{-s/h(f)}$$

since $I_1 \geq 0$. This establishes (36) when $n_{j_*} = h(f) > 2$ and we turn now to the case $n_{j_*} = m_K(f) = d(f) = 2$. In this case, $N = d(f)(t + r) = 2(t + r)$ and so $\gcd(n_{j_*}, N) = 2$ implying $I^{j_*}_{2,2} = 0$; recall that

$$I^{j_*}_{2,2} = \sum_{e=0}^{d-1} \sum_{\substack{mN \leq s-2 \\ n_{j_*} | \, \ell_{m,s}}} I^{m,j_*}_e$$

and $n_{j_*} = 2 \nmid \ell_{m,s} = s - mN - 1$ for any $m \geq 0$ since $N = 2(t + r)$ and $s \equiv 0 \bmod n_{j_*} = 2$. All other $j \in \mathcal{I}_{\mathfrak{p}}$ with $j \neq j_*$ must satisfy $n_j = 1$ since $n_j < d(f) = 2$ and so the analysis above shows $|I_{2,2}| \leq \epsilon s^{i(f)} q^{-s/h(f)}$ if q is large enough which leads to the bound (36) as before.

We turn to the case $m_K(f) < d(f)$ and here, again by Lemma 2.2 (recall that we are not treating $f \in E_1$, see Section 4.8 for this case), we have $n_j < d(f)$ for every $j \in \mathcal{I}_{\mathfrak{p}}$. If $d(f) > 4/3$, the improved estimate (31) shows that for each $j \in \mathcal{I}_{\mathfrak{p}}$, $|I^j_{2,2}| \leq \epsilon q^{-s/d(f)}$ for q large enough. If $d(f) \leq 4/3$, then necessarily $\alpha = \beta = 0$ and either $n = 1$ or $n = 2$. If $n = 1$, then $f(x, y) = a(y^t - \zeta x^r)$ for some $\zeta \in K$ and the character sum $S_\chi(f; \pi^s)$ can be easily evaluated when $s \equiv 0 \bmod N = rt$ (see for example, Section 5); in particular one verifies that (36) or more generally the lower bound (10) in Theorem 1.3 in this case. When $n = 2$, then necessarily $t = 1$, $r = 2$, $N = 4$, $d(f) = 4/3$ and so $f(x, y) = a(y - \zeta x^2)(y - \eta x^2)$ for some $\zeta \neq \eta \in K$. In this case we can tweak the argument above and improve upon the estimate (32) for each $I^j_{2,2}$; in fact, since $N = 4$ and $s \equiv 0 \bmod N$ in this case, the terms $mN = s - 1, mN = s - 2$ and $mN = s - 3$ do not arise in the m sum defining $I^j_{2,2}$ leading to the improved bound

$$|I^j_{2,2}| \ \leq \ C q^{-[\frac{1}{2} + \frac{3}{n_j} - \frac{4}{d(f)}]} q^{-s/d(f)}.$$

Since $n_1 = n_2 = 1$ and $d(f) = 4/3$ in this case, we again can conclude $|I^j_{2,2}| \leq \epsilon q^{-s/d(f)}$ if q is large enough. Altogether, when $m_K(f) < d(f)$ and $f \notin E_1$, we have $|I_{2,2}| \leq \epsilon q^{-s/d(f)}$ if q is large enough and so, since $I_1 \geq c q^{-s/d(f)}$ when $s \equiv 0 \bmod N$ by (19),

$$|I| = |I_1 + I_{2,1} + I_{2,2}| \geq I_1 + I_{2,1} - \epsilon q^{-s/d(f)} \geq (c/2) q^{-s/d(f)} = (c/2) s^{i(f)} q^{-s/h(f)}$$

since $I_{2,1} \geq 0$. This establishes (36) when $m_K(f) < d(f)$ and $f \notin E_1$.

When $f \in E_m$ for some $m \geq 2$, the estimate (36) holds with the exponent $i(f)$ replaced by $i_{\mathfrak{p}}(f)$. When the conjugate pair ζ, ζ^* lies outside $\bar{K}$, $i_{\mathfrak{p}}(f) = 0$ and

$\mathcal{I}_{\mathfrak{p}} = \emptyset$. Hence $I_{2,1} = I_{2,2} = 0$ when s is restricted to $s \equiv 0 \bmod N$ and so $I = I_1 \geq cq^{-s/d(f)}$ by (19) when $s \equiv 0 \bmod N$, proving (36) with $i(f) = i_{\mathfrak{p}}(f)$ in this case. When the conjugate pair belongs to $\bar{K}$, then $i_{\mathfrak{p}}(f) = 1$ and $\mathcal{I}_{\mathfrak{p}} = \{1, 2\}$ lists the two multiplicities $n_1 = n_2 = m = d(f) = h(f)$ corresponding to the roots ζ and ζ^*. The bound (26) shows that $I_1 + I_{2,1} \geq I_{2,1} \geq csq^{-s/h(f)}$ for $s \equiv 0 \bmod m$. Proceeding as in the analysis above when $f \notin E_m$, we see that $I_{2,2} = 0$ when $s \equiv 0 \bmod N$ since then $I^*_{2,2} = 0$ and $I^j_{2,2} = 0$ for both $j = 1$ and $j = 2$; in fact, $n_1 = n_2 = m \geq 2$ never divides $\ell_{k,s} = s - kN - 1$ for any $k \geq 0$ if $s \equiv 0 \bmod N$. In fact, writing $s = k_* N$ and noting $N = 2m$, we have $\ell_{k,s} = 2m(k_* - k) - 1$ and so m does not divide $\ell_{k,s}$ for any k since $m \geq 2$. Therefore $I = I_1 + I_{2,1} \geq csq^{-s/h(f)}$ in this case, establishing (36) with $i(f)$ replaced with $i_{\mathfrak{p}}(f)$.

We note that when $f \in E_1$, the multiplicities n_1, n_2 of the roots ζ and ζ^* are equal to 1 which divides $\ell_{k,s}$ for every k and so $I_{2,2}$ will give a nontrivial contribution to the character sum $\mathcal{S}_\chi$. In fact the contribution $I_{2,2}$ cancels exactly with $I_{2,1}$ for $f \in E_1$ when $s \equiv 0 \bmod N = 2$ (see Section 4.8).

4.3. **Estimates for II.** Next we treat II which we write as

$$II \;=\; \sum_{\substack{k_1,k_2\geq 0\\ tk_2<rk_1}} q^{-k_1-k_2} \iint_{|x|=1,|y|=1} \mathcal{C}(\pi^{-s+k_1\alpha+k_2(\beta+tn)} f_{k_1,k_2}(x,y))\, d\mu(x) d\mu(y)$$

where

$$f_{k_1,k_2}(x,y) = ax^\alpha y^{\beta+tn} + c\pi^{rk_1-tk_2} x^{\alpha+r} y^{\beta+t(n-1)} + \cdots + b\pi^{n(rk_1-tk_2)} x^{\alpha+rn} y^\beta.$$

By property (C2) we see that the above sum vanishes when $k_1\alpha + k_2(\beta+tn) \leq s-2$ and therefore $II = II_1 + II_2$ where

$$II_1 \;=\; (1-q^{-1})^2 \sum_{\substack{tk_2<rk_1\\ s\leq k_1\alpha+k_2(\beta+tn)}} q^{-k_1-k_2},$$

using property (C1), and

$$II_2 \;=\; \sum_{\substack{tk_2<rk_1\\ k_1\alpha+k_2(\beta+tn)=s-1}} q^{-k_1-k_2} \iint_{|x|=1,|y|=1} \mathcal{C}(\pi^{-1} a x^\alpha y^{\beta+tn})\, d\mu(x) d\mu(y).$$

When we turn to establish (10) in Theorem 1.3 for character sums, we will ensure that s lies along the subsequence $s \equiv 0 \bmod \gcd(\alpha, \beta+tn)$ so that if $\gcd(\alpha, \beta+tn) \geq 2$, the sum defining II_2 is empty for these values of s. On the other hand, if $\gcd(\alpha, \beta+tn) = 1$, then the double integral above is $-(1-q^{-1})q^{-1}$; see Section 6 for this easy computation. This gives a better bound than the $q^{-1/2}$ bound which property (C3) gives and we will use this improvement for (10).

In the summand defining II_1, we have the bounds

$$(s - k_1\alpha)/(\beta + tn) \;\leq\; k_2 \;<\; (r/t)k_1$$

and so we can preform the k_2 sum first to bound

$$II_1 \ \leq \ Cq^{-s/(\beta+tn)} \sum_{ts/N<k_1} q^{-k_1[1-\alpha/(\beta+tn)]}. \tag{37}$$

We divide the analysis into three cases: (A) $\alpha < d(f)$, (B) $\alpha = d(f)$ and (C) $\alpha > d(f)$. This division into three cases is equivalent to the exponent $[1-\alpha/(\beta+tn)]$ in (37) being positive, zero and negative, respectively. By Lemma 2.2, case (B) implies $m_K(f) = d(f)$ and case (C) implies $m_K(f) > d(f)$. Therefore in these cases, we have $\alpha = h(f)$.

For case (A), we use (37) to see that

$$II_1 \ \leq \ Cq^{-s/d(f)} \tag{38}$$

for some constant $C > 0$ depending only on the degree of f. For cases (B) and (C), we divide $II_1 = II_{1,1} + II_{1,2}$ into two parts by splitting the k_1 sum,

$$II_{1,1} \ = \sum_{\substack{tk_2<rk_1,\ k_1\leq s/\alpha \\ s\leq k_2(\beta+tn)+k_1\alpha}} q^{-k_1-k_2}, \quad II_{1,2} \ = \sum_{\substack{tk_2<rk_1,\ s/\alpha\leq k_1 \\ s\leq k_2(\beta+tn)+k_1\alpha}} q^{-k_1-k_2}.$$

For $II_{1,2}$ in cases (B) and (C), we simply use the restrictions $k_1 \geq s/\alpha$ and $k_2 \geq 0$ to obtain

$$II_{1,2} \ \leq \ Cq^{-s/\alpha} \ = \ Cq^{-s/h(f)}. \tag{39}$$

For $II_{1,1}$ in cases (B) and (C), we use (37) to see that

$$II_{1,1} \ \leq \ Csq^{-s/h(f)} \quad \text{and} \quad II_{1,1} \ \leq \ Cq^{-s/h(f)}, \tag{40}$$

respectively.

For II_2, if $\mathcal{C}$ satisfies property (C3)' (the case of polynomial congruences), then $II_2 = 0$ and so we need to bound II_2 only for character sums and in this case we are assuming $d(f) \geq 2$. Using property (C3) to bound the integral in II_2 by $q^{-1/2}$, we obtain

$$|II_2| \ \leq \ Cq^{-1/2}q^{-(s-1)/(\beta+tn)} \sum_{ts/N\leq k_1\leq (s-1)/\alpha} q^{-k_1[1-\alpha/(\beta+tn)]}$$

and splitting the analysis into cases (A), (B) and (C) as above, we conclude that if $h(f) \geq 2$ (which is implied by our underlying assumption $d(f) \geq 2$),

$$|II_2| \leq Cq^{-s/d(f)}, \quad |II_2| \leq Csq^{-s/d(f)} \ \text{ and } \ |II_2| \leq Cq^{-s/\alpha}, \tag{41}$$

respectively; in fact the initial estimate for II_2 implies $|II_2| \leq Cq^{-[1/2-1/d(f)]}q^{-s/d(f)}$, $|II_2| \leq Cq^{-[1/2-1/d(f)]}sq^{-s/d(f)}$ and $|II_2| \leq q^{-[1/2-1/h(f)]}q^{-s/h(f)}$ in the respective cases (A), (B) and (C). This shows that if $h(f) > 2$, then for any $\epsilon > 0$,

$$|II_2| \ \leq \ \epsilon s^{i(f)}q^{-s/h(f)} \tag{42}$$

if q is large enough and this is the case when $\mathfrak{p} \notin \mathcal{P}(f)$. We will use (42) for the proof of (10) in Theorem 1.3 (recall that for polynomial congruences, $II_2 = 0$).

Putting (38), (39), (40) and (41) together gives us the favourable upper bound

$$|II| \ \leq \ C\, s^{\nu(f)}q^{-s/h(f)} \tag{43}$$

for $\mathcal{C} = \mathbf{1}_{\bar{0}}$, polynomial congruences, and

$$|II| \ \leq \ C\, s^{i(f)} q^{-s/h(f)} \tag{44}$$

for $\mathcal{C} = \psi$, character sums, assuming $d(f) \geq 2$.

By the remark following the definition of II_2, if $\gcd(\alpha, \beta + tn) = 1$, then the estimates (41) improve to

$$|II_2| \ \leq \ q^{-1+1/h(f)} s^{i(f)} q^{-s/h(f)} \tag{45}$$

and so in this case, (42) holds if $h(f) > 1$.

Recall that in Section 4.2.3, we successfully bounded $|I|$ from below (for character sums) for infinitely many $s \geq 1$ for any nonlinear $f \notin E_1$ satisfying $m_K(f) < d(f)$ or $m_K(f) \geq d(f)$ such that either $m_K(f) > 2$ or $m_K(f) = d(f) = 2$. To bring II in line with these results let us observe that II_2 satisfies (42) for infinitely many $s \geq 1$ when $f \notin E_1$ and when $m_K(f) < d(f) \leq 2$ holds, or $m_K(f) > 2 \geq d(f)$ holds or $m_K(f) = d(f) = 2$ holds. Here we will restrict to those s satisfying $s \equiv 0 \bmod \gcd(\alpha, \beta + tn)$.

We consider two situations. First, suppose that $\gcd(\alpha, \beta + tn) \geq 2$. Then $II_2 = 0$ since $s \equiv 0 \bmod \gcd(\alpha, \beta + tn)$ and so (42) is trivially satisfied in this case. Second, suppose that $\gcd(\alpha, \beta + tn) = 1$ in which case we can use (45) and reduce to the situation where $d(f) \leq 1$. Hence we need only consider the cases when $m_K(f) < d(f) \leq 1$ and when $m_K(f) > 2 > 1 \geq d(f)$ and we will show that these situations cannot arise if $f \notin E_1$.

If it were the case that $m_K(f) > 2 > 1 \geq d(f)$, then there would be a unique root $\zeta_* \in K$ with multiplicity $n_* \geq 3$ and hence $3rt/(t + r) \leq d(f) \leq 1$ which is clearly impossible. If is were the case that $m_K(f) < d(f) \leq 1$, then $m_K(f)$ must be zero and so there must be at least two nonzero roots $\zeta, \zeta_* \notin K$ and hence $n \geq 2$. But this implies $(t\alpha + r\beta + nrt)/(t + r) = d(f) \leq 1$ which is impossible unless $\alpha = \beta = 0$, $t = r = 1$ and $n = 2$. However this is precisely the case when $f \in E_1$.

4.4. **Estimates for III.** The analysis for the term III is the same as for II. We write III as

$$III \ = \ \sum_{\substack{k_1, k_2 \geq 0 \\ rk_1 < tk_2}} q^{-k_1 - k_2} \iint_{|x|=1, |y|=1} \mathcal{C}(\pi^{-s + k_1(\alpha + rn) + k_2\beta} g_{k_1,k_2}(x, y))\, d\mu(x) d\mu(y)$$

where

$$g_{k_1,k_2}(x, y) = bx^{\alpha + rn} y^{\beta} + \cdots + a\pi^{n(tk_2 - rk_1)} x^{\alpha} y^{\beta + tn}.$$

By property (C2) we see that the above sum vanishes when $k_1(\alpha + rn) + k_2\beta \leq s - 2$ and therefore $III = III_1 + III_2$ where

$$III_1 \ = \ (1 - q^{-1})^2 \sum_{\substack{rk_1 < tk_2 \\ s \leq k_1(\alpha + rn) + k_2\beta}} q^{-k_1 - k_2},$$

using property (C1), and

$$III_2 \;=\; \sum_{\substack{rk_1<tk_2\\ k_1(\alpha+rn)+k_2\beta=s-1}} q^{-k_1-k_2}\iint_{|x|=1,|y|=1}\mathcal{C}(\pi^{-1}bx^{\alpha+rn}y^{\beta})\,d\mu(x)d\mu(y).$$

The same estimates for II hold for III with the same proofs. So we will only state them. The following estimates hold:

$$|III| \;\le\; Cs^{\nu(f)}q^{-s/h(f)} \tag{46}$$

for polynomial congruences and

$$|III| \;\le\; Cs^{i(f)}q^{-s/h(f)} \tag{47}$$

for character sums, assuming $d(f)\ge 2$. For polynomial congruences, $III_2=0$ and for character sums, we have for every $\epsilon>0$,

$$|III_2| \;\le\; \epsilon s^{i(f)}q^{-s/h(f)} \tag{48}$$

if q large enough whenever $m_K(f)<d(f)$ or $d(f)\le m_K(f)$ with $2<m_K(f)$ or $2=m_K(f)=d(f)$.

4.5. **The upper bounds in Theorem 1.3.** Since

$$\iint_{\bar{\mathfrak{o}}\times\bar{\mathfrak{o}}}\mathcal{C}(\pi^{-s}f(x,y))\,d\mu(x)d\mu(y) \;=\; I+II+III,$$

we combine the estimates (33), (43) and (46) for $\mathcal{C}=\mathbf{1}_{\bar{\mathfrak{o}}}$ to see that the upper bound in (8) holds for general quasi-homogeneous $f\notin E_m$ for any $m\ge 1$, with the appropriate modifications, the Varchenko exponent $\nu(f)$ replaced by $\nu_{\mathfrak{p}}(f)$, when $f\in E_m$.

When $\mathcal{C}=\psi$, we combine the estimates (33), (44) and (47) for $\mathcal{C}=\psi$ to see that the bound (7) in Theorem 1.3 holds for f with $d(f)\ge 2$, with the appropriate modifications when $f\in E_m, m\ge 2$ lies in one of the exceptional classes. The case $f\in E_1$ for character sums is treated in Section 4.8 below.

4.6. **The lower bounds** (9) **and** (10) **in Theorem 1.3.** As we observed earlier, for the problem of polynomial congruences, since $\mathcal{N}(f;\pi^s)\ge I$, the bound (9) in Theorem 1.3 follows from (35) whenever f does not belong to any exceptional class $E_m, m\ge 1$. Similarly, when $f\in E_m$ for some $m\ge 1$, we have

$$\mathcal{N}(f;\pi^s)\ge I\ge cs^{\nu_{\mathfrak{p}}(f)}q^{-s/h(f)}$$

for infinitely many $s\ge 1$,

For the problem of character sums, we will show that (10) holds for any nonlinear $f\notin E_m, m\ge 1$ whenever $m_K(f)<d(f)$ or whenever $d(f)\le m_K(f)$ and either $2<m_K(f)$ or $2=m_K(f)=d(f)$. The case $f\in E_1$ is treated in Section 4.8 and the remaining cases will be treated in Section 5. The argument establishing (36) showed $I=P+E$ where $P\ge 0$, $P\ge cs^{i(f)}q^{-s/h(f)}\ge 0$ and $|E|\le (1/2)P$ for

infinitely many $s \geq 1$. Hence $I+II+III = [P+II_1+III_1]+[E+II_2+III_2]$ and by (42), (48) and the fact that $II_1, III_1 \geq 0$, we see that for infinitely many $s \geq 1$,

$$|I+II+III| \geq P - |E| - |II_2| - |III_2| \geq (c/2)\, s^{i(f)} q^{-s/h(f)} - (c/4) s^{i(f)} q^{-s/h(f)}$$

if q large enough. The same argument shows that

$$\mathcal{S}_\chi(f;\pi^s) = |I+II+III| \geq c s^{i_{\mathfrak{p}}(f)} q^{-s/h(f)}$$

for infinitely many $s \geq 1$ whenever $f \in E_m$ for some $m \geq 2$.

4.7. **The lower bound in** (8) **of Theorem 1.3.** To complete the proof of Theorem 1.3 for polynomial congruences, we need to establish the lower bound in (8), with the appropriate modifications when $f \in E_m$ for some $m \geq 1$. This is a bound for the number of polynomial congruences $\mathcal{N}(f;\pi^s) = I+II+III$ so $I = I_1 + I_{2,1}$, $II = II_1$ and $III = III_1$ and of course each of the terms are nonnegative. In the cases $m_K(f) > d(f)$ and $m_K(f) = d(f)$ (the two cases where $\mathcal{I}_{\mathfrak{p}}$ is necessarily nonempty), the lower bound in (8) follows from (25); in fact in these cases, the factor q^{-2} can be replaced by q^{-1}. When $f \in E_m$ for some $m \geq 1$ where the conjugate roots ζ, ζ^* lie in $\bar{K}_{\mathfrak{p}}$, then $\nu_{\mathfrak{p}}(f) = 1$, $\mathcal{I}_{\mathfrak{p}} = \{1,2\}$, and (25) again implies $\mathcal{N}(f;\pi^s) \geq csq^{-s/h(f)} q^{-1}$ in this case.

In order to establish (8) in case $m_K(f) < d(f)$, we need a bound from below for

$$I_1 + II_1 + III_1 \;=\; (1-q^{-1})^2 \sum_{\substack{k_1,k_2 \geq 0 \\ s \leq k_1\alpha + k_2\beta + \min(rk_1, tk_2)n}} q^{-k_1-k_2}.$$

We claim that the uniform bound

$$cq^{-s/d(f)} q^{-2} \;\leq\; I_1 + II_1 + III_1 \tag{49}$$

holds which will complete the proof of (8) in Theorem 1.3 when $f \notin E_m$ for any $m \geq 1$. Writing $s \geq 1$ as $s = Nm_* + T$ for some integers $m_* \geq 0$ and $0 \leq T \leq N-1$, we define the integer $0 \leq L < t$ so that $L - 1 < (Tt)/N \leq L$. With L, we define the integers $k_1^* := tm_* + L$ and k_2^* so that

$$k_2^* - 1 \;<\; rm_* + \frac{T}{\beta + tn} - \frac{\alpha L}{\beta + tn} \;\leq\; k_2^*.$$

One easily checks that the integer k_2^* defined above is nonnegative. We consider two cases: when $tk_2^* \leq rk_1^*$ and when $rk_1^* < tk_2^*$. In the first case, we see from the definition k_2^*, $s \leq k_1^*\alpha + k_2^*(\beta + tn)$. In the second case one checks that $s \leq k_1^*(\alpha + rn) + \beta k_2^*$ hold, or equivalently,

$$\frac{T - (\alpha + rn)L}{\beta} \;\leq\; \frac{T - \alpha L}{\beta + tn}$$

which boils down to $(Tn)/N \leq L$. Hence in either case,

$$I_1 + II_1 + III_1 \gtrsim q^{-k_1^* - k_2^*} \geq q^{-s/d(f)} q^{T/d(f)} q^{-[T-\alpha L]/(\beta+tn) - L - 1} \geq q^{-s/d(f)} q^{\alpha/(\beta+tn) - 2}$$

which gives the bound in (49). Here we used $(Tt)/N \geq L - 1$. When $f \in E_m$ for some $m \geq 1$ where the conjugate roots ζ, ζ^* do not lie in $\bar{K}_{\mathfrak{p}}$, then $\nu_{\mathfrak{p}}(f) = 0$, $\mathcal{I}_{\mathfrak{p}} = \emptyset$ and the bound (49) implies that $\mathcal{N}(f;\pi^s) \geq cq^{-s/h(f)} q^{-2}$ in this case.

Let us look now at the example $f(x,y) = y^4 - 2x^6 \in \mathbb{Z}[X,Y]$ mentioned after the statement of Theorem 1.2. Here $h(f) = 12/5$, $\nu(f) = 0$ and when we restrict to $s \equiv 1 \bmod 12$, we have

$$I_1 + II_1 + III_1 = (1-q^{-1})^2 \sum_{s \leq 2\min(2k_1, k_2)} q^{-k_1-k_2} \leq cq^{-5s/12} q^{-19/12}.$$

Furthermore if $p \equiv 3$ or $5 \bmod 8$, then $\pm\sqrt{2} \notin \mathbb{Q}_p$ and so $I_{2,1} = 0$. Therefore for these values of p,

$$\mathcal{N}(f; p^s) = I + II + III = I_1 + I_{2,1} + II_1 + III_1 = I_1 + II_1 + III_1$$

and so $\mathcal{N}(f; p^s) \leq cq^{-s/h(f)} q^{-19/12}$ when $s \equiv 1 \bmod 12$. This illustrates that we cannot replace the factor q^{-2} with q^{-1} in the lower bound (5) or (8) of Theorems 1.2 and 1.3.

4.8. **Estimates for $f \in E_1$.** Here we treat separately the case of character sums $\mathcal{S}_\chi(f; \pi^s)$ when $f \in E_1$; that is, when $f(x,y) = a(y - \zeta x)(y - \zeta^* x)$ where ζ, ζ^* are conjugate roots of degree 2 over K. For such f, $h(f) = d(f) = 1$ and the claimed estimates for $\mathcal{N}(f; \pi^s)$ in Theorem 1.3 have already been established; namely,

$$csq^{-s}q^{-2} \ \leq \ \mathcal{N}(f; \pi^s) \ \leq Csq^{-s}$$

and $csq^{-s} \leq \mathcal{N}(f; \pi^s)$ when $s \equiv 0 \bmod 2$.

The estimates for character sums $\mathcal{S}(f; \pi^s)$ when $f \in E_1$ are different from those for polynomial congruences; the uniform upper bound (7) in Theorem 1.3 is

$$|S_\chi(f; \pi^s)| \ \leq \ Cq^{-s} \tag{50}$$

whenever $\mathfrak{p} \notin \mathcal{P}(f)$. Furthermore the estimate (10) reads that for infinitely many $s \geq 1$,

$$cq^{-s} \ \leq \ |S_\chi(f; \pi^s)| \tag{51}$$

holds whenever $\mathfrak{p} \notin \mathcal{P}(f)$. The upper bound (50) follows from the work of Denef and Sperber [4] since f is nondegenerate with respect to its Newton diagram (see also the work of Cluckers [1] for the abstract setting of general local fields). Strictly speaking the estimate (51) does not follow from the work of Denef and Sperber since the vertices $\{(0,2),(2,0)\}$ of the Newton polygon of f lie in $\{0,1,2\}^2$. Nevertheless we can see that (51) holds from our analysis above. Recall our basic decomposition $S_\chi(f; \pi^s) = I + II + III$ where $I = I_1 + I_2$, $II = II_1 + II_2$ and $III = III_1 + III_2$; furthermore, $II_2 = 0$ when $s \equiv 0 \bmod \gcd(\alpha, \beta + tn)$ and $III_2 = 0$ when $s \equiv 0 \bmod \gcd(\beta, \alpha + rn)$ (here $\gcd(\alpha, \beta + tn) = \gcd(\beta, \alpha + rn) = 2$ in our case $f \in E_1$). Due to the nondegeneracy of f, we also have $I_2 = 0$ if $s \equiv 0 \bmod 2$. This follows by the same argument establishing property (C2) for character sums, adapted to double sums; in fact if $s \equiv 0 \bmod 2$, then $\sigma := s - 2m \geq 2$ in the m sum defining I_2 and so if we write $\vec{u} := (x,z) \leq \pi^\sigma \bar{\mathfrak{o}}$ (using our shorthand notation introduced in section 2.6) as $\vec{u} = \vec{v} + \pi^{\sigma-1}\vec{w}$ with $\vec{v} \leq \pi^{\sigma-1}\bar{\mathfrak{o}}$ and $\vec{w} \leq \pi\bar{\mathfrak{o}}$, then $\phi(\vec{u}) \equiv \phi(\vec{v}) + \pi^{\sigma-1}\nabla\phi(\vec{v}) \cdot \vec{w} \bmod \pi^{2\sigma-2}\bar{\mathfrak{o}}$ which in turn is equivalent mod π^σ since $\sigma \geq 2$ (here $\phi(x,z) = h(z)x^2$).

Also $\pi \not| \vec{u}$ is equivalent to $\pi \not| \vec{v}$ and when this happens, $\pi \not| \nabla\phi(\vec{v})$. Therefore

$$I_2 = \sum_{\sigma \geq 2} q^{-2(s-\sigma)} q^{-2\sigma} \sum_{\substack{\vec{v} \leq \pi^{\sigma-1}\bar{\mathfrak{o}} \\ \pi \not| \vec{v}}} \chi'(\pi^{-\sigma}\phi(\vec{v})) \sum_{\vec{w} \leq \pi\bar{\mathfrak{o}}} \chi'(\pi^{-1}\nabla\phi(\vec{v}) \cdot \vec{w}) \ = \ 0$$

as in the verification of property (C2) for character sums. Since $II_1, III_1 \geq 0$, (51) follows from (19) which holds for $s \equiv 0 \bmod 2$ since $N = 2$ in this case.

5. The case $d(f) < 2$ for character sums

Here we consider the character sums (or oscillatory integrals, see (15))

$$\mathcal{S}_\chi(f; \mathfrak{p}^s) \ = \ \iint_{\bar{\mathfrak{o}} \times \bar{\mathfrak{o}}} \psi(\pi^{-s} f(x,y)) d\mu(x) d\mu(y)$$

when $d(f) < 2$ and when f consists of more than one monomial. We note that in this case the exceptional classes E_m for $m \geq 2$ do not arise. In fact if $f \in E_m$, then $d(f) = m$, $m_K(f) = 0$ and $h(f) = m$. If furthermore $d(f) < 2$, then this forces $f \in E_1$ and such an f does *not* belong to the exceptional class for the character sum estimate (7) in Theorem 1.3. However such an f *does* belong to the exceptional class for the polynomial congruences estimate (8). In this case, the Varchenko exponent $\nu(f) = \nu_{\mathfrak{p}}(f)$ depends on the prime ideal $\mathfrak{p}$ as described in Theorem 1.3.

To be quite specific, our goal here is to establish the estimates (7) and (10) in Theorem 1.3 when $d(f) < 2$. In fact we need only establish (10) when $f \notin E_1$ (this case was already treated in Section 4.8), when f is not linear and when $d(f) \leq m_K(f) \leq 2$ with $d(f) < 2$; see Section 4.6.

We observe that when $d(f) < 2$ the exponent $i(f)$ is equal to zero even if a vertex of the Newton diagram of f lies on the bisectrix. In fact if $h(f) < 2$, then $i(f) = 0$ by definition and if $d(f) < 2 \leq h(f)$, then $m_K(f) \neq d(f)$ and so again $i(f) = 0$.

When $d(f) < 2$, the list of possibilities for f is small and in the subcase $h(f) < 2$, it turns out that f is nondegenerate with respect to its Newton diagram so we can appeal to the work of Denef and Sperber [4] or Cluckers [2] to establish the estimate (7) in this case (alternatively we can follow the arguments in the previous sections, noting improved finite field character sums at the appropriate places). Strictly speaking the estimates in [4] or [2] carry a linear factor of s when a vertex of the Newton diagram lies on the bisectrix. However we will see that when $d(f) < 2$ and f is not a monomial, this only happens if $f(x,y) = ax(y - \zeta x^r)$ for some $r \geq 1$ or $f(x,y) = ay(y - \zeta x)$ where ζ is nonzero and lies in K (these are the only such cases which arise under our assumption $\kappa_1 \leq \kappa_2$; in general we should swap x and y and include $f(x,y) = ay(x - \zeta y^r)$ for any $r \geq 1$).

In these two cases $h(f) = d(f) = m_K(f) = 1$ and (for $f(x,y) = ax(y - \zeta x^r)$, say) $\mathcal{S}_\chi(f; \mathfrak{p}^s) =$

$$\int_{|x| \leq 1} \psi(\pi^{-s} a\zeta x^{r+1}) d\mu(x) \int_{|y| \leq 1} \psi(\pi^{-s} axy) d\mu(y) = \int_{|x| \leq q^{-s}} \psi(\pi^{-s} a\zeta x^{r+1}) d\mu(x).$$

The last integral equals q^{-s} since $|\pi^{-s}a\zeta x^{r+1}| \le q^s q^{-s(r+1)} \le 1$ when $|x| \le q^{-s}$ and this implies the claimed estimates (7) and (10) in this case. A similar identity holds for $f(x,y) = ay(y-\zeta x)$.

We now list of possibilities for f when $d(f) < 2$ and f is not a monomial. Writing

$$f(x,y) \;=\; ax^\alpha y^\beta \prod_{j=1}^{M} (y^t - \zeta_j x^r)^{n_j}$$

as in (11) of Section 2, then $d(f) < 2$ implies

$$d(f) \;=\; \frac{t\alpha + r\beta + rtn}{r+t} \;<\; 2 \quad \text{or} \quad t\alpha + r\beta + rtn \;\le 2r + 2t - 1 \tag{52}$$

and this restricts the size of $n = \sum_{j\ge 1} n_j$, the total number of *nonzero* roots counted with multiplicities; we necessarily have $1 \le n \le 3$.

We enumerate the cases by the possible values of n, starting with $n = 3$. In this case we see from (52) that necessarily $\alpha = \beta = 0$ and $t = r = 1$. This leads to the only possibilities for f being

$$f(x,y) \;=\; a(y-\eta x)(y-\zeta x)(y-\zeta^* x) \tag{53}$$

where $\eta \in K$ is nonzero and either ζ and ζ^* are conjugate elements of degree 2 over K or both ζ and ζ^* are elements of K.

Next we turn to the case $n = 2$. In this case we see from (52) that necessarily $t = 1$ and $0 \le \alpha, \beta \le 1$ with at least one equal to zero. This leads to the only possibilities being

$$f(x,y) \;= ax^\alpha y^\beta (y-\zeta x^r)(y-\zeta^* x^r) \tag{54}$$

with the above restriction on α, β and either ζ, ζ^* are conjugate elements of degree 2 over K or the roots ζ and ζ^* both belong to K. Finally we turn to the case $n = 1$ where we have a single nonzero root ζ lying in K and so f must be of the form

$$f(x,y) \;=\; ax^\alpha y^\beta (y^t - \zeta x^r). \tag{55}$$

From (52) we see that $1 \le t \le 3$ and $0 \le \alpha, \beta \le 1$; if $t = 3$, then necessarily $r = 4$ or 5 and $\alpha = \beta = 0$. If $t = 2$, then either α or β (or both) is zero. Furthermore when $t = 2$, if $\beta \ne 0$, then necessarily $\beta = 1$ and $r = 3$.

We treat each case above separately. When f is of the form (53), then it is nondegenerate with respect to its Newton diagram if the roots ζ, ζ^* form a conjugate pair of degree 2 over K or they are distinct roots in K. In these cases $d(f) = 3/2 = h(f)$, $m_K(f) = 1$ and the estimates (7) and (10) follow from the results in [4] and [2]. Strictly speaking the lower bound (10) is only shown in [4] in the setting of the integers $\mathbb{Z}$. However since $m_K(f) = 1 < 3/2 = d(f)$, the lower bound (10) has already been established in Section 4.6.

The remaining cases for (53) are when the roots $\zeta = \zeta^*$ coincide and lie in K. In this case $d(f) = 3/2 < 2 \le m_K(f) = h(f)$ and so we need to establish both bounds, (7) and (10). We first consider

$$f(x,y) \;=\; a(y-\eta x)(y-\zeta x)^2$$

where $\zeta \neq \eta$; here $d(f) = 3/2$ and $m_K(f) = h(f) = 2$. In this case we make the change of variables $z = y - \zeta x$ in the y integral (15) representing the sum $\mathcal{S}_\chi$ and write

$$\begin{aligned}\mathcal{S}_\chi(f;\mathfrak{p}^s) &= \int\limits_{|x|\leq 1,\ |z+\zeta x|\leq 1} \psi(\pi^{-s}az^2(z-\zeta' x))d\mu(z)d\mu(x) \\ &= \int\limits_{|z|\leq 1} \psi(\pi^{-s}az^3)d\mu(z) \int\limits_{|x|\leq 1} \psi(-\pi^{-s}\zeta' z^2 x)d\mu(x)\end{aligned}$$

where $\zeta' = \eta - \zeta$. Recall that $|\zeta| = |\eta - \zeta| = 1$ when $\mathfrak{p} \notin \mathcal{P}(f)$ so that when $|z| \leq 1$, $|x + \zeta^{-1}z| \leq 1$ if and only if $|x| \leq 1$. The x integral can be evaluated leading to the identity $\mathcal{S}_\chi(f;\mathfrak{p}^s) = q^{-s/2}$ if s is even and $\mathcal{S}_\chi(f;\mathfrak{p}^s) = q^{-s/2}q^{-1/2}$ if s is odd. From these identities, we see that (7) and (10) hold.

The last case for (53) is when $f(x,y) = a(y-\zeta x)^3$ and here $d(f) = 3/2 < m_K(f) = h(f) = 3$. A straightforward computation shows $\mathcal{S}_\chi(f;\mathfrak{p}^s) = q^{-s/3}$ if $s \equiv 0 \bmod 3$, $\mathcal{S}_\chi(f;\mathfrak{p}^s) = q^{-s/3}q^{-1/3}$ if $s \equiv 2 \bmod 3$ and

$$\mathcal{S}_\chi(f;\mathfrak{p}^s) = q^{-s/3}q^{1/3}\,\mathcal{S}_\chi(f;\mathfrak{p})$$

if $s \equiv 1 \bmod 3$. Since

$$\mathcal{S}_\chi(f;\mathfrak{p}) = \int_{|x|\leq 1} \psi(\pi^{-1}ax^3)d\mu(x),$$

we have $|\mathcal{S}_\chi(f;\mathfrak{p})| \leq Cq^{-1/2}$ from property $(C3)$ in Section 4 for character sums and so the estimate (7) holds in this case. Considering the sequence $s = 3k$ shows that (10) also holds in this case.

We now turn to those f in (54) where f is nondegenerate with respect to its Newton diagram unless the roots ζ, ζ^* coincide and lie in K. In the nondegenerate case, the estimate (7) follows again from [4] or [2]. For the lower bound (10), we note that $m_K(f) \leq 1 < 2r/(r+1) \leq d(f)$ unless $\alpha = \beta = 0$ and $r = 1$ in which case $m_K(f) = 0 < 1 = d(f)$. In either case $m_K(f) < d(f) < 2$ and so (10) follows from Section 4.6.

When $\zeta = \zeta^* \in K$, we have $f(x,y) = ax^\alpha y^\beta(y - \zeta x^r)^2$ where $0 \leq \alpha, \beta \leq 1$, not both of which are 1. If $\alpha = \beta = 0$, a simple change of variables shows

$$\mathcal{S}_\chi(f;\mathfrak{p}^s) = \int_{|x|\leq 1} \psi(\pi^{-s}ax^2)d\mu(x)$$

and the integral above has modulus equal to $q^{-s/2}$ (we are assuming the characteristic of K, if positive, is greater than 2 in this case and so the element $2 = 2 \cdot \mathbf{1}$ is nonzero; furthermore, we ensure that the nonzero $2 = 2 \cdot \mathbf{1}$ lies in our collection of algebraic elements $\mathcal{A}$ so that $|2| = 1$ whenever $\mathfrak{p} \notin \mathcal{P}(f)$). If either α or β equals to 1, then a computation similar to the ones performed above shows that $\mathcal{S}(f;\mathfrak{p}^s) = q^{-s/2}$ is s is even and equal to $q^{-s/2}q^{-1/2}$ when s is odd. In each case we see that both (7) and (10) hold.

Every f arising in (55) is nondegenerate with respect to its Newton diagram and so [4] or [2] shows that (7) holds for each such f except $f(x,y) = ay(y - \zeta x)$ or

$f(x,y) = ax(y-\zeta x^r)$ where the bisectrix passes through the vertex $(1,1)$ of the Newton diagram. We treated these special cases at the beginning of this subsection, noting the linear factor s does not arise in the estimates as predicted by Theorem 1.3. As for the lower bound (10), we need only verify this bound when $d(f) \leq m_K(f) \leq 2$ and $d(f) < 2$; the remaining cases have been treated in Section 4.6. One easily checks that $f(x,y) = ay^2(y-\zeta x)$ with $\zeta \in K \setminus \{0\}$ is the only example in (55) satisfying these conditions. In this case the oscillatory integral in (15) becomes

$$\int_{|y|\leq 1} d\mu(y) \int_{|x|\leq 1} \psi(\pi^{-s} a y^2 (y-\zeta x)) d\mu(x) = \int_{|y|\leq 1} d\mu(y) \int_{|z|\leq 1} \psi(\pi^{-s} a y^2 z) d\mu(z)$$

using the change of variables $z = y - \zeta x$ in the x integral and noting $|\zeta| = 1$ whenever $\mathfrak{p} \notin \mathcal{P}(f)$. The integral on the right hand side is equal to $q^{-s/2}$ if $s \equiv 0 \mod 2$ and $q^{-s/2}q^{-1/2}$ if $s \equiv 1 \mod 2$. Since $d(f) = 3/2 < m_K(f) = 2 = h(f)$, we see that (10) holds when $s \equiv 0 \mod 2$ in this case.

6. Appendix: the case when $f(x,y) = ax^\alpha y^\beta$ is a monomial

For completeness we treat the simple case when $f(x,y) = ax^\alpha y^\beta$ is a single monomial and give a quick analysis of the integrals

$$I_{\alpha,\beta} := \iint_{\bar{\mathfrak{o}}\times\bar{\mathfrak{o}}} \mathcal{C}(\pi^{-s} a x^\alpha y^\beta) d\mu(x) d\mu(y)$$

where $\mathcal{C}$ is either ψ, the additive character on $\bar{\mathfrak{o}}$ so that $I_{\alpha,\beta} = \mathcal{S}_\chi(f;\mathfrak{p}^s)$ is a character sum over the factor ring $\mathfrak{o}/\mathfrak{p}^s$, or it is equal to the indicator function $\mathbf{1}_{\bar{\mathfrak{o}}}$ of $\bar{\mathfrak{o}}$ so that $I_{\alpha,\beta} = \mathcal{N}(f;\mathfrak{p}^s)$ counts the number of polynomial congruences $f(x,y) \equiv 0 \mod \mathfrak{p}^s$. Since f is quasi-homogeneous, at least one exponent α or β is nonzero. Also $|a| = |a|_{\mathfrak{p}} = 1$ for $\mathfrak{p} \notin \mathcal{P}(f)$. In this case the height $h(f)$ is equal to $\max(\alpha,\beta)$ and $\nu(f) = 1$ or 0 depending on whether $\alpha = \beta$ or not, respectively. The same is true for $i(f)$ except when $\alpha = \beta = 1$ we have $i(f) = 0$ (in this case, $\nu(f) = 1$).

When f is linear, that is, when $f(x,y) = ax$ or $f(x,y) = ay$, we have $h(f) = 1$, $i(f) = \nu(f) = 0$, $\mathcal{S}_\chi(f;\pi^s) = 0$ and $\mathcal{N}(f;\pi^s) = q^{-s}$ so that the bounds (7), (8) and (9) trivially hold in this case (recall that the lower bound (10) holds in all cases except when f is linear in which case it cannot possibly hold).

When $f(x,y) = axy$, we have $h(f) = 1$, $i(f) = 0$ and $\nu(f) = 1$. In this case, $\mathcal{S}_\chi(f;\pi^s) = q^{-s}$ and $\mathcal{N}(f;\pi^s) = (1-q^{-1})sq^{-s} + q^{-s}$; see below for this computation. Hence the estimates in Theorem 1.3 all hold in this case.

Therefore we may assume that $h(f) = \max(\alpha,\beta) \geq 2$. Without loss of generality, suppose that $\alpha \leq \beta$. We decompose $I_{\alpha,\beta} =$

$$\iint_{\bar{\mathfrak{o}}\times\bar{\mathfrak{o}}} \mathcal{C}(\pi^{-s} a x^\alpha y^\beta)\, d\mu(x) d\mu(y) = \sum_{k\geq 0} q^{-k} \int_{|y|=1} d\mu(y) \int_{|x|\leq 1} \mathcal{C}(\pi^{-s+\beta k}[a y^\beta] x^\alpha)\, d\mu(x)$$

$$= (1-q^{-1}) \sum_{\beta k \geq s} q^{-k} \quad + \quad \sum_{\beta k \leq s-1} q^{-k} \int_{|y|=1} \int_{|x|\leq 1} \mathcal{C}(\pi^{-(s-\beta k)}[a y^\beta] x^\alpha) d\mu(x) d\mu(y).$$

If $\alpha = \beta$, then we can make the change of variables $z = yx$ in the x integral so that

$$I_{\beta,\beta} = (1-q^{-1})\big[\sum_{\beta k \geq s} q^{-k} \ + \sum_{\beta k \leq s-1} q^{-k} \int_{|z|\leq 1} \mathcal{C}(\pi^{-(s-\beta k)} a z^{\beta}) d\mu(z)\big]$$

and the z integral vanishes when $\beta = 1$ and $\mathcal{C} = \psi$. Furthermore the z integral is equal to $q^{-(s-k)}$ when $\beta = 1$ and $\mathcal{C} = \mathbf{1}_{\bar{\mathfrak{o}}}$. This gives that values of $\mathcal{S}_{\chi}(f;\pi^s)$ and $\mathcal{N}(f;\pi^s)$ for $f(x,y) = axy$ mentioned above. For $\beta \geq 2$, the z integral is equal to $q^{-s/\beta} q^k$ when $s \equiv 0 \bmod \beta$ and this holds for both polynomial congruences, $\mathcal{C} = \mathbf{1}_{\bar{\mathfrak{o}}}$, and character sums, $\mathcal{C} = \psi$. This shows that both (9) and (10) hold for $s \equiv 0 \bmod \beta$ when $\alpha = \beta \geq 2$. For general $s \geq 1$, we have the upper bound

$$\big|\int_{|z|\leq 1} \mathcal{C}(\pi^{-(s-\beta k)} a z^{\beta}) d\mu(z)\big| \ \leq \ q^{-s/\beta} q^k$$

for the z integral, valid for both $\mathcal{C} = \mathbf{1}_{\bar{\mathfrak{o}}}$ or $\mathcal{C} = \psi$. This gives the upper bounds in (7) and (8) when $\alpha = \beta \geq 2$. Finally we note that when $\mathcal{C} = \mathbf{1}_{\bar{\mathfrak{o}}}$, the z integral has the lower bound $q^{-s/\beta} q^k q^{-1}$ for general $s \geq 1$ and this gives the lower bound in (8) in this case.

Finally we turn to treat the case $h(f) = \max(\alpha,\beta) \geq 2$ and $\alpha < \beta$. We will assume $\alpha \geq 1$; the case $\alpha = 0$ is easier. As in the case for $\alpha = \beta$, we have the upper bound

$$\Big|\int_{|y|=1} \int_{|x|\leq 1} \mathcal{C}(\pi^{-(s-\beta k)}[a y^{\beta}] x^{\alpha}) d\mu(x) d\mu(y)\Big| \ \leq \ C q^{-(s-\beta k)/\alpha}$$

and this leads to the upper bounds in (7) and (8) for the case $\alpha < \beta$. Furthermore, if $s = m_* \beta$ for some $m_* \geq 1$, this upper bound implies

$$\Big|\sum_{k \leq m_* - 1} q^{-k} \int_{|y|=1} \int_{|x|\leq 1} \mathcal{C}(\pi^{-(s-\beta k)}[a y^{\beta}] x^{\alpha}) d\mu(x) d\mu(y)\Big| \ \leq \ C q^{-s/\beta} q^{-([\beta/\alpha]-1)}$$

and therefore, when $s \equiv 0 \bmod \beta$, $|I_{\alpha,\beta}| \geq c q^{-s/\beta}$ if q is large enough and this gives the lower bounds (9) and (10) in this case. Finally we observe that when $\mathcal{C} = \mathbf{1}_{\bar{\mathfrak{o}}}$, the lower bound

$$\int_{|y|=1} \int_{|x|\leq 1} \mathcal{C}(\pi^{-(s-\beta k)}[a y^{\beta}] x^{\alpha}) d\mu(x) d\mu(y) \ \geq \ q^{-(s-\beta k)/\alpha} q^{-1}$$

leads to the lower bound in (8) for the case $\alpha < \beta$ and $h(f) = \max(\alpha,\beta) \geq 2$.

This completes our analysis for the monomial case $f(x,y) = a x^{\alpha} y^{\beta}$ and hence this completes the proof of Theorem 1.3.

References

[1] R. Cluckers, *Igusa and Denef-Sperber conjectures on nondegenerate p-adic exponential sums*, Duke Math. J. **141** (2008), no. 1, 205-216.

[2] R. Cluckers, *Exponential sums: questions by Denef, Sperber and Igusa* Trans. Amer. Math. Soc. **362** (2010), no. 7, 3745-3756.

[3] R. Cluckers, *Igusa's conjecture on exponential sums modulo p and p^2 and the motivic osillation index* Internat. Math. Res. Not. IMRN **2008** (2008), no. 4.

[4] J. Denef and S. Sperber, *Exponential sums mod p^n and Newton polydegra*, Bull. Belg. Math. Soc. Simon Stevin **suppl.** (2001), 55-63.

[5] J. Igusa, *Lectures on forms of higher degree*, Lectures on mathematics and physics, Tata institute of fundamental research, vol. 59, Springer-Verlag, 1978.
[6] J. Igusa, *An introdution to the theory of local zeta functions*, AMS/IP Studies in Advanced Mathematics, 14, AMS, Providence, RI; International Press, Cambridge, MA, 2000.
[7] I.A. Ikromov and D. Müller, *On adapted coordinate systems*, Trans. Amer. Math. Soc. **363** (2011), no. 6, 2821-2848.
[8] I.A. Ikromov and D. Müller, *Uniform estimates for the Fourier transform of surface carried measures in* $\mathbb{R}^3$ *and an application to Fourier restriction*, preprint.
[9] S. Lang, *Algebra*, Addison-Wesley Publishing Co. (1965).
[10] S. Lang, *Algebraic number theory*, Second edition, Springer-Verlag (1994).
[11] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Second edition, Springer-Verlag (1990).
[12] D.H. Phong and E.M. Stein, *Oscillatory integrals with polynomial phases*, Inventiones Math. **110** (1992), 39-62.
[13] D.H. Phong, E.M. Stein and J.A. Sturm, *On the growth and stability of real analytic functions*, Amer. J. Math **121** (1999), 519-554.
[14] J. Wright, *From oscillatory integrals and sublevel sets to polynomial congruences and character sums*, J. Geom. Anal. **21** (2011), 224-240.
[15] J. Wright, *On polynomial congruences*, preprint.
[16] J. Wright, *From oscillatory integrals to complete exponential sums*, Math. Res. Letters **18** (2011), no. 2, 231-250.

Maxwell Institute of Mathematical Sciences and the School of Mathematics, University of Edinburgh, JCMB, King's Buildings, Mayfield Road, Edinburgh EH9 3JZ, Scotland

E-mail address: J.R.Wright@ed.ac.uk