From Oscillatory Integrals and Sublevel Sets to Polynomial Congruences and Character Sums

FROM OSCILLATORY INTEGRALS AND SUBLEVEL SETS TO POLYNOMIAL CONGRUENCES AND CHARACTER SUMS

JAMES WRIGHT

ABSTRACT. We present a slight extension of a classical lemma of Hensel and give various applications to polynomial congruences and character sums; in particular, we give a new proof of a classical result of Hua on complete exponential sums.

1. INTRODUCTION

In this note we revisit some problems and results in elementary number theory from a harmonic analyst's perspective. Our motivation comes from studying various euclidean harmonic analysis problems, for example the Fourier restriction problem, in the setting of the ring of integers mod n, $\mathbb{Z}/n\mathbb{Z}$. Such problems have been extensively studied in the setting of finite fields (see for example, [6]) and have served as good models for the original euclidean problems. However a difference one finds when passing from the euclidean setting to the finite field setting is the lack of scales at one's disposal. Moving from finite fields, say $\mathbb{Z}/p\mathbb{Z}$ where p is prime, to the ring $\mathbb{Z}/n\mathbb{Z}$ for general n, the various divisors of n serve as different scales. By introducing an appropriate "absolute value" or "norm" for integers mod n, euclidean scaling arguments can be made to work in this setting and one sees that euclidean problems are modeled more closely in $\mathbb{Z}/n\mathbb{Z}$ than in the finite field setting.

To illustrate this consider the oscillatory integral

$$I \ = \ \int_0^1 e^{2\pi i[a_d x^d + \cdots + a_1 x]}\, dx$$

with a polynomial phase with real coefficients. A basic estimate for this integral is $|I| \leq C_d \|\vec{a}\|^{-1/d}$ and this is best possible when one measures decay in terms of the euclidean (or any other) norm of the coefficients of the phase. This estimate is useful in a number of euclidean harmonic analysis problems and when one passes to the integers mod n setting, it is the exponential sum

$$S \ = \ \frac{1}{n} \sum_{x=1}^{n} e^{2\pi i[a_d x^d + \cdots + a_1 x]/n}$$

where the phase is now a polynomial with integer coefficients which plays the analogous role. If one introduces the "norm" $\|\vec{a}\| := \max(|a_j|)$ based on the "absolute value"[1] $|a| := n/gcd(a, n)$ (here $gcd(a, n)$ denotes the greatest common divisor of a and n), then a classical result of Hua [4] from the 1930's gives the estimate[2] $|S| \leq C_d\|\vec{a}\|^{-1/d}$ which of course looks very similar to the basic estimate for the oscillatory integral I. From a harmonic analysis point of view, it is the implied uniformity in the estimate for I which is important and when one looks at these (harmonic analysis) problems in $\mathbb{Z}/n\mathbb{Z}$, the uniformity issues remain important. In particular an estimate for the exponential sum S where the constant C_d is allowed to grow in n is not good and so Hua's estimate for S is the suitable one for such purposes.

When $n = p$ is a rational prime, the exponential sum S becomes a sum over a finite field and the work of A. Weil [8] gives the improved estimate $|S| \leq C_d\|\vec{a}\|^{-1/2}$ which, in a way, is a reflection of the lack of scales in a finite field. For this and similar reasons one gets results in the finite field setting which are different from their euclidean cousins (for the Fourier restriction problem, see [6], and for precise smoothing estimates, see [1]). This is not the case when one considers these problems in $\mathbb{Z}/n\mathbb{Z}$ for general n (or other settings where one has lots of divisors, given by either prime elements or prime ideals) and in fact one gets the same results and/or conjectures as in the euclidean setting. We pursue these matters elsewhere.

In this paper we develop an approach, inspired by a standard method to establish the sublevel set estimate

$$\left|\left\{0 \leq x \leq 1 : |a_d x^d + \cdots a_1 x + a_0| \leq 1\right\}\right| \leq C_d\|\vec{a}\|^{-1/d}, \tag{1}$$

to prove estimates for the number of solutions to polynomial congruences and estimates for character sums. In the same way how character sums count solutions to congruences, the basic estimate for the oscillatory integral I, $|I| \leq C_d\|\vec{a}\|^{-1/d}$, implies (1). However in the euclidean case, this implication can be reversed. First let us sketch a typical argument which establishes (1). By a trivial scaling, (1) is equivalent to

$$\left|\left\{0 \leq x \leq 1 : |\phi(x)| \leq \delta\right\}\right| \leq C_d \delta^{1/d} \tag{2}$$

where the polynomial phase $\phi(x) = a_d x^d + \cdots + a_0$ is normalised so that $\|\vec{a}\| = 1$. The normalisation implies that some derivative $|\phi^{(n)}(x)| \geq c_d$ has a uniform bound from below on $[0, 1]$ (at this point we can forget that ϕ is a polynomial). Hence $\phi^{(n-1)}$ is monotone and so has at most one zero in $[0, 1]$ and we remove an interval around this root, leaving two intervals on which $\phi^{(n-1)}$ has a uniform bound from below and $\phi^{(n-2)}$ is monotone and so has at most one zero on each of these two intervals. Iterating this procedure leads to a crude but useful uniform set inclusion

$$\{0 \leq x \leq 1 : |\phi(x)| \leq \delta\} \subset \bigcup_{z \in \mathcal{Z}} \bar{B}_{c\,\delta^{1/n}}(z) \tag{3}$$

---

[1]of course these are *not* norms or absolute values but they are based on an actual absolute value, normalised with respect to the integer n – see Section 3 below

[2]strictly speaking Hua's estimate gives an ϵ loss in n but his arguments have been refined to give the stated estimate; see for example [2] and [7]

where $\mathcal{Z} = \{z : \phi^{(k)}(z) = 0 \text{ for some } k \leq n\}$ and $\bar{B}$ denotes a closed interval with the indicated radius and centre. The set inclusion (3) clearly implies (2) and hence (1).

In Section 3 we will prove (3) in the setting of the ring of integers with respect to *any* valuation (non-archimedean absolute value) under the hypothesis that some derivative of ϕ is uniformly bounded below; see Proposition 3.1. We will see that in this setting, a sublevel set is the set of solutions to a congruence. The non-archimedean nature of the absolute value makes all the instances of the intermediate value and mean value theorems used in the above argument invalid in such a setting but nevertheless a nondegeneracy condition on some derivative of the phase ϕ will still imply that the sublevel set is attracted to the roots of the derivatives of ϕ in the way described by (3). This will be achieved by employing an extension of a classical lemma of Hensel which we carry out in the next section.

Using the fact that (2) follows from a uniform bound from below of some derivative of ϕ, one can give a quick proof of the basic estimate for the oscillatory integral I; simply decompose the integral $I = I_1 + I_2$ where $|\phi'(x)| \leq \theta$ and $|\phi'(x)| \geq \theta$, respectively. A simple integration by parts gives an estimate for I_1 and for I_2, one can use a sublevel set estimate for ϕ', knowing a uniform bound from below of a derivative of ϕ'. Choosing θ appropriately gives $|I| \leq C_d \|\vec{a}\|^{-1/d}$. A similar approach will give estimates for character sums under a nondegeneracy condition of some derivative of the phase ϕ although we will need to use the analysis of $\{|\phi(x)| \leq \delta\}$ which will prove the analogue of (3) to establish these character sum estimates, instead of simply employing the analogue of (3) directly.

It is doubtful that we give any new results in what follows. The novelty lies in the approach and the elementary, direct methods used. However this perspective has been developed further; for instance, finer structural analysis of sublevel sets $\{|\phi(x)| \leq \delta\}$ in non-archimedean settings are possible, giving new results for the number of solutions to polynomial congruences and complete exponential sums. These results will appear elsewhere.

Added in press: We have become aware recently of a preprint of Raf Cluckers, "Analytic van der Corput lemma for p-adic and $\mathbb{F}_q((t))$ oscillatory integrals, singular fourier transforms, and restriction theorems" which establishes oscillatory integral estimates in the local field setting similar to the ones discussed in the last remark after Proposition 4.1 below.

2. An extension of Hensel's classical lemma

Here we give a extension of Hensel's classical lemma in one variable, allowing for the derivative of the phase to be more degenerate than usual; the degeneracy is compensated by imposing conditions on higher derivatives. The formulation and proof is valid in any complete valuation ring.

Proposition 2.1. *Let K be a field which is complete with respect to a nontrivial, non-archimedean absolute value $|\cdot|$ (a valuation) and suppose $\mathfrak{o}$ is the associated*

ring of integers (that is, $\mathfrak{o} = \{x \in K : |x| \leq 1\}$). Furthermore let ϕ be a polynomial with coefficients in $\mathfrak{o}$ and suppose at $x_0 \in \mathfrak{o}$, there is an $L \geq 1$ so that

for each $1 \leq k \leq L - 1$, $|[\phi^{(k+1)}(x_0)/(k+1)!]\phi(x_0)| < |(\phi^{(k)}(x_0)/k!)\phi'(x_0)|$

and $|\phi(x_0)| < |(\phi^{(L)}(x_0)/L!)\phi'(x_0)|$. Then there is a unique $x \in \mathfrak{o}$ with $\phi(x) = 0$ so that $|x - x_0| \leq |\phi(x_0)\phi'^{-1}(x_0)|$.

Remarks:

- The hypothesis for the case $L = 1$ reduces to the single condition $|\phi(x_0)| < |\phi'(x_0)^2|$ on the derivative and this is a formulation of the classical lemma of Hensel. Although typically Hensel's lemma is presented in the ring of rational integers $\mathbb{Z}$ with a p-adic valuation, it has found many applications in more general situations and one often finds it stated in the generality given above; see for example, [5].
- We could have cast the proposition in any subring $\mathfrak{o}$ of the ring of integers associated to a non-archimedean absolute value (not necessarily complete) and then refine x_0 with the above hypotheses to a true root x of ϕ in the completion of $\mathfrak{o}$. Stating the proposition in this way is slightly less general but arises naturally in applications. For example, our polynomial ϕ could have coefficients in some Dedekind domain $\mathfrak{o}$ and the hypotheses could be satisfied with respect to a discrete valuation arising from some nonzero prime ideal.
- When the non-archimedean absolute value is discrete, the proposition has the following nice formulation: let $\mathfrak{o}$ be a complete discrete valuation ring with valuation ν, written additively, normalised so that $\nu(\pi) = 1$ for some prime element π. Suppose $\phi \in \mathfrak{o}[X]$ has an approximate root at $x_0 \in \mathfrak{o}$ in the sense that $\phi(x_0) \equiv 0 \bmod \pi^s \mathfrak{o}$. Then if $\delta_1 + \delta_k < s + \delta_{k+1}$, $1 \leq k \leq L-1$ and $\delta_1 + \delta_L < s$ for some $L \geq 1$ where $\delta_k := \nu(\phi^{(k)}/k!)$, there exists a unique root $x \in \mathfrak{o}$ of ϕ with $x \equiv x_0 \bmod \pi^{s-\delta_1}\mathfrak{o}$.
- Basic examples of complete discrete valuation rings to keep in mind are the ring of integers in a local field; finite field extensions of p-adic fields $\mathbb{Q}_p$ in the characteristic zero case and formal Laurent series $\mathbb{F}_q((X))$ over a finite field in the positive characteristic case.
- Finally, as the proof below shows, the phase ϕ does not necessarily have to be a polynomial. The key property which ϕ needs to satisfy is the following expansion estimate around any point $y \in \mathfrak{o}$: $\phi(y+h) = \sum_{k=0}^{m}[\phi^{(k)}(y)/k!]h^k + R_m(y,h)$ where $|R_m(y,h)| \leq |h|^{m+1}$.

Proof As usual we construct a sequence of approximate roots by the recursive Newton formulae

$$x_{n+1} \; = \; x_n \; - \; \frac{\phi(x_n)}{\phi'(x_n)}, \quad n \geq 0$$

which we will show converges to an $x \in \mathfrak{o}$ with the desired properties. Since $|\phi'(x_0)|$ is assumed to be positive, $\phi'(x_0) \neq 0$ in $\mathfrak{o}$ and so the above formula for $n = 0$ makes sense; the right-hand side being an element of K a priori but since

$|\phi(x_0)/\phi'(x_0)| \le 1$ by a simple consequence of our hypotheses, we see that

$$|x_1 - x_0| = \frac{|\phi(x_0)|}{|\phi'(x_0)|} \le 1 \qquad (4)$$

and so, in particular, x_1 lies in $\mathfrak{o}$. By induction we will show $|\phi'(x_n)| = |\phi'(x_0)|$ for all $n \ge 1$ (hence $\phi'(x_n)$ never vanishes) which will make sense of the formulae for all $n \ge 0$.

The convergence rate of various quantities in the proof will be measured by $d := |\phi''(x_0)/2||\phi(x_0)\phi'^{-2}(x_0)|$; our $k = 1$ hypothesis states that $d < 1$ (we make the obvious modification in the $L = 1$ case). The key to the proof is to observe that the following claim holds.

Claim: For each $n \ge 1$,

$(1)_n \quad |x_n - x_{n-1}| = |\phi(x_0)\phi'^{-1}(x_0)| \, d^{2^{n-1}-1}$;

$(2)_n \quad |\phi(x_{n-1})| = |\phi(x_0)| \, d^{2^{n-1}-1}$;

$(3)_n \quad |\phi^{(k)}(x_{n-1})/k!| = |\phi^{(k)}(x_0)/k!|, \quad 1 \le k \le L.$

The case $n = 1$ follows from (4). The proof for general n will proceed by induction. Before we do this we note that the claim implies that $x_n \to x$ in $\mathfrak{o}$ for some $x \in \mathfrak{o}$ and $\phi(x) = 0$. Furthermore by $(1)_n$, we have $|x_n - x_0| \le |\phi(x_0)\phi'^{-1}(x_0)|$ by the non-archimedean nature of $|\cdot|$ and hence, $|x - x_0| \le |\phi(x_0)\phi'^{-1}(x_0)|$.

We now turn to the proof of the claim. Suppose the three statements $(1)_n, (2)_n$ and $(3)_n$ hold. We first show $(3)_{n+1}$: for each $1 \le k \le L$,

$$\phi^{(k)}(x_n)/k! = \sum_{\ell=0}^{L-k} \binom{\ell + k}{k} \frac{\phi^{(\ell+k)}(x_{n-1})}{(\ell + k)!}(x_n - x_{n-1})^\ell + R_{k,L,n} \qquad (5)$$

and by $(1)_n$,

$$|R_{k,L,n}| \le |x_n - x_{n-1}|^{L-k+1} = \left[|\phi(x_0)\phi'^{-1}(x_0)|\right]^{L-k+1} d^{[2^{n-1}-1](L-k+1)}$$

This in turn is strictly less than $|\phi^{(L)}(x_0)/L!| \, |\phi(x_0)\phi'^{-1}(x_0)|^{L-k} \, d^{(2^{n-1}-1)(L-k)}$ by our top hypothesis $|\phi(x_0)| < |\phi^{(L)}(x_0)/L!| \, |\phi'(x_0)|$ and the fact that $d < 1$. Furthermore, if we set

$$F_\ell := \left|\frac{\phi^{(\ell+k)}(x_0)}{(\ell + k)!}\right| |\phi(x_0)\phi'^{-1}(x_0)|^\ell \, d^{(2^{n-1}-1)\ell}$$

so that the above estimate for $|R_{k,L,n}|$ is less than F_{L-k}, we see that $(1)_n$ and $(3)_n$ imply that the absolute value of the ℓth term in the sum in (5) is less than or equal to F_ℓ (with equality when $\ell = 0$) and our hypotheses iteratively give the string of inequalities $F_\ell < F_{\ell-1}$ for $1 \le \ell \le L - k$. Therefore by the non-archimedean nature of $|\cdot|$, we have

$$|\phi^{(k)}(x_n)/k!| = F_0 = |\phi^{(k)}(x_0)/k!| \quad \text{for } 1 \le k \le L$$

which establishes $(3)_{n+1}$.

We now turn to $(2)_{n+1}$: expanding ϕ around x_{n-1} we have

$$\phi(x_{n-1} + h) \;=\; \phi(x_{n-1}) + \phi'(x_{n-1})h + \sum_{\ell=2}^{L} \frac{\phi^{(\ell)}(x_{n-1})}{\ell!} h^{\ell} \;+\; R_{L,n}(h)$$

where $|R_{L,n}(h)| \leq |h|^{L+1}$. We now take

$$h \;=\; -\frac{\phi(x_{n-1})}{\phi'(x_{n-1})} \;=\; x_n - x_{n-1}$$

so that $\phi(x_{n-1}) + \phi'(x_{n-1})h = 0$; hence

$$|R_{L,n}(h)| \;\leq\; |x_n - x_{n-1}|^{L+1} \;<\; |\phi^{(L)}(x_0)/L!|\,|x_n - x_{n-1}|^{L}$$

by $(1)_n$ and our hypotheses. Also, in a similar way, $|\phi^{(\ell)}(x_0)/\ell!||x_n - x_{n-1}|^{\ell} < |\phi^{(\ell-1)}(x_0)/(\ell-1)!||x_n - x_{n-1}|^{\ell-1}$ for each $\ell \geq 3$. Therefore by $(3)_n$ and the non-archimedean nature of $|\cdot|$,

$$|\phi(x_n)| \;=\; |\phi''(x_0)/2||x_n - x_{n-1}|^2 \;=\; |\phi(x_0)|\,|\phi(x_0)\phi'^{-2}(x_0)\phi''(x_0)/2|\,d^{2^{n-1}-1}$$

which in turn is equal to $|\phi(x_0)|d^{2^n-1}$ after one unravels the notation. This completes the proof of $(2)_{n+1}$.

For $(1)_{n+1}$, using the already established $(2)_{n+1}$ and $(3)_{n+1}$,

$$\left|\frac{\phi(x_n)}{\phi'(x_n)}\right| \;=\; \left|\frac{\phi(x_0)}{\phi'(x_0)}\right| d^{2^n-1}$$

and hence from our recursive formula $x_{n+1} = x_n - \phi(x_n)\phi'^{-1}(x_n)$, we conclude $|x_{n+1} - x_n| = |\phi(x_0)\phi'^{-1}(x_0)|d^{2^n-1}$ which is $(1)_{n+1}$.

Finally we turn to the uniqueness of the solution $x \in \mathfrak{o}$. Suppose there is a (possibly different) solution $y \in \mathfrak{o}$ of $\phi(y) = 0$ with $|y - x_0| \leq |\phi(x_0)\phi'^{-1}(x_0)|$. We prove by induction the following estimate:

$$|y \;-\; x_n| \;\leq |\phi(x_0)\phi'^{-1}(x_0)|\; d^{2^n-1} \tag{6}$$

which clearly implies $y = x$. By induction suppose (6) holds at the nth step; then by expanding ϕ around x_n, we have

$$0 \;=\; \phi(y) \;=\; \sum_{\ell=0}^{L} \frac{\phi^{(\ell)}(x_n)}{\ell!}(y - x_n)^{\ell} \;+\; R_{L,n} \tag{7}$$

where $|R_{L,n}| \leq |y - x_n|^{L+1}$ which in turn is strictly less than $|\phi^{(L)}(x_0)/L!|\,|y - x_n|^{L}$ by our hypotheses, (6), $(3)_n$ and the fact that $d < 1$. Similarly we can compare the absolute values of consecutive terms in the sum in (7); in fact, using $(3)_n$ this reduces to

$$\left|\frac{\phi^{(\ell)}(x_0)}{\ell!}(y - x_n)^{\ell}\right| < \left|\frac{\phi^{(\ell-1)}(x_0)}{(\ell-1)!}(y - x_n)^{\ell-1}\right| \text{ or } \left|\frac{\phi^{(\ell)}(x_0)}{\ell!}\right||y - x_n| < \left|\frac{\phi^{(\ell-1)}(x_0)}{(\ell-1)!}\right|$$

for $3 \leq \ell$ and this follows by our hypotheses, (6) and the fact that $d < 1$. Hence by (7), $|\phi(x_n) + \phi'(x_n)(y - x_n)| \;=\; |\phi''(x_0)/2|\,|y - x_n|^2$ which when dividing by $\phi'(x_n)$, using $(3)_n$, gives

$$|y - x_{n+1}| \;=\; |\phi'(x_0)^{-1}\phi''(x_0)/2||\phi(x_0)\phi'^{-1}(x_0)|^2\, d^{2^{n+1}-2}$$

and this in turn is equal to $|\phi(x_0){\phi'}^{-1}(x_0)| \, d^{2^{n+1}-1}$ from the definition of d. This completes the $(n+1)$st step of (6) and hence the uniqueness part of the proposition. ∎

3. Polynomial congruences

Here we present our basic application of Proposition 2.1 from the previous section. Our goal is to examine the set of elements satisfying the congruence $\phi(x) \equiv 0$ mod $\mathfrak{a}$ in a ring $\mathfrak{o}$ when some derivative of ϕ satisfies an appropriate nondegeneracy condition. We will then look at situations where this examination gives an estimate on the number of solutions of such congruences.

The basic set-up will be the same as in the previous section; let $\mathfrak{o}$ be the ring of integers of a complete, non-archimedean absolute value $|\cdot|$, not necessarily discrete (completeness is not necessary here; see the remarks below). We will study the above congruences for $\phi \in \mathfrak{o}[X]$. Set $\bar{B}_r(x) := \{y \in \mathfrak{o} : |y - x| \leq r\}$.

Proposition 3.1. *With $\mathfrak{o}$ as above, suppose $\phi \in \mathfrak{o}[X]$ satisfies $|\phi^{(n)}(x)/n!| \geq 1$ on $\mathfrak{o}$ for some n. Furthermore we assume that the characteristic of $\mathfrak{o}$ (if positive) is larger than n. Then for $0 < \delta \leq 1$,*

$$\left\{x \in \mathfrak{o} : \ |\phi(x)| \ \leq \ \delta\right\} \ \subset \ \bigcup_{z \in \mathcal{Z}_n} \bar{B}_{c\delta^{1/n}}(z) \tag{8}$$

where $c = c_n > 0$ depends only on n and

$$\mathcal{Z}_n \ := \ \left\{x \in \mathfrak{o} : \phi^{(k)}(x) = 0, \text{ for some } \ 0 \leq k \leq n\right\}.$$

Remarks:

- The condition on the characteristic of $\mathfrak{o}$, if positive, being larger than n guarantees that for each $1 \leq k \leq n$, thought of as element of $\mathfrak{o}$ via the map $k \to k \cdot \mathbf{1}$ where $\mathbf{1}$ is the identity element of $\mathfrak{o}$, is nonzero in $\mathfrak{o}$. Hence $|k!| > 0$ for such k. If $|k!| = 1$ for $1 \leq k \leq n$, then the constant c_n in the theorem can be taken to be equal to 1. For notational convenience, we will assume $|k!| = 1$ for $1 \leq k \leq n$ in the proof of Proposition 3.1; otherwise small constants need to be inserted in the various sets $I_r, 1 \leq r \leq n$, used in the proof below.
  Furthermore the various derivatives of ϕ, up to order n which is less than the degree d of ϕ, will then be nonzero polynomials and so $\#\mathcal{Z}_n \leq d(d+1)/2$ since $\mathfrak{o}$ is an integral domain.
- The set $\mathfrak{a} = \{y \in \mathfrak{o} : |y| \leq \delta\}$ is an ideal of $\mathfrak{o}$ and therefore the set on the left-hand side of (8) is the set of elements $x \in \mathfrak{o}$ satisfying the congruence $\phi(x) \equiv 0$ mod $\mathfrak{a}$. As usual by a solution to the congruence $\phi(x) \equiv 0$ mod $\mathfrak{a}$ we mean an element $\overline{x} = x + \mathfrak{a}$ in the residue class ring $\mathfrak{o}/\mathfrak{a}$ and we denote by $\#\{\phi(x) \equiv 0 \text{ mod } \mathfrak{a}\}$, the number of solutions to this congruence. Proposition 3.1 allows us to estimate this number; indeed if N is an upper

bound on the number of disjoint balls $\bar{B}_\delta(y)$ which lie inside some fixed $\bar{B}_{c\delta^{1/n}}(z)$, then

$$\#\{\phi(x) \equiv 0 \bmod \mathfrak{a}\} \;\leq\; [d(d+1)/2]\, N. \tag{9}$$

The number N is easy to compute when the valuation $|\cdot|$ is discrete (see below); however in this case, N it is finite if and only if the residue class field is finite.

- The ring $\mathfrak{o}$ does not need to be complete; it suffices to assume that $\mathfrak{o}$ is endowed with a non-archimedean absolute value $|\cdot|$ so that $|x| \leq 1$ for every $x \in \mathfrak{o}$. However in this case, the elements of $\mathcal{Z}_n$ will belong to $\bar{\mathfrak{o}}$, the completion of $\mathfrak{o}$ with respect to $|\cdot|$ and the balls $\bar{B}$ on the right-hand side of (8) will be sets in $\bar{\mathfrak{o}}$ (of course $\mathfrak{o}$ sits inside $\bar{\mathfrak{o}}$ in a canonical way as a dense subring).

Proof As discussed in the remarks following the statement of the proposition, we will assume that $|k!| = 1$ when $1 \leq k \leq n$ for notational convenience; obvious changes to the sets I_r used below need to be made when we only have $0 < c_0 \leq |k!| \leq 1$ for such k. We decompose

$$\{x \in \mathfrak{o} : \; |\phi(x)| \;\leq\; \delta\} \;=\; I_1 \;\cup\; I_2 \;\cup\; \cdots \;\cup\; I_n$$

into disjoint sets where $I_1 := \{x : |\phi^{(n-1)}(x)| \leq \delta^{1/n}, \dots\}$ and for $2 \leq r \leq n$,

$$I_r = \{x \in \mathfrak{o} : \; |\phi^{(n-r)}(x)| \leq \delta^{1/n}|\phi^{(n-r+1)}(x)|, \; \mathcal{S}_r(x), \; \text{and} \; \dots\}$$

where $\dots$ denotes the underlying condition $|\phi(x)| \leq \delta$ and $\mathcal{S}_r(x)$ denotes the string of inequalities

$$|\phi^{(n-r+1)}(x)| > \delta^{1/n}|\phi^{(n-r+2)}(x)| > \cdots > \delta^{(r-2)/n}|\phi^{(n-1)}(x)| > \delta^{(r-1)/n}.$$

The condition $|\phi(x)| \leq \delta$ is used only to guarantee that the sets I_r do indeed decompose all of $\{x : |\phi(x)| \leq \delta\}$.

Now fix any $x_0 \in I_r$; one can easily check that the hypotheses of Proposition 2.1 are satisfied at x_0 for $\psi(x) = \phi^{(n-r)}(x)$ and $L = r - 1$. Hence Proposition 2.1 gives us a unique root z of ψ (and hence $z \in \mathcal{Z}$) so that $|x_0 - z| \leq |\psi(x_0)[\psi'(x_0)]^{-1}|$. But $\psi(x_0)[\psi'(x_0)]^{-1} = \phi^{(n-r)}(x_0)[\phi^{(n-r+1)}]^{-1}$ which in absolute value is less than or equal to $\delta^{1/n}$ by the first condition set out in I_r. This puts $x_0 \in \bar{B}_{\delta^{1/n}}(z)$ as desired. ∎

We will now apply Proposition 3.1 in the setting of Dedekind domains where discrete valuations arise in a natural way. Hence $\mathfrak{o}$ will denote a Dedekind domain; that is, $\mathfrak{o}$ is an integral domain which is Noetherian, integrally closed, and such that every nonzero prime ideal is maximal (equivalently the nonzero fractional ideas of $\mathfrak{o}$ form a group under multiplication, or more analytically, $\mathfrak{o}$ is the ring of integers for a set of places with the *strong approximation property* as defined by Artin).

In order to keep things finite, our underlying assumption will be that every residue class field $\mathfrak{o}/\mathfrak{p}$ ($\mathfrak{p}$ a nonzero prime) is finite. Then if $\mathfrak{a}$ is a nonzero ideal of $\mathfrak{o}$,

$$\mathfrak{o}/\mathfrak{a} \;\simeq\; \prod_{\mathfrak{p}} \mathfrak{o}/\mathfrak{p}^{n_\mathfrak{p}} \quad \text{and} \quad \|\mathfrak{a}\| \;=\; \prod_{\mathfrak{p}} \|\mathfrak{p}\|^{n_\mathfrak{p}} \tag{10}$$

where $\mathfrak{a} = \prod \mathfrak{p}^{n_\mathfrak{p}}$ is the unique factorisation of $\mathfrak{a}$ into nonzero prime ideals $\mathfrak{p}$ and $\|\mathfrak{a}\|$ denotes the number of elements in the residue class ring $\mathfrak{o}/\mathfrak{a}$ (often referred to as the absolute norm of an ideal); see for example, [5]. Recall that by a solution to a polynomial congruence $\phi(x) \equiv 0 \bmod \mathfrak{a}$ we mean an element $\overline{x} = x + \mathfrak{a}$ in the residue class ring $\mathfrak{o}/\mathfrak{a}$ and we denote by $\#\{\phi(x) \equiv 0 \bmod \mathfrak{a}\}$, the number of solutions to this congruence; furthermore we denote by

$$|\{\phi(x) \equiv 0 \bmod \mathfrak{a}\}| := \frac{1}{\|\mathfrak{a}\|} \#\{\phi(x) \equiv 0 \bmod \mathfrak{a}\},$$

the relative (or normalised) number of solutions which by our underlying finiteness assumption makes sense.

Since every nonzero ideal $\mathfrak{a} = \prod \mathfrak{p}^{n_\mathfrak{p}}$ has a unique factorisation into a product of powers of distinct prime ideals, each pair of factors being relatively prime, the Chinese remainder theorem and (10) show that

$$|\{\phi(x) \equiv 0 \bmod \mathfrak{a}\}| = \prod_\mathfrak{p} |\{\phi(x) \equiv 0 \bmod \mathfrak{p}^{n_\mathfrak{p}}\}|$$

and so we may assume that our ideal is a power $\mathfrak{p}^s$ of a fixed prime ideal $\mathfrak{p}$. Any such prime ideal $\mathfrak{p}$ gives rise to a discrete valuation on $\mathfrak{o}$ (and hence on its field of fractions); in multiplicative form, we write $|x|_\mathfrak{p} = \|\mathfrak{p}\|^{-t}$ if $\mathfrak{p}^t$ appears as the $\mathfrak{p}$ factor in the prime ideal decomposition of $x\mathfrak{o}$, the principal ideal generated by x. Since the prime $\mathfrak{p}$ is fixed, we simply write $|x|$ to denote $|x|_\mathfrak{p}$ in the following. With this notation, the congruence $\phi(x) \equiv 0 \bmod \mathfrak{p}^s$ can be written as $|\phi(x)| \leq \|\mathfrak{p}\|^{-s}$.

By the last remark after the statement of Proposition 3.1, taking $\delta = \|\mathfrak{p}\|^{-s}$, we can conclude that (8) holds if $|\phi^{(n)}(x)/n!| \geq 1$ on $\mathfrak{o}$ (and if the characteristic of $\mathfrak{o}$, when positive, is larger than n). Furthermore by the second remark after the statement of Proposition 3.1, in order to convert (8) into an estimate on the number of congruences in this context, we simply need to count, in the completion $\bar{\mathfrak{o}}$ of $\mathfrak{o}$ with respect to $|\cdot|$, the number N of disjoint balls $\bar{B}_\delta(y)$ contained in a fixed $\bar{B}_{c\delta^{1/n}}(z)$. Via the unique power series representations of elements in $\bar{\mathfrak{o}}$ (see the fourth remark below), one easily gets a bound (when $c = 1$, say) $N \leq \|\mathfrak{p}\|^{s - \frac{s}{n}}$ with equality if $s \equiv 0 \bmod n$; otherwise there is a slight gain for N. Therefore in this context, Proposition 3.1 has the following consequence.

Corollary 3.2. *In the above setting, suppose that for some $n \geq 1$, $\phi^{(n)}(x)/n! \not\equiv 0$ mod $\mathfrak{p}$ for any $x \in \mathfrak{o}$. Furthermore, suppose that the charateristic of $\mathfrak{o}$, when positive, is greater than n. Then*

$$|\{\phi(x) \equiv 0 \bmod \mathfrak{p}^s\}| \leq C_d \|\mathfrak{p}^s\|^{-1/n} \tag{11}$$

for some constant C_d depending only on the degree d of $\phi \in \mathfrak{o}[X]$.

Remarks:

- The condition on $\phi^{(n)}$ and both the right and left hand sides of (11) are multiplicative over powers of prime ideals and so the proposition could have been stated for general ideals. In the case the constant c is 1 in (8), one can take $C_d = [d(d+1)/2]$.

- The hypothesis on the nth derivative of ϕ can be relaxed to the following: the congruences $\phi^{(n)}(x) \equiv 0 \bmod \mathfrak{p}$ and $\phi^{(n-1)}(x) \equiv 0 \bmod \mathfrak{p}$ have no common solutions. The same remark applies to Proposition 3.1.
- With our notation, the hypothesis on ϕ becomes $|\phi^{(n)}(x)/n!| \geq 1$ on $\mathfrak{o}$ and (11) can be written as

$$|\{|\phi(x)| \leq \|\mathfrak{p}\|^{-s}\}| \leq C_d \|\mathfrak{p}\|^{-s/n}$$

which bears a striking similarity to the basic sublevel estimate (2) on $\mathbb{R}$ discussed in the introduction.
- Consider the completion $\bar{\mathfrak{o}}$ of $\mathfrak{o}$ with respect to the valuation $|\cdot| = |\cdot|_{\mathfrak{p}}$ arising from the prime ideal $\mathfrak{p}$ mentioned above. Then $\bar{\mathfrak{o}}$ is a complete discrete valuation ring and the valuation $|\cdot|$ extends uniquely to $\bar{\mathfrak{o}}$. Let π be a prime element generating the maximal ideal $\pi\bar{\mathfrak{o}}$ of $\bar{\mathfrak{o}}$. From the isomorphism $\mathfrak{o}/\mathfrak{p} \to \bar{\mathfrak{o}}/\pi\bar{\mathfrak{o}}$ we see that $\bar{\mathfrak{o}}$ is compact by our finiteness hypothesis; furthermore, each element $x \in \bar{\mathfrak{o}}$ has a unique convergent power series expansion

$$x = \sum_{j=0}^{\infty} x_j \pi^j = x_0 + x_1\pi + x_2\pi^2 + \cdots$$

where the coefficients $\{x_j\}$ lie in a fixed set of representations of the elements in the residue class field $\bar{\mathfrak{o}}/\pi\bar{\mathfrak{o}}$. Furthermore, since $\bar{\mathfrak{o}} = \mathfrak{o} + \pi^t\bar{\mathfrak{o}}$ for any $t \geq 0$ and $\pi^s\bar{\mathfrak{o}} \cap \mathfrak{o} = \mathfrak{p}^s$ (see [5] for these various elementary facts) one easily checks that the number of solutions of $\phi(x) \equiv 0 \bmod \mathfrak{p}^s$, counted as elements in $\mathfrak{o}/\mathfrak{p}^s$, is equal to the number of solutions of $\phi(x) \equiv 0 \bmod \pi^s\bar{\mathfrak{o}}$, counted as elements in $\bar{\mathfrak{o}}/\pi^s\bar{\mathfrak{o}}$.

  Therefore, without loss of generality, we may reduce to the case that $\mathfrak{o}$ is a complete discrete valuation ring; in fact, the compact ring of integers of a local field by our finiteness hypothesis.
- If $\phi(x) = a_d x^d + \cdots + a_0 \in \mathfrak{o}[X]$, then we may assume, without loss of generality, that at least one coefficient a_j does not lie in $\mathfrak{p}^s$; furthermore, if ϕ is normalised in the sense that at least one coefficient a_j does not lie in $\mathfrak{p}$, then if n is largest exponent so that $a_n \notin \mathfrak{p}$, $\phi^{(n)}(x)/n! \not\equiv 0 \bmod \mathfrak{p}$ for any $x \in \mathfrak{o}$ and hence Proposition 3.2 implies (11) holds with this n.

  By the previous remark we may make the reduction to a discrete valuation ring (hence a principal ideal domain) and here one can reduce easily to a normalised phase ϕ. With the notation above, we may assume $\mathfrak{p} = \pi\mathfrak{o}$ for some prime element π and so $\phi(x) = e\,\varphi(x)$ where φ is normalised and e is a greatest common divisor of the coefficients $a_n, a_{n-1}, \ldots, a_0$ and π^s; hence $e\mathfrak{o} = \langle a_n, \ldots, a_0, \pi^s \rangle = (\pi\mathfrak{o})^t$ for some $0 \leq t \leq s$ and therefore $|e| = |\pi|^t = \|\mathfrak{p}\|^{-t}$. Since

$$|\{|\phi(x)| \leq \|\mathfrak{p}\|^{-s}\}| = |\{|\varphi(x)| \leq \|\mathfrak{p}\|^{-s+t}\}|$$

and since the hypothesis of Proposition 3.2 is satisfied for some $0 \leq n \leq d$, $d = \text{degree } \phi$, we obtain the estimate

$$|\{|\phi(x)| \leq \|\mathfrak{p}\|^{-s}\}| \leq C_d \|\mathfrak{p}\|^{-(s-t)/d}.$$

If we introduce the notation $\|x\|_s := |x|/|\pi|^s$, a normalised "norm" with respect to the factor ring $\mathfrak{o}/\mathfrak{p}^s$ (as we did in the introduction in the setting of the rational integers $\mathbb{Z}$) and extend this to n-tuples $\vec{x} = (x_1, \ldots, x_n)$

of elements in this factor ring via $\|\vec{x}\|_s := \max_j \|x_j\|_s$, then the estimate above can be written as

$$|\{\|\phi(x)\|_s \leq 1\}| \ \leq \ C_d \|\vec{a}\|_s^{-1/d} \tag{12}$$

where $\vec{a} = (a_n, \dots, a_0)$ collects together the coefficients of ϕ. This should be compared to (1) in the introduction.

- Consider the case $\mathfrak{o} = \mathbb{Z}$ and $\mathfrak{p} = p\mathbb{Z}$, p a prime so that $|\cdot|$ is the p-adic valuation. In this setting, the estimate (11) is a result of Hua which follows from his classical estimate on complete exponential sums discussed in the introduction. Our approach is somewhat backwards, establishing (8) or (11) first, by direct means, and then using this, we move on to character sums which is the subject of the next section.

4. Character sum estimates

The analysis in the proof of Proposition 3.1 can be applied to give bounds for character sums. We begin in the following setting: suppose $\mathfrak{o}$ is a complete, discrete, valuation ring with π a prime element so that the residue class field $\mathfrak{o}/\pi\mathfrak{o}$ is finite, say with $q = p^c$ elements where p is prime (again completeness is not necessary; see the remarks below). We take the valuation normalised so that $|\pi| = q^{-1}$.

Via the unique power series representation of elements $x = \sum_{j \geq 0} x_j \pi^j$ in $\mathfrak{o}$ with the x_j lying in a fixed set of representations of the elements of the field $\mathfrak{o}/\pi\mathfrak{o}$, we identify each element $\bar{x} = x + \pi^s \mathfrak{o} = \bar{B}_{q^{-s}}(x)$ in the factor ring $\mathfrak{o}/\pi^s\mathfrak{o}$ with the truncated expansion $x_0 + x_1\pi + \cdots + x_{s-1}\pi^{s-1}$ of x, uniquely determined by $\bar{x}$.

Let χ' be a non-principal additive character on the factor ring $\mathfrak{o}/\pi^s\mathfrak{o}$ and $\bar{\phi}$ a polynomial with coefficients in $\mathfrak{o}/\pi^s\mathfrak{o}$. With the above identifications, the character sum

$$S := q^{-s} \sum_{\bar{x} \in \mathfrak{o}/\pi^s\mathfrak{o}} \chi'(\bar{\phi}(\bar{x})) \ = \ q^{-s} \sum_{x \leq \pi^s} \chi(\phi(x)) \tag{13}$$

where χ is a non-principal additive character of $\mathfrak{o}$ which is equal to 1 on $\pi^s\mathfrak{o}$ and $\phi \in \mathfrak{o}[X]$ (the coefficients a_j of ϕ being some choice of representation in $\mathfrak{o}$ of the corresponding coefficient $\bar{a}_j$ of $\bar{\phi}$); here we use the nonstandard notation $\sum_{x \leq \pi^s}$ to indicate the finite sum over elements in $\mathfrak{o}$ of the form $x = x_0 + x_1\pi + \cdots + x_{s-1}\pi^{s-1}$ where each x_j varies over the q representations in $\mathfrak{o}$ of the elements in the residue class field.

With this notation, the elements $x \leq \pi^s$ can be decomposed as $x = y + \pi^t z$ where $y, z \in \mathfrak{o}$ vary over the sets $y \leq \pi^t$ and $z \leq \pi^{s-t}$, respectively (here $0 < t < s$ is a parameter defining the decomposition) and this in turn gives rise to a decomposition

$$\sum_{x \leq \pi^s} \chi(\phi(x)) \ = \ \sum_{y \leq \pi^t} \sum_{z \leq \pi^{s-t}} \chi(\phi(y + \pi^t z))$$

which we will repeatedly perform. Finally we make the simple observation that if χ is a non-principal character on $\mathfrak{o}$ which is equal to 1 on $\pi^s\mathfrak{o}$ and $\pi^s \nmid c$ (that is,

$|c| > q^{-s}$) for some $c \in \mathfrak{o}$, then $\sum_{x \leq \pi^s} \chi(cx) = 0$. In fact if $|c| = q^{-t}$, decompose the sum via $x = v + \pi^{s-t}u$ so that

$$\sum_{x \leq \pi^s} \chi(cx) \; = \; \sum_{v \leq \pi^{s-t}} \chi(\pi^t c'v) \sum_{u \leq \pi^t} \chi(\pi^s c'u) \; = \; q^t \sum_{v \leq \pi^{s-t}} \chi(\pi^t c'v)$$

where $c' = \pi^{-t}c$ is a unit in $\mathfrak{o}$; here we used the fact that χ is equal to 1 on $\pi^s\mathfrak{o}$. But $\widetilde{\chi}(v) := \chi(\pi^t c'v)$ is a non-principal character on $\mathfrak{o}$ which is equal to 1 on $\pi^{s-t}\mathfrak{o}$ and hence the last sum above can be written as

$$\sum_{\bar{v} \in \mathfrak{o}/\pi^{s-t}\mathfrak{o}} \widetilde{\chi}'(\bar{v})$$

where $\widetilde{\chi}'$ is a non-trivial, non-principal character on the factor ring $\mathfrak{o}/\pi^{s-t}\mathfrak{o}$ and therefore this sum vanishes.

Proposition 4.1. *With the above setup, suppose ϕ satisfies $|\phi^{(n)}(x)/n!| \geq 1$ on $\mathfrak{o}$ for some n (equivalently $\bar{\phi}^{(n)}(x)/n!$ never vanishes when thought of as an element in the residue class field). If the characteristic of $\mathfrak{o}$, when positive, is larger than n, then $|S| \leq C_d\, q^{-s/n}$ for some C_d depending only on the degree d of ϕ.*

Remarks:

- As mentioned above, completeness of the ring is not necessary. Suppose that $\mathfrak{o}$ is a ring endowed with a discrete valuation (non-archimedean absolute value) so that $|x| \leq 1$ for every $x \in \mathfrak{o}$ and let $\bar{\mathfrak{o}}$ be its completion. It is easy to see that the prime element π and representations $\{x_j\}$ in $\bar{\mathfrak{o}}$ of the residue class field of $\bar{\mathfrak{o}}$, which give us the power series representations, can be chosen from the ring $\mathfrak{o}$ itself. From the second remark after Proposition 2.1 and third remark after Proposition 3.1, one can easily check that the proof below carries through with no change and so Proposition 4.1 holds in this more general setting. In particular we obtain bounds for character sums in the setting of a Dedekind domain $\mathfrak{o}$ where any nonzero prime ideal $\mathfrak{p}$ gives rise to a discrete valuation.
- In the setting of the previous remark (where we do not assume completeness), suppose in addition that $\mathfrak{o}$ is a principal ideal domain. Then any polynomial $\phi(x) = a_d x^d + \cdots + a_1 x \in \mathfrak{o}[X]$ which is normalised so that the greatest common divisor of the a_j's and π^s is equal to 1 (which we may assume without loss of generality) will satisfy the hypothesis of Proposition 4.1 for some $n \leq d$; see the fifth remark after the statement of Corollary 3.2. Now consider the ring of rational integers $\mathbb{Z}$ with the p-adic valuation given by a prime p. Proposition 4.1 then implies a classical result of Hua [4] on complete exponential sums; namely

$$\left| p^{-s} \sum_{x=1}^{p^s} e^{2\pi i [a_d x^d + \cdots + a_1 x]/p^s} \right| \; \leq \; C_d\, p^{-s/d} \tag{14}$$

  where $gcd(a_d, \ldots, a_1, p^s) = 1$. Hua's original argument gives an estimate $d^3 q^{-s/d}$ in (14) but his argument has been refined over the years to give a much better estimate; for instance, if S denotes the exponential sum in (14), then one has the uniform estimate $|S| \leq 4.41 p^{-s/d}$ for any d and 4.41

can be replaced by 1 if d is large enough (see [3] and [2], [7]). The constant C_d in Propsition 4.1 only gives $d^2/2$ if $p > d$ but the proof below gives a very different approach than traditional proofs of Hua's result.

- When $\mathfrak{o}$ is complete with respect to a discrete valuation so that the residue class field is finite, the ring $\mathfrak{o}$ is then the compact ring of integers of a local field K, the quotient field of $\mathfrak{o}$. We then have at our a disposal a Haar measure μ on K which we normalise so that $\mu(\mathfrak{o}) = 1$. Let $\psi(x) = c_d x^d + \cdots c_1 x \in K[X]$ and let χ be an element in the (additive) dual of K which is not the identity, and normalised so that χ is equal to 1 on $\mathfrak{o}$. Consider the "oscillatory" integral

$$I = \int_{\mathfrak{o}} \chi(\psi(x)) \, d\mu(x).$$

Without loss of generality, suppose that $\max_j(|c_j|) = q^s$ for some $s > 0$. Let c denote a coefficient of ψ where this maximum is achieved and set $\phi(x) = c^{-1}\psi(x) \in \mathfrak{o}[X]$. Then $\chi'(u) := \chi(cu)$ is a non-principal character on $\mathfrak{o}$ which is equal to 1 on $\pi^s \mathfrak{o}$ and hence induces a character on the factor ring $\mathfrak{o}/\pi^s \mathfrak{o}$ so that

$$I = q^{-s} \sum_{y \in \mathfrak{o}/\pi^s \mathfrak{o}} \chi'(\phi(y))$$

with our usual identifications. As we discussed before, the phase ϕ satisfies our hypothesis for some $n \le d$ and so Proposition 4.1 implies that $|I| \le (d^2/2)q^{-s/d}$ where we recall $q^s = \max(|c_j|)$. When $\mathfrak{o}$ is the ring of p-adic integers (so $q = p$), the refinements of Hua's result give $|I| \le 4.41 q^{-s/d}$.

Proof We divide the proof into three cases: first we consider the case when $s \equiv 0$ mod n.

Using the representation of the character sum S in (13), we decompose the sum on the right via $x = y + \pi^{s/n} z$ and write

$$S = q^{-s} \sum_{y \le \pi^{\frac{s}{n}}} \chi(\phi(y)) \cdot \sum_{z \le \pi^{\frac{n-1}{n} s}} \chi(\pi^{s/n} \psi_y(z)), \qquad (15)$$

using our nonstandard notation to indicate the range of sums; here

$$\psi_y(z) = \sum_{j=1}^{n-1} \frac{\phi^{(j)}(y)}{j!} \pi^{\frac{s}{n}(j-1)} z^j.$$

For each y we will denote the inner sum in the above decomposition (15) by T_y. Our goal is simply to show that $\#\{y : T_y \ne 0\} \le d^2$ which, together with the trivial bound $|T_y| \le q^{\frac{n-1}{n} s}$, gives the desired estimate in this case.

We slightly modify the central objects in Proposition 3.1; replace $\mathcal{Z}$ with

$$\mathcal{Z}' := \{x_* \in \mathfrak{o} : \phi^{(j)}(x_*) = 0, \text{ for some } 1 \le j \le n - 1\},$$

take $\delta = |\pi|^s = q^{-s}$ and replace the sets I_r with

$$I_r' = \{y \le \pi^{s/n} : |\phi^{(n-r)}(y)| \le q^{-s/n} |\phi^{(n-r+1)}(y)| \text{ and } \mathcal{S}_r(y) \text{ holds}\}$$

when $1 \le r \le n-1$, dropping the condition $|\phi(y)| \le \delta$. Finally we set $I'_n := \{y \le \pi^{s/n} : \mathcal{S}_n(y) \text{ holds}\}$, further dropping the condition $|\phi(y)| \le \delta^{1/n}|\phi'(y)|$ appearing in I_n. We note that $\#\mathcal{Z}' \le d^2/2$.

This gives us a disjoint decomposition of the y sum in (15)

$$S = q^{-s} \sum_{r=1}^{n} \sum_{y \in I'_r} \chi(\phi(y)) \cdot T_y,$$

but the analysis in the proof of Proposition 3.1 shows that Proposition 2.1 implies that to every $y \in I'_r, 1 \le r \le n-1$, there is a unique element in $\mathcal{Z}'$ associated to it; hence there at most $\#\mathcal{Z}'$ terms in the sum

$$\sum_{r=1}^{n-1} \sum_{y \in I'_r} \chi(\phi(y)) \cdot T_y.$$

Finally we claim that for every $y \in I'_n$, the sum T_y vanishes and this will finish the proof in this case. In fact recall that if $y \in I'_n$,

$$|\phi'(y)| > q^{-s/n}|\phi''(y)| > \cdots > q^{-\frac{n-2}{n}s}|\phi^{(n-1)}(y)| > q^{-\frac{n-1}{n}s}. \qquad (16)$$

Hence a greatest common divisor of the coefficients of $\psi_y(z)$, together with $\pi^{\frac{n-1}{n}s}$, is $\pi^{t+\frac{s}{n}}$ where t is defined by $|\phi''(y)| = q^{-t}$. We decompose the sum T_y via $z = v + \pi^\theta u$ where $0 < \theta := s(1 - \frac{2}{n}) - t < \frac{n-1}{n}s$. Using (16) and the fact that χ is equal to 1 on $\pi^s\mathfrak{o}$, we see that

$$T_y = \sum_{v \le \pi^\theta} \chi(\pi^{s/n}\psi_y(v)) \sum_{u \le \pi^{t+\frac{s}{n}}} \chi(\pi^{\frac{s}{n}+\theta}\phi'(y)u).$$

But the inner sum in u vanishes by our earlier observation since $\widetilde{\chi}(w) := \chi(\pi^{\frac{s}{n}+\theta}w) = \chi(\pi^{s-(t+s/n)}w)$ is a non-principal character on the factor ring $\mathfrak{o}/\pi^{t+\frac{s}{n}}\mathfrak{o}$ and $\pi^{t+s/n}$ does not divide $\phi'(y)$ by (16). This completes the proof in the first case.

We turn now to the second case: when $s \equiv \ell \mod n$ with $2 \le \ell \le n-1$. This case is almost identical to the first case with one small twist which will prepare us for the final case. Write $s = ng + \ell$ for some g and decompose the sum S via $x = y + \pi^{g+1}z$ so that

$$S = q^{-s} \sum_{y \le \pi^{g+1}} \chi(\phi(y)) \cdot \sum_{z \le \pi^{(n-1)g+\ell-1}} \chi(\pi^{g+1}\psi_y(z)), \qquad (17)$$

where

$$\psi_y(z) = \sum_{j=1}^{n-1} \frac{\phi^{(j)}(y)}{j!}\pi^{(g+1)(j-1)}z^j.$$

For each y we will denote again the inner sum in the above decomposition (17) by T_y. We now proceed exactly as in the first case, using the set $\mathcal{Z}'$, the sets $I'_r, 1 \le r \le n$ except that $\pi^{s/n}$ is replaced everywhere by π^{g+1}, and Proposition 2.1 to conclude

$$S = q^{-s} \sum_{y \in I'_n} \chi(\phi(y)) \cdot T_y + E$$

where
$$|E| \;\leq\; \#\mathcal{Z}' q^{-s} q^{(n-1)g+\ell-1} \;=\; \#\mathcal{Z}' q^{-(g+1)} \;\leq\; \#\mathcal{Z}' q^{-s/n}. \qquad (18)$$

As in the first case we will show that $T_y = 0$ for every $y \in I'_n$.

For each $1 \leq j \leq n-1$, suppose $|\phi^{(j)}(y)| = q^{-\eta_j}$ so that for $y \in I'_n$, we have
$$\eta_2 + g + 1 < \eta_3 + 2(g+1) < \cdots < \eta_{n-1} + (n-2)(g+1) < (n-1)(g+1)$$
or
$$\eta_2 + g \;\leq\; \eta_3 + 2g \;\leq\; \cdots \;\leq\; \eta_{n-1} + (n-2)g \;\leq\; (n-1)g. \qquad (19)$$

Hence a greatest common divisor of the coefficients of $\psi_y(z)$, together with $\pi^{(n-1)g+\ell-1}$, is π^{η_2+g+1} (here we are using $\ell \geq 2$ in a crucial way). Now arguing exactly as in the first case, we see that $T_y = 0$ for every $y \in I'_n$, establishing the desired estimate for S in this case.

Finally we turn to the last case: when $s \equiv 1 \bmod n$ which is the most difficult. Again we write $s = ng + 1$ and begin as in the second case, decomposing S as in (17):
$$S \;=\; q^{-s} \sum_{y \leq \pi^{g+1}} \chi(\phi(y)) \cdot \sum_{z \leq \pi^{(n-1)g}} \chi(\pi^{g+1} \psi_y(z)),$$

where
$$\psi_y(z) \;=\; \sum_{j=1}^{n-1} \frac{\phi^{(j)}(y)}{j!} \pi^{(g+1)(j-1)} z^j.$$

As before we denote the inner sum in z by T_y. With the second case highlighting the difficulty to come, we decompose the y sum further, writing
$$S \;=\; S_1 + S_2 \quad \text{where} \quad S_2 \;=\; q^{-s} \sum_{y \in \Lambda} \chi(\phi(y)) \cdot T_y$$

and
$$\Lambda \;=\; \big\{ y \leq \pi^{g+1} : \pi^g | \phi^{(n-1)}(y), \; \pi^{2g} | \phi^{(n-2)}(y), \ldots, \pi^{(n-2)g} | \phi''(y) \big\}.$$

The sum S_1 is treated exactly as in the second case; that is, every element of $y \in \cup_{r-1}^{n-1} I'_r$ is uniquely associated to some $x_* \in \mathcal{Z}'$ and $T_y = 0$ for every $y \in I'_n$. To see this last point, the vanishing of T_y, recall that in the case when $s \equiv \ell \bmod n$ with $\ell \geq 2$, this vanishing followed from the observation that a greatest common divisor of the coefficients of $\psi_y(z)$ and $\pi^{(n-1)g+\ell-1}$ is π^{η_2+g+1} which in turn followed from (19) and the assumption $\ell \geq 2$. However we can still deduce this observation about the greatest common divisor if there is at least one *strict* inequality in (19). But, in the sum S_1, $y \notin \Lambda$ and this forces at least one strict inequality in (19). We record the estimate obtained for S_1, referring back to (18),
$$|S_1| \;\leq\; \#\mathcal{Z}' q^{-(g+1)} \;\leq\; (d^2/2)\, q^{-s/n} q^{-(1-\frac{1}{n})}. \qquad (20)$$

We turn to the sum S_2. It is no longer the case that T_y will automatically vanish but nevertheless (19) implies that T_y simplifies to
$$T_y \;=\; \sum_{z \leq \pi^{(n-1)g}} \chi(\pi^{g+1} \phi'(y) z)$$

which vanishes unless $\pi^{(n-1)g} | \phi'(y)$. Hence $S_2 = q^{-(g+1)} \sum_{y \in \Lambda'} \chi(\phi(y))$ where now

$$\Lambda' = \left\{ y \le \pi^{g+1} : \pi^g | \phi^{(n-1)}(y), \ \pi^{2g} | \phi^{(n-2)}(y), \dots, \pi^{(n-2)g} | \phi''(y), \pi^{(n-1)g} | \phi'(y) \right\}.$$

We wish to decompose S_2 further via $y = v + \pi^g u$ but we first observe that with respect to this decomposition, $y \in \Lambda'$ if and only if $v \in \Lambda''$ where

$$\Lambda'' = \left\{ v \le \pi^g : \pi^g | \phi^{(n-1)}(v), \ \pi^{2g} | \phi^{(n-2)}(v), \dots, \pi^{(n-2)g} | \phi''(v), \pi^{(n-1)g} | \phi'(v) \right\}.$$

This is established by the following claim.

Claim: For each $1 \le j \le n-1$, $\phi^{(n-j)}(y) \equiv \phi^{(n-j)}(v) \mod \pi^{jg}$.

We prove this by induction on j; the $j = 1$ case being trivial. But

$$\phi^{(n-j)}(y) \ \equiv \ \phi^{(n-j)}(v) + \sum_{r=1}^{j-1} \frac{\phi^{(n-j+r)}(v)}{r!} \pi^{rg} u^r \quad \mathrm{mod} \quad \pi^{jg}$$

which in turn is equivalent to $\phi^{(n-j)}(v) \mod \pi^{jg}$ by induction.

We now carry out this decomposition of S_2 via $y = v + \pi^g u$, using the claim, and write

$$S_2 \ = \ q^{-(g+1)} \sum_{v \in \Lambda''} \sum_{u \le \pi} \chi(\phi(v + \pi^g u)).$$

Expanding around v we get $\phi(v + \pi^g u) \equiv \phi(v) + \psi_v(u) \mod \pi^s$ where

$$\psi_v(u) \ = \ \phi'(v)\pi^g u + \frac{\phi''(v)}{2} \pi^{2g} u^2 + \cdots + \frac{\phi^{(n)}(v)}{n!} \pi^{ng} u^n$$

and so $S_2 = q^{-(g+1)} \sum_{v \in \Lambda''} \chi(\phi(v)) \sum_{u \le \pi} \chi(\psi_v(u))$. Since $v \in \Lambda''$, we may factor out π^{ng} from ψ_v to write

$$S_2 \ = \ q^{-(g+1)} \sum_{v \in \Lambda''} \chi(\phi(v)) \sum_{u \le \pi} \chi(\pi^{ng} \rho_v(u))$$

where $\rho_v(u) = \pi^{-ng} \psi_v(u) \in \mathfrak{o}[X]$. The character $\widetilde{\chi}(w) := \chi(\pi^{ng} w)$ induces a non-principal character on the finite field $\mathfrak{o}/\pi\mathfrak{o}$ and the inner sum in u above becomes a nontrivial character sum over a finite field and so we can apply A. Weil's estimate to it since $\pi \nmid \phi^{(n)}(v)$. This estimate gives $|I_v| \le (n-1)q^{1/2}$ where I_v denotes the inner sum and hence $|S_2| \le (n-1)q^{-s/n} q^{-(\frac{1}{2}-\frac{1}{n})} \# \Lambda''$.

For each $v \in \Lambda''$, $\pi^g | \phi^{(n-1)}(v)$ and since $\pi \nmid \phi^{(n)}(v)$, an application of Proposition 2.1 (in fact we need only the classical Hensel lemma here) shows that there is a unique $x_* \equiv v \mod \pi^g$ so that $\phi^{(n-1)}(x_*) = 0$. Therefore $\# \Lambda'' \le d - n + 1$ which implies the estimate

$$|S_2| \ \le \ (d^2/4) \, q^{-s/n} q^{-(\frac{1}{2}-\frac{1}{n})} \tag{21}$$

since $(n-1)(d-n+1) \le d^2/4$. Since $S = S_1 + S_2$, the estimates (20) and (21) combine to give the desired estimate in this final case, completing the proof of the proposition. ∎

References

[1] A. Carbery, B. Stones and J. Wright, *Averages in vector spaces over finite fields*, Math. Proc. Camb. Phil. Soc. 144 no. 13 (2008), 13-27.

[2] J.R. Chen, *On Professor Hua's estimate of exponential sums*, Sci. Sinica 20 (1977), 711-719.

[3] T. Cochrane and Z. Zheng, *On upper bounds of Chalk and Hua for exponential sums*, Proc. Amer. Math. Soc. 129 no. 9 (2001), 2505-2516.

[4] L.K. Hua, *On an exponential sum*, J. Chinese Math. Soc. 20 (1940), 301-312..

[5] S. Lang, *Algebraic numbers*, Addison-Wesley Publishing Company, 1964.

[6] G. Mochenhaupt and T. Tao, *Restriction and Kakeya phenomena for finite fields*, Duke Math. J. 121 (2004), 35-74.

[7] S.B. Steckin, *Estimate on a complete rational trigonometric sum*, Proc. Steklov Inst. 143 (1977), 188-220.

[8] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. USA 34 (1948), 204-207.

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