

# ON POLYNOMIAL CONGRUENCES

JAMES WRIGHT

ABSTRACT. We extend a result of Loxton and Smith [4] giving a bound on the number of solutions to a polynomial congruence. More importantly we also give a general lower bound on the number of such solutions which illustrates the sharpness of the upper bound.

## 1. INTRODUCTION

In this note we study the number of solutions to the polynomial congruence  $f \equiv 0 \pmod{p^\alpha}$  for some rational prime  $p$  and any positive integer  $\alpha$ . Since the number of solutions to such a congruence is multiplicative, this leads to bounds on the number of solutions to  $f \equiv 0 \pmod{q}$  for any natural number  $q$ . Let

$$f(x) = a_d x^d + \cdots + a_1 x + a_0 = a_d \prod_{j=1}^m (x - \xi_j)^{e_j}$$

be a polynomial in  $\mathbb{Z}[X]$  of degree  $d = \sum_j e_j$  where  $\xi_1, \dots, \xi_m$  are the distinct roots of  $f$  lying in  $K$ , the algebraic number field generated by these roots. We fix a prime  $p$  and define the  $p$ -adic valuation  $\text{ord}_p(x)$  on elements in  $\mathbb{Z}$  as the nonnegative integer  $\theta$  so that  $p^\theta$  appears as the  $p$  factor in the prime decomposition of  $x$ . We also fix any extension of this valuation to  $K$  which we also denote by  $\text{ord}_p$ . By a *root cluster*  $\mathcal{C}$  we mean a subset  $\mathcal{C} \subset \{\xi_1, \dots, \xi_m\}$  of the roots of  $f$  and we denote by  $S(\mathcal{C}) = \sum_{j: \xi_j \in \mathcal{C}} e_j$  the number of roots in this cluster, counted with multiplicity. Furthermore, for each root  $\xi_j$  and cluster  $\mathcal{C}$  containing  $\xi_j$ , we define

$$\delta_p(\xi_j; \mathcal{C}) := \text{ord}_p \left( a_d \prod_{k: \xi_k \notin \mathcal{C}} (\xi_j - \xi_k)^{e_k} \right)$$

and

$$\theta_j = \theta_j(\alpha) := \max_{\xi_j \in \mathcal{C}} \frac{(\alpha - \delta_p(\xi_j; \mathcal{C}))}{S(\mathcal{C})}$$

where the maximum is taken over all root clusters  $\mathcal{C}$  containing the root  $\xi_j$ .

Finally we pick out a special set of indices  $\mathcal{I} := \{1 \leq j \leq m : \mathcal{B}_{\theta_j}(\xi_j) \cap \mathbb{Z} \neq \emptyset\}$  where we use the notation  $\mathcal{B}_\theta(z)$  to denote the set  $\{y \in K : \theta \leq \text{ord}_p(y - z)\}$  in  $K$  (using the multiplicative form  $|y| := p^{-\text{ord}_p(y)}$  of this valuation on  $K$ , this set is simply the “ball”  $\{y \in K : |y - z| \leq p^{-\theta}\}$ ). Our result gives the following bound on the number  $N(f; p^\alpha)$  of elements in  $\{x \pmod{p^\alpha} : f(x) \equiv 0 \pmod{p^\alpha}\}$ .

---

1991 *Mathematics Subject Classification.* 11A07, 11C08.

The author was supported in part by an EPSRC grant.

**Theorem 1.1.** *With the notation as above, if  $\min_{j \in \mathcal{I}} \theta_j \leq \alpha$ , we have*

$$p^{\alpha - \min_{j \in \mathcal{I}} \theta_j - 1} \leq N(f; p^\alpha) \leq m p^{\alpha - \min_{j \in \mathcal{I}} \theta_j} \quad (1)$$

where the minimum  $\min_{j \in \mathcal{I}} \theta_j$  is interpreted as  $\infty$  if  $\mathcal{I} = \emptyset$ .

*Remarks:*

- If one considers only the singleton cluster  $\mathcal{C} = \{\xi_j\}$  for each root  $\xi_j$  in the discussion above, and defines

$$\delta'_p(\xi_j) = \text{ord}_p(f^{(e_j)}(\xi_j)/e_j!) \quad \text{and} \quad \theta'_j(\alpha) = (\alpha - \delta'_p(\xi_j))/e_j$$

accordingly, then the upper bound in Theorem 1.1 gives  $N(f; p^\alpha) \leq m p^{\alpha - \min_j \theta'_j}$  which implies the upper bound obtained by Loxton and Smith in [4]. See also [2] and [1] where the proof in [4] is simplified. In fact our argument is similiar to the elementary proof in [1] of the “new version of Hensel’s lemma” found in [2], adapted to root clusters.

- The statement of Theorem 1.1 holds in the setting of any Dedekind domain  $A$  endowed with a valuation arising from a nonzero prime ideal  $\mathfrak{p}$  so that the residue class field  $A/\mathfrak{p}$  is finite. Such a valuation allows us to define  $\theta_j$  and  $\mathcal{I}$  analogously for  $f(x) = a_d \prod (x - \xi_j)^{e_j} \in A[X]$  and if  $N_f$  denotes the number of solutions to the congruence  $f \equiv 0 \pmod{\mathfrak{p}^\alpha}$ , then

$$\|\mathfrak{p}\|^{\alpha - \min_{j \in \mathcal{I}} \theta_j - 1} \leq N_f \leq m \|\mathfrak{p}\|^{\alpha - \min_{j \in \mathcal{I}} \theta_j} \quad (2)$$

when  $\min_{j \in \mathcal{I}} \theta_j \leq \alpha$ ; here  $\|\mathfrak{p}\|$  denotes the number of elements in  $A/\mathfrak{p}$ .

- The arguments below easily generalise to treat polynomials  $f \in \mathbb{Z}_p[X]$  (or  $f \in \bar{A}[X]$ ) with coefficients in the  $p$ -adic integers.

*Examples:* The upper and lower bounds in (1) (or (2)) almost match, up to a factor of  $m$  for the upper bound and  $p^{-1}$  for the lower bound. These bounds are easily computed in practice when all the roots  $\xi_j$  of  $f$  are  $p$ -adic integers (or lie in the completion  $\bar{A}$  with respect to the  $\mathfrak{p}$ -adic valuation on  $A$ ). In this case the set of indices  $\mathcal{I}$  is the set of all  $j$ ,  $1 \leq j \leq m$ . For example if  $f(x) = ax + b$ ,  $a, b \in \mathbb{Z}$  has degree 1, and  $p^s = \gcd(a, p^\alpha)$ , then of course  $f(x) \equiv 0 \pmod{p^\alpha}$  is solvable if and only if  $p^s | b$  in which case there are exactly  $p^s$  solutions. If  $p^t || b$ , then the only (rational) root  $-b/a$  is a  $p$ -adic integer exactly when  $s \leq t$  which is the condition for solvability and in this case  $\theta_1 = \alpha - s$  so that the upper bound in the (1) is  $p^s$ .

Now consider a polynomial  $f(x) = a(x - z_1)^{e_1}(x - z_2)^{e_2}(x - z_3)^{e_3}$  in  $\mathbb{Z}[X]$  of degree  $d = e_1 + e_2 + e_3$  which has three roots  $z_1, z_2, z_3$  in  $\mathbb{Z}_p$ , with the property  $\text{ord}_p(z_1 - z_2) = \text{ord}_p(z_1 - z_3) = s$  but  $t := \text{ord}_p(z_2 - z_3) > s$  and  $ds \leq \alpha - \tau \leq e_1 s + (e_2 + e_3)t$  where  $\tau = \text{ord}_p(a)$ . Then if  $e_2 \leq e_1$ , the root cluster  $\mathcal{C} = \{z_2, z_3\}$  plays an important role and one computes that

$$\min_{1 \leq j \leq 3} \theta_j = \theta_2 = (\alpha - \delta_p(z_2; \mathcal{C})) / (e_2 + e_3) = (\alpha - \tau - e_1 s) / (e_2 + e_3).$$

Therefore Theorem 1.1 shows that in this case

$$p^{[(e_2 + e_3 - 1)\alpha + \tau + e_1 s] / (e_2 + e_3) - 1} \leq N(f; \alpha) \leq 3 p^{[(e_2 + e_3 - 1)\alpha + \tau + e_1 s] / (e_2 + e_3)}.$$

*Acknowledgement:* I wish to thank the analysis group at the University of Wisconsin-Madison for their hospitality while this paper was written and for gently nudging me to think more about clusters as formulated in the papers [5], [6] of Phong, Stein and Sturm.

## 2. STRUCTURE OF SUBLEVEL SETS FOR GENERAL POLYNOMIALS

Here we present a general structural statement about sublevel sets of polynomials which is a slight extension of a result of Phong and Stein [6] and lies at the heart of the proof of our main result Theorem 1.1. Let  $A$  be any commutative ring with identity which carries a nontrivial valuation which we write in multiplicative form  $|\cdot|$  for the elements  $x \in A$ .

**Proposition 2.1.** *Suppose  $A$  is a commutative ring with a nontrivial valuation  $|\cdot|$  and let  $P(x) = a_d \prod (x - \xi_j)^{e_j}$  be a polynomial in  $A[X]$  with distinct roots  $\xi_1, \dots, \xi_m$  lying in some field extension  $K$ . Then*

$$\{x \in A : |P(x)| \leq \delta\} = \bigcup_{j=1}^m \bigcap_{\xi_j \in \mathcal{C}} [B_{r_{\mathcal{C},j}}(\xi_j) \cap A] = \bigcup_{j=1}^m [B_{r_j}(\xi_j) \cap A] \quad (3)$$

where the intersection above are taken over all root clusters  $\mathcal{C}$  containing  $\xi_j$ . Here

$$r_{\mathcal{C},j} = r_{\mathcal{C},j}(\delta) := \left[ \frac{\delta}{|a_d \prod_{\xi_k \notin \mathcal{C}} (\xi_j - \xi_k)^{e_k}|} \right]^{1/S(\mathcal{C})},$$

$r_j = \min_{\mathcal{C} \ni \xi_j} r_{\mathcal{C},j}$  and  $B_r(z) := \{y \in K : |y - z| \leq r\}$  is the ‘ball’ centred at  $z \in K$  with radius  $r$  where the valuation  $|\cdot|$  on  $K$  is any extension of the original valuation on  $A$ .

*Remarks:*

- The proof of (3) is very elementary and is similar to the proof of a new version of Hensel’s lemma found in [1]. In fact the proof below gives the following extension of this new version of Hensel’s lemma; namely in the setting of the introduction, if  $f(x) = a_d(x - \xi_1)^{e_1} \cdots (x - \xi_m)^{e_m} \in \mathbb{Z}[X]$  with  $x \in K$ ,  $f(x) \neq 0$  and  $\text{ord}_p(x - \xi_1) = \max_k \text{ord}_p(x - \xi_k)$ , say, then

$$\max_{\xi_1 \in \mathcal{C}} (\text{ord}_p f(x) - \delta_p(\xi_1; \mathcal{C})) / S(\mathcal{C}) \leq \text{ord}_p(x - \xi_1)$$

where the maximum is taken over all root clusters  $\mathcal{C}$  containing  $\xi_1$ .

- Although Phong, Stein and Sturm in [6] only give an upper bound on the measure of polynomial sublevel sets when  $A = \mathbb{R}$ , their argument gives set inclusions in (3) in the setting of the reals. We remark that there is analogous statement of Proposition 2.1 valid in archimedean settings as well ( $\mathbb{R}$  or  $\mathbb{C}$  for example) but then a few factors of 2 appear in the definition of  $r_{\mathcal{C},j}$ . See [3] where an upper set inclusion was observed in the above abstract setting and used to establish global sublevel set estimates for certain classes of polynomials.

**Proof** This will be done by establishing two set inclusions. Set  $A_j := \{x \in A : |x - \xi_j| = \min_k(|x - \xi_k|)\}$  and note that

$$\{x \in A : |P(x)| \leq \delta\} \subset \bigcup_{j=1}^m \{x \in A_j : |P(x)| \leq \delta\}.$$

Now fix  $j$ ,  $1 \leq j \leq m$ , and observe that when  $x \in A_j$ ,

$$|P(x)| \geq |a_d \prod_{\xi_k \notin \mathcal{C}} (\xi_j - \xi_k)^{e_k}| \cdot \left| \prod_{\xi_k \in \mathcal{C}} (x - \xi_k)^{e_k} \right|$$

for any cluster  $\mathcal{C}$  containing  $\xi_j$  since  $|\xi_j - \xi_k| \leq \max(|\xi_j - x|, |x - \xi_k|) = |x - \xi_k|$  when  $x \in A_j$ . Therefore for  $x \in A_j$ , if also  $|P(x)| \leq \delta$ , then

$$|x - \xi_j|^{S(\mathcal{C})} \leq \left| \prod_{\xi_k \in \mathcal{C}} (x - \xi_k)^{e_k} \right| \leq r_{\mathcal{C},j}^{S(\mathcal{C})}$$

for any cluster  $\mathcal{C}$  containing  $\xi_j$  and this gives

$$\{x \in A_j : |P(x)| \leq \delta\} \subset \bigcap_{\mathcal{C}:\xi_j \in \mathcal{C}} [B_{r_{\mathcal{C},j}}(\xi_j) \cap A],$$

establishing the first set inclusion.

For the second set inclusion, if  $x$  lies in the set on the left in (3), then there is a  $j$ ,  $1 \leq j \leq m$ , so that  $x \in \bigcap_{\xi_j \in \mathcal{C}} B_{r_{\mathcal{C},j}}(\xi_j)$  where the intersection is taken over all root clusters  $\mathcal{C}$  containing  $\xi_j$ . Next we consider a particular cluster containing  $\xi_j$ , depending on  $x$ ; namely

$$\mathcal{C}_x := \{\xi_k : |\xi_j - \xi_k| \leq |x - \xi_j|\}$$

and so in particular  $|x - \xi_j| \leq r_{\mathcal{C}_x,j}$ . Therefore

$$|P(x)| = \left| a_d \prod_{\xi_k \notin \mathcal{C}_x} (\xi_j - \xi_k)^{e_k} \right| \left| \prod_{\xi_k \in \mathcal{C}_x} (x - \xi_k)^{e_k} \right|$$

since  $|x - \xi_k| = |\xi_k - \xi_j + \xi_j - x| = |\xi_k - \xi_j|$  for  $\xi_k \notin \mathcal{C}_x$ . On the other hand, when  $\xi_k \in \mathcal{C}_x$ ,  $|x - \xi_k| \leq \max(|x - \xi_j|, |\xi_j - \xi_k|) = |x - \xi_j|$  and hence

$$|P(x)| \leq \left| a_d \prod_{\xi_k \notin \mathcal{C}_x} (\xi_j - \xi_k)^{e_k} \right| |x - \xi_j|^{S(\mathcal{C}_x)} \leq \delta$$

since, as we observed earlier,  $|x - \xi_j| \leq r_{\mathcal{C}_x,j}$ . This completes the proof of the proposition.  $\blacksquare$

### 3. PROOF OF THE MAIN RESULT

In this section we give the proof of Theorem 1.1 which we will see is valid in somewhat abstract settings. For the moment suppose that  $A$  is a general commutative ring with a valuation  $|\cdot|$  (hence we may apply the basic result Proposition 2.1 in Section 2) so that  $|x| \leq 1$  for all  $x \in A$ ; thus  $A$  is a subring of the ring of integers associated to  $|\cdot|$ . We note that the ball  $I = \{y \in A : |y| \leq \delta\}$ , centred at the origin 0, is an ideal of  $A$  and for any polynomial  $f \in A[X]$ , the elements  $x \in A$  lying in the sublevel set  $\{x \in A : |f(x)| \leq \delta\}$  are simply those elements solving the congruence  $f(x) \equiv 0 \pmod{I}$ . Furthermore if  $\delta \leq 1$  and  $x \in A$  solves  $f(x) \equiv 0 \pmod{I}$  (that

is,  $|f(x)| \leq \delta$ ), then any element  $y$  in the coset  $x + I$  also solves  $f(y) \equiv 0 \pmod{I}$ . Therefore we say that a solution to the polynomial congruence  $f \equiv 0 \pmod{I}$  is an element  $\bar{x} = x + I$  of the factor group  $A/I$  whenever  $x$  (and hence all members of  $x + I$ ) satisfy  $f(x) \equiv 0 \pmod{I}$ . It is convenient to think of an element  $\bar{x} = x + I$  in  $A/I$  as the ball  $B_\delta(x) = \{y \in A : |y - x| \leq \delta\} = x + I$  centred at  $x$  (or for that matter centred at any member of the coset  $x + I$  due to the non-archimedean nature of  $|\cdot|$ ) with radius  $\delta \leq 1$ .

Therefore to count the number of solutions to the congruence  $f \equiv 0 \pmod{I}$ , it suffices to count the number of pairwise disjoint balls  $B_\delta(y)$  which lie in  $\{x \in A : |f(x)| \leq \delta\}$ . Now we apply Proposition 2.1 to conclude that (3) holds for our  $f \in A[X]$ ; namely

$$\{x \in A : |f(x)| \leq \delta\} = \bigcup_{j \in \mathcal{I}} [\mathfrak{B}_{r_j}(z_j) \cap A] \quad (4)$$

where the balls  $\mathfrak{B}_r(z) = \{y \in K : |y - z| \leq r\}$  lie in some extension ring  $K$  where the roots  $\{z_1, \dots, z_m\}$  of  $f(x) = a_d \prod (x - z_j)^{e_j}$  live. In this context the radii  $r_j$  are defined as the minimum of the  $r_{\mathcal{C},j}$  over all root clusters  $\mathcal{C}$  containing  $z_j$  and  $\mathcal{I} := \{1 \leq j \leq m : \mathfrak{B}_{r_j}(z_j) \cap A \neq \emptyset\}$ . To obtain an upper bound of the number of solutions to  $f \equiv 0 \pmod{I}$ , we need to find an upper bound on the number of pairwise disjoint balls  $B_\delta(x)$  in  $A$  which lie in the set on the right hand side above. To do this we make the trivial but important observation that when  $j \in \mathcal{I}$ , there is an element  $w_j \in A$  so that

$$\mathfrak{B}_{r_j}(z_j) \cap A = B_{r_j}(w_j) = \{y \in A : |y - w_j| \leq r_j\},$$

due to the non-archimedean nature of  $|\cdot|$ .

We now split the indices  $j \in \mathcal{I}$  into two classes  $\mathcal{J}_1$  and  $\mathcal{J}_2$  where

$$\mathcal{J}_1 := \{j \in \mathcal{I} : \delta \leq r_j\}$$

and  $\mathcal{J}_2$  is defined as the complement of this set in  $\mathcal{I}$ ; in particular for each  $j \in \mathcal{J}_2$ ,  $r_j < \delta$ .

Accordingly, each solution to the congruence  $f \equiv 0 \pmod{I}$ , that is a ball  $B_\delta(y)$  which lies in  $\{x \in A : |f(x)| \leq \delta\}$ , comes in one of two types: we will say that a solution is of Type I if the corresponding ball lies entirely in one of balls  $B_{r_j}(w_j)$  with  $j \in \mathcal{J}_1$  and a solution is of Type II if it is not of Type I in which case it is a disjoint union of balls arising from some subcollection of  $j \in \mathcal{J}_2$ . Let  $\mathcal{N}_1$  be the number of solutions of Type I and  $\mathcal{N}_2$  be the number of solutions of Type II. Furthermore, for each  $r$  with  $\delta \leq r$ , let  $N_r = N_r(\delta)$  be a uniform upper bound on the number of pairwise disjoint balls  $B_\delta(y)$  in  $A$  which lie in some  $B_r(w)$  (uniform over all centres  $w \in A$ ). Therefore we have

$$\mathcal{N}_1 \leq \sum_{j \in \mathcal{J}_1} N_{r_j} = \sum_{j \in \mathcal{J}_1} N_{r_j}(\delta) \quad (5)$$

and so we will obtain an upper bound on the number of solutions to the congruence  $f \equiv 0 \pmod{I}$  once we can bound  $\mathcal{N}_2$  and determine  $N_r(\delta)$  for any  $\delta \leq r$ .

Before turning to concrete situations let us give a brief general discussion how to obtain lower bounds on the number of pairwise disjoint balls  $B_\delta(y)$  in  $A$  which lie inside

$$\bigcup_{j=1}^m [\mathfrak{B}_{r_j}(z_j) \cap A] = \bigcup_{j \in \mathcal{I}} B_{r_j}(w_j)$$

which in turn gives a lower bound on the number of solutions to the congruence  $f \equiv 0 \pmod{I}$ . Hence, if there is an index  $j \in \mathcal{I}$  so that  $r_j \geq \delta$ , we see that a general lower bound is  $\max_{j \in \mathcal{I}} M_{r_j}$  where  $M_r = M_r(\delta)$  is a uniform lower bound on the number of pairwise disjoint balls  $B_\delta(y)$  in  $A$  which lie in any given  $B_r(w)$  (again uniform with respect to centres  $w \in A$  and here  $M_r$  is only defined when  $\delta \leq r$ ).

We now turn to a concrete situation where bounds on  $N_r(\delta)$  and  $M_r(\delta)$  are easily computed. Let  $A$  be a Dedekind domain and suppose  $\mathfrak{p}$  is a nonzero prime ideal of  $A$  whose residue class field  $A/\mathfrak{p}$  is finite. The prime ideal  $\mathfrak{p}$  gives rise to a non-archimedean valuation  $\text{ord}_{\mathfrak{p}}$  on  $A$  (for  $x \in A$ , we define  $\text{ord}_{\mathfrak{p}}(x)$  to be the non-negative integer  $t$  so that  $\mathfrak{p}^t$  appears as the  $\mathfrak{p}$  factor in the prime ideal decomposition of the principal ideal  $xA$ , generated by  $x$ ), which in multiplicative form we write  $|x| := \|\mathfrak{p}\|^{-\text{ord}_{\mathfrak{p}}(x)}$  for elements  $x \in A$  where  $\|\mathfrak{p}\|$  denotes the number of element in the field  $A/\mathfrak{p}$ . An easy computation shows that when  $\delta = \|\mathfrak{p}\|^{-\alpha}$  for some positive integer  $\alpha$ , we can take  $N_r(\delta) = \|\mathfrak{p}\|^\alpha r$  and  $M_r(\delta) = \|\mathfrak{p}\|^{\alpha-1} r$  whenever  $\delta \leq r$ .

Keeping in the above concrete situation, we are in a position to give upper and lower bounds for the number of solutions to the congruence  $f \equiv 0 \pmod{I}$  where  $f \in A[X]$  is a polynomial  $f(x) = a_d \prod_{j=1}^m (x - \xi_j)^{e_j}$  with distinct roots  $\xi_1, \dots, \xi_m$  lying in some field extension  $K$  and the ideal  $I$  is  $\mathfrak{p}^\alpha$  where  $\alpha$  is a positive integer. Extending the valuation  $\text{ord}_{\mathfrak{p}}$  or  $|\cdot|$  to  $K$  as before allows us to use the same notation  $\delta_{\mathfrak{p}} = \delta_{\mathfrak{p}}(\xi_j; \mathcal{C})$  and  $\theta_j = \theta_j(\alpha)$  in this more general setting as we did when  $A = \mathbb{Z}$ . Furthermore we keep using the notation  $r_{\mathcal{C},j}$  and  $r_j$  with  $\delta = \|\mathfrak{p}\|^{-\alpha}$  used above in the more abstract setting of a general commutative ring  $A$ . We note that in this context,

$$r_{\mathcal{C},j} = \|\mathfrak{p}\|^{-(\alpha - \delta_{\mathfrak{p}}(\mathcal{C}; \xi_j))/S(\mathcal{C})} \quad \text{and} \quad r_j = \|\mathfrak{p}\|^{-\theta_j(\alpha)}.$$

First we write down the lower bound for the number of solutions to  $f \equiv 0 \pmod{\mathfrak{p}^\alpha}$ ; if  $\min_{j \in \mathcal{I}} \theta_j \leq \alpha$ , then we can find a  $j \in \mathcal{I}$  such that  $r_j \geq \delta$  and so from above we have the lower bound

$$\max_{j \in \mathcal{I}} M_{r_j}(\alpha) = \|\mathfrak{p}\|^{\alpha-1} \max_{j \in \mathcal{I}} r_j = \|\mathfrak{p}\|^{\alpha-1 - \min_{j \in \mathcal{I}} \theta_j}$$

which is the lower bound claimed in (2) and also in Theorem 1.1 when  $A = \mathbb{Z}$ .

For the upper bound, recall that we have divided the solutions of  $f \equiv 0 \pmod{\mathfrak{p}^\alpha}$  into two types. A bound for the number  $\mathcal{N}_1$  of Type I solutions is given above as  $\sum_{j \in \mathcal{J}_1} N_{r_j}(\delta)$  and so we have

$$\mathcal{N}_1 \leq \sum_{j \in \mathcal{J}_1} \|\mathfrak{p}\|^\alpha r_j \leq \|\mathfrak{p}\|^\alpha \sum_{j \in \mathcal{J}_1} \|\mathfrak{p}\|^{-\theta_j}. \quad (6)$$

We now provide a bound for  $\mathcal{N}_2$ , the number of solutions to  $f \equiv 0 \pmod{\mathfrak{p}^\alpha}$  of Type II. Recall that a solution  $B_\delta(x) = x + I \in A/I$  (here  $\delta = \|\mathfrak{p}\|^{-\alpha}$  and  $I = \mathfrak{p}^\alpha$ ) of Type II is a union of disjoint balls  $B_{r_j}(w_j)$  for a certain collection of  $j \in \mathcal{J}_{2,x} \subset \mathcal{J}_2$  and

centres  $w_j \in A$ . To help us count these solutions we pass to the completion  $\bar{A}$  of  $A$  with respect to the valuation  $\text{ord}_{\mathfrak{p}}$ , and denoting by  $\bar{B}_r(y) = \{z \in \bar{A} : |z - y| \leq r\}$  the ‘completed’ ball in  $\bar{A}$  of  $B_r(y) = \{x \in A : |x - y| \leq r\}$  in  $A$ , we still have the decomposition

$$\bar{B}_\delta(x) = \bigcup_{j \in \mathcal{J}_{2,x}} \bar{B}_{r_j}(w_j)$$

for each solution of Type II. Let  $x_1, \dots, x_{\mathcal{N}_2}$  enumerate the solutions of Type II. Since  $\bar{A}$  is the compact ring of integers of a local field by our finite hypothesis on  $A/\mathfrak{p}$ , we have at our disposal a Haar measure  $d\mu$  on  $\bar{A}$  which we normalise so that  $\mu(\bar{A}) = 1$ . From this we see that  $\mu(\bar{B}_r(w)) = \|\mathfrak{p}\|^{-s}$  where  $s$  is the unique integer satisfying  $\|\mathfrak{p}\|^{-s} \leq r < \|\mathfrak{p}\|^{-s+1}$ .

Therefore

$$\mathcal{N}_2 = \|\mathfrak{p}\|^\alpha \sum_{r=1}^{\mathcal{N}_2} \mu(\bar{B}_\delta(x_r)) \leq \|\mathfrak{p}\|^\alpha \sum_{j \in \mathcal{J}_2} \mu(\bar{B}_{r_j}(w_j)) \leq \|\mathfrak{p}\|^\alpha \sum_{j \in \mathcal{J}_2} \|\mathfrak{p}\|^{-\theta_j}$$

which together with (6) gives us the desired upper bound

$$\mathcal{N}_1 + \mathcal{N}_2 \leq \sum_{j \in \mathcal{I}} \|\mathfrak{p}\|^{\alpha - \theta_j} \leq m \|\mathfrak{p}\|^{\alpha - \min_{j \in \mathcal{I}} \theta_j},$$

completing the proof of (2) and Theorem 1.1 when we restrict to  $A = \mathbb{Z}$ .

#### REFERENCES

- [1] J.H.H. Chalk and R. A. Smith, *Sándor’s theorem on polynomial congruences and Hensel’s lemma*, C.R. Math. Rep. Acad. Sci. Canada **4** (1982), no. 1, 49-54.
- [2] J.H.H Chalk, *A p-adic approach to solutions of a polynomial congruence modulo  $p^\alpha$* , *Mathematika* **37** (1990), no. 2, 209-216.
- [3] M.W. Kowalski and J. Wright, *An elementary inequality with some applications*, preprint.
- [4] J.H. Loxton and R. A. Smith, *On Hua’s estimate for exponential sums*, J. London Math. Soc. **26** (1982), 15-20.
- [5] D.H. Phong and E.M. Stein, *Oscillatory integrals with polynomial phases*, *Inventiones Math.* **110** (1992), 39-62.
- [6] 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.

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