Indian J. Pure Appl. Math., **41**(1): 15-23, February 2010

SMALL SOLUTIONS OF POLYNOMIAL CONGRUENCES

M. Ram Murty[1]

Department of Mathematics, Queen's University, Kingston, Ontario, K7L 3N6, Canada
e-mail: murty@mast.queensu.ca

Abstract Let p be prime and $q|p-1$. Suppose $x^q \equiv a(\mathrm{mod}\ p)$ has a solution. We estimate the size of the smallest solution x_0 with $0 < x_0 < p$. We prove that $|x_0| \ll p^{3/2}q^{-1}\log p$. By applying the Burgess character sum estimates, and estimates of certain exponential sums due to Bourgain, Glibichuk and Konyagin, we derive refinements of our result.

Key words Polynomial congruences, character sums, applications of exponential sums.

1. Introduction

Suppose that we are given a polynomial $f(x) \in \mathbb{Z}[x]$ and p is a prime for which the congruence

$$f(x) \equiv 0(\mathrm{mod}\ p)$$

has a solution. We would like to estimate the smallest solution x_0 of this congruence which satisfies $0 \leq x_0 < p$. Apart from its intrinsic interest, such questions have arisen in the context of cryptography (see for example, [5]). It is somewhat surprising that the trivial bound $|x_0| < p$ cannot be improved upon in the generic case. For example, if $D > 1$ is squarefree, let us consider $f(x) = x^2 - D$. Suppose we are able to prove a bound of the form $|x_0| < p^{1-\delta}$ for some $\delta > 0$. Then, every prime $p \leq T$ for which

$$x^2 \equiv D(\mathrm{mod}\ p),$$

has a solution, divides

$$V := \prod_{n \leq T^{1-\delta}} (n^2 - D)$$

[1]Research partially supported by an NSERC grant.

and the number of prime divisors of V is

$$\ll \log V = \sum_{n \leq T^{1-\delta}} \log |n^2 - D| \ll T^{1-\delta} \log T.$$

But the set of primes $p \leq T$ for which $x^2 \equiv D (\mathrm{mod}\ p)$ has a solution is precisely the set of primes $p \leq T$ which split completely in $\mathbb{Q}(\sqrt{D})$ and the prime divisors of D. By the prime number theorem for quadratic fields, this number is

$$\frac{\pi(T)}{2} + o(T/\log T),$$

where $\pi(T)$ is the number of primes $\leq T$. Since $\pi(T) \sim T/\log T$, we derive a contradiction. This shows that there are infinitely many primes p for which the smallest solution x_0 of the congruence $x^2 \equiv D (\mathrm{mod}\ p)$ satisfies $|x_0| > p^{1-\delta}$ for any fixed $\delta > 0$. In fact, our argument shows that $p^{1-\delta}$ can be replaced by $p/\log^3 p$.

One can extend this to any irreducible polynomial $f(x) \in \mathbb{Z}[x]$. Indeed, suppose that for every prime p for which $f(x) \equiv 0 (\mathrm{mod}\ p)$ has a solution, there is a solution x_0 with $|x_0| < p/\log^3 p$. Then, the number of primes $p \leq T$ for which $f(x) \equiv 0 (\mathrm{mod}\ p)$ has a solution is

$$\ll d(\log H(f)) \frac{T}{\log^2 T},$$

where d is the degree of f and $H(f)$ is the largest absolute value of the coefficients of f. One can show, by an application of the Chebotarev density theorem (see [9] for the statement of this theorem), that the number of primes $p \leq T$ for which $f(x) \equiv 0 (\mathrm{mod}\ p)$ has a solution is

$$\sim \delta_f \pi(T) + o(T/\log T), \tag{1}$$

for some $\delta_f > 0$. For T sufficiently large, we derive a contradiction. This proves that there are infinitely many primes p for which the smallest solution x_0 of

$$f(x) \equiv 0 (\mathrm{mod}\ p),$$

satisfies $|x_0| > p/\log^3 p$.

A closer examination of the above argument shows that we have fixed the degree of f and are varying the primes. In fact, the generalized Riemann hypothesis (see [9]) allows us to replace (1) by

$$\delta_f \pi(T) + O(T^{1/2} \log D_f T),$$

where D_f is the absolute value of the discriminant of f. In particular, the argument of the previous paragraph will give us the desired contradiction provided that

$$\log p \gg d(\log H(f))/\delta_f.$$

That is, p must be sufficiently larger than a certain function of the degree of f and $H(f)$. If the splitting field of f has degree d, then $\delta_f = 1/d$ and in such a case, we require that $p \geq \exp(d^2)$ to deduce a contradiction.

In other words, if the degree of f is too small compared with p, there will be primes p for which our congruence does not have small solutions. It therefore seems reasonable to reformulate our question as follows:

Question. Let $\delta > 0$ be fixed. If $\deg f \geq p^\delta$ and

$$f(x) \equiv 0 (\mathrm{mod}\, p)$$

has a solution, is there a solution x_0 with $|x_0| < p^{1-\epsilon}$ for some $\epsilon = \epsilon(\delta) > 0$?

Our goal in this paper is to show that for certain classes of polynomials, the answer is "yes." More precisely, we will consider polynomials of the form $x^q - a$ with q prime. The distribution of solutions of this particular congruence have been studied by several authors (see for example, Chapter 13 of [8]). Here we are concerned with estimating the size of the smallest solution. We will attack this question using two different approaches. The first method applies classical theory of Dirichlet L-functions and the second method applies recent estimates for exponential sums obtained by Bourgain, Glibichuk and Konyagin [2].

2. The Classical Method

We will assume q to be prime, though this is not a serious restriction. In studying the congruence $x^q \equiv a (\mathrm{mod}\, p)$, we may suppose that $q|p-1$, for otherwise, the map $x \mapsto x^q$ is an automorphism of $(\mathbb{Z}/p\mathbb{Z})^*$. Since we are assuming the congruence has a solution, we have by Euler's criterion,

$$a^{\frac{p-1}{q}} \equiv 1 (\mathrm{mod}\, p).$$

Let $r = (p-1)/q$. All solutions of $x^q \equiv a (\mathrm{mod}\, p)$ lie in a coset of the subgroup H of qth roots of $1 \pmod p$. We now consider the cosets of H and seek to estimate the smallest element in each coset. This is easily done by considering

$$S := \sum_{n \leq T} \frac{1}{p-1} \sum_{\chi} \overline{\chi}(a)\chi(n^q).$$

The inner sum is 1 precisely when $n^q \equiv a (\mathrm{mod}\, p)$ and 0 otherwise. The sum is easily estimated using the classical Pólya-Vinogradov inequality. This states that if χ is a non-trivial Dirichlet character (mod p), then

$$\sum_{n \leq x} \chi(n) = O(\sqrt{p} \log p).$$

For a proof, we refer the reader to [6]. Inserting this into our sum above, we obtain

$$S = \frac{qT}{p-1} + O(p^{1/2} \log p),$$

where the implied constant in the O-estimate is absolute. From this, we see that the main term is greater than the error term provided

$$T \gg p^{3/2}(\log p)/p.$$

This proves:

Theorem 1. *Let p be prime and q a prime divisor of $p-1$. Suppose that $a^{(p-1)/q} \equiv 1 (\mathrm{mod}\ p)$. Then, the congruence*

$$x^q \equiv a (\mathrm{mod}\ p),$$

has a solution x_0 with $|x_0| \ll p^{3/2} q^{-1} \log p$.

We remark that using a refined character estimate due to Hua, one can eliminate the $\log p$ factor. We also note that q need not be prime. The estimate is non-trivial only if $q > p^{1/2}$. Hua's inequality (see Lemma 2 of [13]) says that if χ is a non-trivial Dirichlet character mod p, then

$$\left| \sum_{|n| \leq x} \left(1 - \frac{|n|}{x}\right) \chi(n) \right| \ll p^{1/2}.$$

Instead of considering the sum S above, we can consider the modified sum:

$$S' := \sum_{|n| \leq T} \frac{1}{p-1} \sum_{\chi} \overline{\chi}(a) \chi(n^q) \left(1 - \frac{|n|}{T}\right).$$

An easy calculation shows that

$$S' = \frac{qT}{2(p-1)} + O(p^{1/2}).$$

From this, we deduce the following refinement:

Theorem 2. *Let p be prime and q a prime divisor of $p-1$. Suppose that the congruence*

$$x^q \equiv a (\mathrm{mod}\ p)$$

has a solution. Then, it has a solution x_0 with $|x_0| \ll p^{3/2}/q$.

The Lindelöf hypothesis for Dirichlet L-functions (which is a consequence of the generalized Riemann hypothesis for Dirichlet L-functions) predicts that

$$\sum_{n \leq x} \chi(n) = O(x^{1/2} p^{\epsilon}),$$

for any $\epsilon > 0$. This is easily shown using methods of contour integration. (The reader may consult (12.54) of [7] for a reference.)

It is clear that if we insert this estimate in the character sums occurring in S, we obtain

$$S = \frac{qT}{p-1} + O(T^{1/2} p^{\epsilon}).$$

This gives:

Theorem 3. *Let p be prime and q a prime divisor of $p-1$ such that $a^{(p-1)/q} \equiv 1 (\mathrm{mod}\ p)$. On the Lindelöf hypothesis, the congruence $x^q \equiv a (\mathrm{mod}\ p)$ has a solution x_0 with $|x_0| \ll (p/q)^2 p^\epsilon$. The p^ϵ factor in the estimate can be replaced by $\log p$ if we are willing to assume the generalized Riemann hypothesis.*

Only the last assertion needs some justification. For in this case, we have (see [6])

$$\sum_{n \leq x} \chi(n)\Lambda(n) \ll x^{1/2} (\log p) \log x,$$

and a routine partial summation estimate allows us to deduce the result claimed.

What is essential to observe is that in all these cases, the estimate is non-trivial only if $q > p^{1/2+\epsilon}$.

In this context, we can also invoke the celebrated estimates of Burgess. The results we obtain in this setting are better than what we have obtained above for certain ranges of values of q.

In 1963, Burgess [3] proved the following:

Lemma 4. *If χ is a Dirichlet character mod p, and $\epsilon > 0$, then*

$$\sum_{n \leq T} \chi(n) \ll_{\epsilon,t} T^{1-1/t} p^{(t+1)/4t^2+\epsilon},$$

for any natural number $t \geq 1$.

A straightforward application of the Burgess estimate leads to:

Theorem 5. *If the congruence $x^q \equiv a (\mathrm{mod}\ p)$ has a solution, then it has a solution x_0 satisfying $|x_0| \ll (p/q)^t p^{1/4+1/4t+\epsilon}$ for any $\epsilon > 0$ and any natural number t. For $t = 1$ this is essentially the result of the previous two theorems. For $t = 2$, the result is superior to the bound given in the previous two theorems, if $q > p^{7/8+\epsilon}$.*

The first assertion is proved as before. For the last assertion, it is easily checked that in the range $q > p^{7/8+\epsilon}$, we have

$$(p/q)^2 p^{3/8+\epsilon} < p^{3/2}/q.$$

By the same logic, one can see that the above estimate is better than the one obtained in the earlier theorems for $t = 3$ in the range $q > p^{11/12+\epsilon}$. In fact, in the general setting, the result above for a given value of $t \geq 2$ is superior to the earlier bounds provided

$$q > p^{1-\frac{3}{2(t-1)}} p^{\frac{t+1}{4t(t-1)}},$$

from which we see that the result for t arbitrarily large is better provided that $q > p^{1-\epsilon}$.

3. The Method of Equidistribution

In this section, we will apply the Erdös-Turán inequality to study the distribution of the roots of the congruence $x^q \equiv a (\mathrm{mod}\ p)$. Here is the basic tool. Suppose that

we are given a sequence of real numbers x_n with $0 \leq x_n < 1$. For $0 \leq \alpha < 1$, let $N(V, \alpha)$ be the number of $n \leq V$ such that $0 \leq x_n \leq \alpha$. Then:

Lemma 6.

$$\left| N(V,\alpha) - V\alpha \right| \leq \frac{V}{M+1} + 3\sum_{m=1}^{M} \frac{1}{m} \left| \sum_{n \leq V} e^{2\pi i m x_n} \right|.$$

For a proof of the lemma, we refer the reader to p. 8 of [10]. Here is how we will apply this result in our investigation. We list the roots of $x^q \equiv a (\mathrm{mod}\ p)$ as $r_1 < r_2 < \cdots < r_q < p$ and consider the equidistribution of the sequence r_i/p. We observe that the set of solutions of the congruence forms a coset of the multiplicative group H of q-th roots of 1 (mod p). To apply the Erdös-Turán inequality, we need the following theorem due to Bourgain, Glibichuk and Konyagin [2]. An explicit determination of $\epsilon(\delta)$ is derived in [1].

Theorem 7. *Fix $\delta > 0$ and a prime p. For any subgroup H of size $\geq p^\delta$, there is $\epsilon(\delta) > 0$ such that*

$$\Big| \sum_{x \in H} e^{2\pi i a x/p} \Big| \ll |H| p^{-\epsilon(\delta)}.$$

We insert this estimate into the Erdös-Turán inequality to get:

Theorem 8. *Let $\delta > 0$ and p be prime. Suppose that $q | p-1$ and $q > p^\delta$. There is a $\epsilon(\delta) > 0$ such that the number of roots r_i of $x^q \equiv a (\mathrm{mod}\ p)$ with $0 < r_i < \alpha p$ is $q\alpha + O(qp^{-\epsilon(\delta)})$. In particular, there is a solution x_0 of the congruence $x^q \equiv a (\mathrm{mod}\ p)$ with $|x_0| < p^{1-\epsilon(\delta)}$.*

In certain ranges of q we can make the above estimates explicit using some work of [8] (see page 23 of [8]). Especially, if H has order q with $p^{1/3} < q < p^{1/2}$, then we have

$$\Big| \sum_{x \in H} e^{2\pi i a x/p} \Big| \ll q^{5/8} p^{1/8}.$$

This estimate allows us to give a precise value of ϵ in the previous theorem. In particular, it allows us to deduce that there is a solution x_0 satisfying $|x_0| < p^{9/8}/q^{3/8}$, provided $p^{1/3} < q < p^{1/2}$.

4. An Average Result

By taking a different perspective and exploiting Theorem 5.5 of [8], we can prove that the upper bound implied by the Lindelöf hypothesis holds "on average" in certain ranges. In fact, one can improve the results of the previous section "for almost all primes" p. More precisely, we will show:

Theorem 9. *The number of primes p with $p \equiv 1 (\mathrm{mod}\ q)$ for which $x^q \equiv a (\mathrm{mod}\ p)$ has no solution x_0 with $|x_0| \ll p^{9/8} q^{-1/2} \log p$ is $O(q^2/\log q)$.*

Our basic tool is Theorem 5.5 of [8] which we record below:

Lemma 10. *For each integer t and prime $p \equiv 1 (\mathrm{mod}\ q)$, we fix some element $g_{t,p}$ of multiplicative order t modulo p. Then, for any fixed integer $k \geq 2$, and arbitrary*

$U > 1$, the bound

$$\max_{(a,p)=1} \Big| \sum_{j=0}^{t-1} e^{2\pi i a g_{t,p}^j/p} \Big| \ll t p^{1/2k^2} (t^{-1/k} + U^{-1/k^2}),$$

holds for all primes $p \equiv 1 (\mathrm{mod}\ q)$ with at most $U/\log U$ exceptions.

Here is the proof of our theorem. Fix a prime q. For each prime p with $p \equiv 1 (\mathrm{mod}\ q)$ and $Q < p < 2Q$, we let $t = (p-1)/q$ and $g_{t,p}$ an element of order t mod p. The solutions of the equation $x^q \equiv a (\mathrm{mod}\ p)$ comprise a coset of the subgroup generated by $g_{t,p}$. By the Erdös-Turán inequality, and an application of the above lemma with $k = 2$ and $U = q^2$, we deduce, as before, that there is a solution x_0 with $|x_0| \ll p^{9/8} q^{-1/2} \log p$ with at most $q^2/\log q$ exceptional primes p. This completes the proof.

Let us observe that the Lindelöf hypothesis gives an estimate of $\ll (p/q)^2 p^\epsilon$. It is easy to see that the estimate obtained in the above theorem is better than the estimate implied by the Lindelöf hypothesis in the range $p^{1/2} < q < p^{7/12}$.

5. Concluding Remarks

It seems reasonable to conjecture that

$$\Big| \sum_{x \in H} e^{2\pi i a x/p} \Big| \ll |H|^{1/2} p^\epsilon.$$

If we admit this conjecture, then the above analysis shows that our congruence has a solution x_0 with

$$|x_0| \ll p^{1+\epsilon}/q^{1/2},$$

for any $\epsilon > 0$.

These results also have applications to several questions in analytic number theory that are rooted in estimates for non-residues (mod p). A celebrated question discussed in [12] asks the following. Let E be a subgroup of the group coprime residue classes (mod n). Suppose that E has index ν. Let

$$1 = g_0(n; E) < g_1(n; E) < \cdots < g_{\nu-1}(N; E)$$

be the smallest positive representatives of the ν cosets of E in $(\mathbb{Z}/n\mathbb{Z})^*$. The general question is to find good upper bounds for $g_i(n; E)$. In the particular case that E is the subgroup of the k-th powers, this question has received considerable attention. In [12], Norton shows that if for any $\epsilon > 0$, $\nu = O(n^\epsilon)$, then

$$g_{\nu-1}(n; E) \ll n^{1/4+\epsilon},$$

where the implied constant may depend on ϵ. In our context, the discussion from the previous sections shows that the solutions of the congruence $x^q \equiv a (\mathrm{mod}\ p)$ comprise a coset of the k-th power residues, where $k = (p-1)/q$. This subgroup has index k. Thus, Norton's result says that if $q > p^{1-\epsilon}$ then the smallest solution

of $x^q \equiv a (\mathrm{mod}\ p)$ (if it exists) satisfies $|x_0| < p^{1/4+\epsilon}$. This is indeed a superior result in the range that $q > p^{1-\epsilon}$.

However, when q is much smaller, the techniques of [12] do not extend and one must modify the technique. This is precisely what is done above. It allows us to deduce that a "small solution" exists even in the wider range that $q > p^{\epsilon}$.

We make final concluding remark that may be of use in computational number theory. Using a simple pigeonhole argument, we will show:

Theorem 11. *Let $f(x, y)$ be a homogeneous polynomial of degree q which is irreducible in $\mathbb{Z}[x, y]$. Suppose that $f(x, y) \equiv 0 (\mathrm{mod}\ p)$ has a non-trivial solution. Then, we can find a non-zero solution (x_0, y_0) with $|x_0|, |y_0| < p^{1/2}$.*

To see this, let $F(x) = f(x, 1)$ and $c \neq 0$ such that $F(c) \equiv 0 (\mathrm{mod}\ p)$. Consider the $[\sqrt{p}]+1$ numbers cu with $u = 0, 1, ..., [\sqrt{p}]$. If we divide the interval $[1, p]$ into subintervals of length $[\sqrt{p}]$, we see by the pigeonhole principle that there are distinct values u_1, u_2 such that the reduced residue classes $(\mathrm{mod}\ p)$ of cu_1 and cu_2 are in the same subinterval. Writing v_1, v_2 for these two reduced residue classes, we find $|v_1 - v_2| < \sqrt{p}$ and $|u_1 - u_2| < \sqrt{p}$. But,

$$f(v_1 - v_2, u_1 - u_2) = f(cu_1 - cu_2, u_1 - u_2) = (u_1 - u_2)^q f(c, 1) \equiv 0 (\mathrm{mod}\ p).$$

Setting $x_0 = v_1 - v_2$ and $y_0 = u_1 - u_2$ gives the desired solution.

Acknowledgement

I would like to thank Stephan Baier, Adam Felix, Sanoli Gun, Kumar Murty, Purusottam Rath and Igor Shparlinski for their comments on an earlier version of this paper. I also thank the referee for helpful remarks.

References

1. J. Bourgain and M. Z. Garaev, On a variant of sum-product estimates and explicit exponential sum bounds in prime fields, *Math. Proc. Cambridge Phil. Soc.*, **146**(1) (2009), 1-21.

2. J. Bourgain, A. A. Glibichuk and S. Konyagin, Estimates for the number of sums and products and for exponential sums in fields of prime order, *J. London Math. Soc.*, **73** (2006), 380-398.

3. D. A. Burgess, On character sums and L-series, *Proc. London Math. Soc.*, **13**(3) (1963), 524-536.

4. A. Cojocaru and M. Ram Murty, *An Introduction to Sieve Methods and their Applications*, London Mathematical Society Student Texts, **66**, Cambridge University Press, 2005.

5. D. Coppersmith, Finding small solutions to small degree polynomials, in *Cryptography and Lattices* (Providence, Rhode Island, 2001), pp. 20-31, *Lecture Notes in Comput. Sci.*, **2146**, Springer, Berlin, 2001.

6. H. Davenport, *Multiplicative Number Theory*, Third edition, Springer, New York, 2000.

7. H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc. Colloquium Publications, **53**, American Mathematical Society, Providence, Rhode Island, 2004.

8. S. Konyagin and I. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Tracts in Mathematics, **136**, Cambridge University Press, 1999.

9. J. Lagarias and A. Odlyzko, *Effective versions of the Chebotarev density theorem, in Algebraic Number Fields*, edited by A. Fröhlich, Academic Press, 1977.

10. H. Montgomery, Ten lectures on the interface between analytic number theory and harmonic analysis, *Conf. Board Math. Sci*., **84**, *American Mathematical Society*, 1994.

11. M. Ram Murty and J. Esmonde, *Problems in Algebraic Number Theory*, 2nd Edition, Springer, 2005.

12. K. Norton, A character-sum estimate and applications, *Acta Arithmetica*, **85**(1) (1998), 51-78.

13. R. Vaughan, Small values of Dirichlet L-functions at 1, in *Analytic Number Theory*, Proceedings of a conference in honor of Heini Halberstam, Volume 2, edited by B. Berndt, H. Diamond and A. Hildebrand, *Progress in Mathematics*, **139**, pp. 755-766, Birkhäuser, 1996.