ACTA ARITHMETICA
144.2 (2010)

On solutions of polynomial congruences

by

SANOLI GUN (Chennai)

1. Introduction. An interesting problem in number theory is to find solutions of polynomial congruences. In a recent work [9], Ram Murty considered the polynomial congruence $x^q \equiv a \pmod{p}$, where p is a prime, q is a divisor of $p-1$ and $a^{(p-1)/q} \equiv 1 \pmod{p}$. He showed that the smallest solution x_0 of the congruence is $\ll p^{3/2}(\log p)/q$. In this paper, we consider consecutive solutions of that congruence when $a = 1$. We show that for a natural number M, the above polynomial congruence has M consecutive solutions for sufficiently large primes p. More precisely, we prove

THEOREM 1.1. *Let p be an odd prime and* M *be a natural number such that $p > 2^{4\mathrm{M}}\mathrm{M}^4$. Further, let q be a prime divisor of $p-1$ with $q > (p-1)^{1-1/4\mathrm{M}}$. Then the congruence*

$$x^q \equiv 1 \pmod{p} \tag{1}$$

has M *consecutive solutions.*

We also consider two-fold generalizations of the question investigated by Ram Murty. In one direction, we study polynomial congruences of the type

$$x^q \equiv a \pmod{d},$$

where d is not necessarily prime, and in another direction, we consider congruences of the form

$$f(x)^q \equiv a \pmod{p}, \qquad (a,p) = 1,$$

where $f(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$. In particular, we prove the following theorems:

THEOREM 1.2. *Let q, d be natural numbers such that $q \mid \phi(d)$. Also let $n(q)$ be the number of elements in $(\mathbb{Z}/d\mathbb{Z})^*$ whose order divides q. Suppose that the polynomial congruence*

$$x^q \equiv a \pmod{d} \tag{2}$$

2010 *Mathematics Subject Classification*: 11T06, 11L40, 11T24.
Key words and phrases: polynomial congruences, character sums.

 © Instytut Matematyczny PAN, 2010

has a solution. Then the smallest solution x_0 satisfies

$$|x_0| \ll \frac{d^{1/2}\phi(d)\log d}{n(q)}.$$

Note that Theorem 1.2 is non-trivial for $n(q) \gg d^{1/2+\varepsilon}$. As an immediate consequence, we have

COROLLARY 1.3. *Let p be an odd prime, $d = p^n, 2p^n$ and $q \mid \phi(d)$. Suppose that the polynomial congruence*

$$x^q \equiv a \pmod{d} \tag{3}$$

has a solution. Then the smallest solution x_0 satisfies

$$|x_0| \ll \frac{p^{3n/2} n \log p}{q}.$$

REMARK 1.1. The case $n = 1$ in the above corollary is a theorem of Ram Murty (see [9]).

THEOREM 1.4. *Let p, q be primes such that $q \,\|\, (p-1)$. Also let $f(x)$ be a polynomial over $\mathbb{Z}/p\mathbb{Z}$ which has m distinct roots and $(\ell, \deg f) = 1$ for any $\ell \mid (p-1)/q$. Suppose that the polynomial congruence*

$$f(x)^q \equiv a \pmod{p}, \qquad (a,p) = 1, \tag{4}$$

has a solution. Then the smallest solution x_0 satisfies

$$|x_0| \ll \frac{m p^{3/2} \log p}{q}.$$

REMARK 1.2. Putting $f(x) = x$ in Theorem 1.4, we again recover the theorem of Ram Murty (see [9]). We also refer to a related article due to Hudson [6].

Next we study the distribution of the roots (if they exist) of the congruence $x^q \equiv a \pmod{d}$ with $(a,d) = 1$. We list the $n(q)$ roots as $r_1 < \cdots < r_{n(q)} < d$. In this context, we have the following theorem:

THEOREM 1.5. *Fix $\alpha \in (0,1)$, $\delta > 0$ and a natural number d. Suppose that $q \mid \phi(d)$ and $n(q) > d^\delta$. Then there exists an $\varepsilon(\delta) > 0$ such that*

$$\#\{r_i \mid r_i^q \equiv a \pmod{d},\ 0 < r_i < \alpha d,\ 1 \le i \le n(q)\} = n(q)\alpha + O(n(q) d^{-\varepsilon(\delta)}).$$

In particular, if there is a solution of $x^q \equiv a \pmod{d}$, then the smallest solution x_0 is $\ll d^{1-\varepsilon(\delta)}$.

As an immediate corollary, we have

COROLLARY 1.6. *Fix $\alpha \in (0,1)$, $\delta > 0$ and $d = p^n, 2p^n$ with p odd prime. Suppose that $q \mid \phi(d)$ and $q > d^\delta$. Then there is $\varepsilon(\delta) > 0$ such that*

$$\#\{r_i \mid r_i^q \equiv a \pmod{d},\ 0 < r_i < \alpha d,\ 1 \le i \le q\} = q\alpha + O(q d^{-\varepsilon(\delta)}).$$

2. Preliminaries. Throughout the paper p is prime, $\mathrm{M}, \mathrm{V}, \ell, q, d$ are natural numbers, χ_0 is the principal character modulo p or d depending on the context. First we shall need the following estimate due to Weil [11].

THEOREM 2.1 (Weil). *For an integer ℓ satisfying $2 \le \ell < p$ and for any non-principal characters $\chi_1, \ldots, \chi_\ell$ and distinct $a_1, \ldots, a_\ell \in \mathbb{Z}/p\mathbb{Z}$, we have*

$$\Big|\sum_{n=1}^{p} \chi_1(n+a_1)\cdots\chi_\ell(n+a_\ell)\Big| \le (\ell-1)\sqrt{p}.$$

For $\ell = 2$, Davenport [4] proved the above bound. Note that when $\ell = 1$, the above sum is 0. Using this, we prove the following lemma.

LEMMA 2.2. *Let $N(p,\mathrm{M})$ denote the number of* M *consecutive solutions of*

$$x^q \equiv 1 \pmod{p}.$$

Then

$$\left|N(p,\mathrm{M}) - p\left(\frac{q}{p-1}\right)^{\mathrm{M}}\right| \le 2^{\mathrm{M}}\mathrm{M}\sqrt{p}.$$

Proof. Write

$$N(p,\mathrm{M}) = \sum_{n=1}^{p}\prod_{j=0}^{\mathrm{M}-1}\left(\frac{1}{p-1}\sum_{\chi}\bar{\chi}(1)\chi((n+j)^q)\right),$$

where the inner sum is over all characters modulo p. Dividing the sum into two parts, with $\chi^q = \chi_0$ and $\chi^q \ne \chi_0$, we have

$$N(p,\mathrm{M}) = (p-1)^{-\mathrm{M}}\sum_{n=1}^{p}\prod_{j=0}^{\mathrm{M}-1}\Big(q + \sum_{\substack{\chi\\ \chi^q\ne\chi_0}}\chi((n+j)^q)\Big) = p\left(\frac{q}{p-1}\right)^{\mathrm{M}} + A,$$

where

$$A = \frac{1}{(p-1)^{\mathrm{M}}}\sum_{\ell=1}^{\mathrm{M}}\sum_{n=1}^{p} q^{\mathrm{M}-\ell}\sum_{\substack{(j_1,\ldots,j_\ell)\\ 0\le j_1<\cdots<j_\ell\le \mathrm{M}-1}}\ \sum_{\substack{(\chi_{m_1},\ldots,\chi_{m_\ell})\\ \chi_{m_i}^q\ne\chi_0}}\prod_{i=1}^{\ell}\chi_{m_i}^q(n+j_i)$$

$$= \sum_{\ell=1}^{\mathrm{M}}\left(\frac{q}{p-1}\right)^{\mathrm{M}-\ell}\sum_{\substack{(j_1,\ldots,j_\ell)\\ 0\le j_1<\cdots<j_\ell\le \mathrm{M}-1}}\frac{1}{(p-1)^\ell}\sum_{\substack{(\chi_{m_1},\ldots,\chi_{m_\ell})\\ \chi_{m_i}^q\ne\chi_0}}\ \sum_{n=1}^{p}\prod_{i=1}^{\ell}\chi_{m_i}^q(n+j_i).$$

Hence by using the estimate of Weil (Theorem 2.1), one has

$$|A| \le \mathrm{M}\sqrt{p}\sum_{\ell=1}^{\mathrm{M}}\binom{\mathrm{M}}{\ell}\left(\frac{q}{p-1}\right)^{\mathrm{M}-\ell} \le 2^{\mathrm{M}}\mathrm{M}\sqrt{p}. \ \blacksquare$$

We refer to [5] where the estimate of Weil has been exploited in another context. We shall need the following generalization of the Pólya–Vinogradov theorem for proving Theorems 1.2 and 1.4.

Lemma 2.3. *If χ ($\neq \chi_0$) is an ℓth order character to the prime modulus p and if $f(x)$ is a polynomial over $\mathbb{Z}/p\mathbb{Z}$ which has m distinct roots and $(\ell, \deg f) = 1$, then*

$$\sum_{n\le T} \chi(f(n)) \ll m\sqrt{p}\log p \qquad \text{for } 1 \le T \le p.$$

To prove Lemma 2.3, we need the following consequence of the works of Weil [12, 13] (see also [2] and page 45 of [10]).

Theorem 2.4. *Let p be prime and χ ($\neq \chi_0$) be a multiplicative character of order ℓ with $\ell \mid (p-1)$. Suppose that $f(x)$ is a polynomial over $\mathbb{Z}/p\mathbb{Z}$ which has m distinct roots and $(\ell, \deg f) = 1$. Then*

$$\Big|\sum_{n=1}^{p} \chi(f(n)) e(an/p)\Big| \le m\sqrt{p},$$

where $e(x) = e^{2\pi i x}$.

Proof of Lemma 2.3. Write

$$S(f,a) = \sum_{n=1}^{p} \chi(f(n)) e(an/p).$$

Now

$$\sum_{n\le T} \chi(f(n)) = \sum_{n=1}^{p} \chi(f(n)) \sum_{b\le T} \bigg(\frac{1}{p}\sum_{a=1}^{p} e(a(n-b)/p)\bigg) \tag{5}$$

since

$$\frac{1}{p}\sum_{a=1}^{p} e(am/p) = \begin{cases} 1 & \text{if } m \equiv 0 \pmod p, \\ 0 & \text{otherwise.} \end{cases}$$

By interchanging the summations in (5), we have

$$\begin{aligned}\sum_{n\le T} \chi(f(n)) &= \frac{1}{p}\sum_{a=1}^{p}\sum_{n=1}^{p} \chi(f(n)) e(an/p) \sum_{b\le T} e(-ab/p) \\ &= \frac{1}{p}\sum_{a=1}^{p} S(f,a) \sum_{b\le T} e(-ab/p) \ll m\sqrt{p}\sum_{a=1}^{p}\frac{1}{a},\end{aligned}$$

by using Theorem 2.4 and the fact that

$$\Big|\sum_{b\le T} e(-ab/p)\Big| \le \frac{1}{|\sin(\pi a/p)|} \ll \frac{p}{a}.$$

Hence

$$\sum_{n\le T}\chi(f(n)) \ll m\sqrt{p}\log p. \ \blacksquare$$

To prove Theorem 1.5, we need the following Erdős–Turán inequality (see page 8 of [8]) and a theorem of Bourgain [1].

Lemma 2.5. *Let* $\{x_n\}$ *be a sequence of real numbers in* $(0,1)$. *For* $\alpha \in (0,1)$ *and* $\mathrm{V}\in\mathbb{N}$, *let* $N(\mathrm{V},\alpha)=\#\{n\le \mathrm{V}\,|\,0\le x_n<\alpha\}$. *Then, for any natural numbers* M, *one has*

$$|N(\mathrm{V},\alpha)-\mathrm{V}\alpha| \le \frac{\mathrm{V}}{\mathrm{M}+1}+3\sum_{m=1}^{\mathrm{M}}\frac{1}{m}\Big|\sum_{n\le \mathrm{V}} e(mx_n)\Big|.$$

Remark 2.1. The constant 3 in the above estimate has been improved to 1 by Mauduit, Rivat and Sárközy [7]. The original inequality without explicit constants is due to Davenport [4].

Theorem 2.6 (Bourgain). *Fix* $\delta>0$ *and a natural number* d. *For any subgroup* H *of* $(\mathbb{Z}/d\mathbb{Z})^*$ *with order* $> d^{\delta}$, *there is an* $\varepsilon'(\delta)>0$ *such that*

$$\Big|\sum_{x\in \mathrm{H}} e(ax/d)\Big| \ll |\mathrm{H}|d^{-\varepsilon'(\delta)}.$$

3. Proof of the theorems

Proof of Theorem 1.1. Using Lemma 2.2, we have

$$p\Big(\frac{q}{p-1}\Big)^{\mathrm{M}}-N(p,\mathrm{M}) \le \Big|N(p,\mathrm{M})-p\Big(\frac{q}{p-1}\Big)^{\mathrm{M}}\Big| \le 2^{\mathrm{M}}\mathrm{M}\sqrt{p}.$$

Thus

$$\sqrt{p}\Big(\frac{q}{p-1}\Big)^{\mathrm{M}} > 2^{\mathrm{M}}\mathrm{M} \tag{6}$$

implies $N(p,\mathrm{M})>0$. By hypothesis, we have

$$\frac{q}{p-1} > \frac{1}{(p-1)^{1/4\mathrm{M}}} > \frac{1}{p^{1/4\mathrm{M}}}.$$

Hence (6) is satisfied if $p>2^{4\mathrm{M}}\mathrm{M}^4$. $\blacksquare$

Remark 3.1. Note that the given conditions in Theorem 1.1 ensure

$$q > (p-1)^{1-1/4\mathrm{M}} \ge (2^{4\mathrm{M}}\mathrm{M}^4)^{1-1/4\mathrm{M}} \ge 2^{2\mathrm{M}}\mathrm{M}^2.$$

Proof of Theorem 1.2. Write

$$\mathrm{S}=\sum_{n\le \mathrm{T}}\frac{1}{\phi(d)}\sum_{\chi}\bar{\chi}(a)\chi(n^q),$$

where the inner sum is over all characters modulo d. Since

$$\sum_{\chi} \bar{\chi}(a)\chi(n^q) = \begin{cases} \phi(d) & \text{if } n^q \equiv a \pmod{d}, \\ 0 & \text{otherwise,} \end{cases}$$

S counts all solutions of (3) up to T. Further,

$$\mathrm{S} = \sum_{n\le \mathrm{T}} \frac{1}{\phi(d)}\Big\{ \sum_{\substack{\chi \\ \chi^q=\chi_0}} \bar{\chi}(a)\chi(n^q) + \sum_{\substack{\chi \\ \chi^q\neq\chi_0}} \bar{\chi}(a)\chi(n^q)\Big\},$$

where χ_0 is the principal character modulo d. Thus, we have

$$\begin{aligned} \mathrm{S} &= \frac{n(q)\mathrm{T}}{\phi(d)} + \frac{1}{\phi(d)} \sum_{\substack{\chi \\ \chi^q\neq\chi_0}} \bar{\chi}(a) \sum_{n\le \mathrm{T}} \chi^q(n) \\ &= \frac{n(q)\mathrm{T}}{\phi(d)} + O(\sqrt{d}\log d), \end{aligned}$$

by Pólya–Vinogradov (see page 143 of [3]). From this, we see that the main term is greater than the error term provided

$$\mathrm{T} \gg \frac{d^{1/2}\phi(d)\log d}{n(q)}.$$

Hence the theorem. ∎

Proof of Theorem 1.4. Write

$$\mathrm{S} = \sum_{n\le \mathrm{T}} \frac{1}{p-1} \sum_{\chi} \bar{\chi}(a)\chi(f(n)^q),$$

where the inner sum is over all characters modulo p. Then S counts the number of solutions of (4) up to T. As before, by dividing the inner sum into two parts depending on whether $\chi^q = \chi_0$ or not, we get

$$\mathrm{S} = \frac{q\mathrm{T}}{p-1} + \frac{1}{p-1} \sum_{\chi^q\neq\chi_0} \bar{\chi}(a) \sum_{n\le \mathrm{T}} \chi^q(f(n)).$$

By the given hypothesis, $(\mathrm{order}(\chi^q), \deg f) = 1$. Hence by Theorem 2.3 we have

$$\mathrm{S} = \frac{q\mathrm{T}}{p-1} + O(m\sqrt{p}\log p).$$

This completes the proof. ∎

Proof of Theorem 1.5. List the roots of the polynomial congruence

$$x^q \equiv a \pmod{d}, \qquad (a,d) = 1, \tag{7}$$

as $r_1 < \cdots < r_{n(q)}$. Consider the sequence $\{r_i/d\}$ of rational numbers in $(0,1)$. Then by the Erdős–Turán inequality (Lemma 2.5), we have

$$|N(n(q),\alpha) - n(q)\alpha| \le \frac{n(q)}{\mathrm{M}+1} + 3\sum_{m=1}^{\mathrm{M}} \frac{1}{m}\bigg|\sum_{i\le n(q)} e\bigg(\frac{mr_i}{d}\bigg)\bigg|$$

for any $\alpha \in (0,1)$ and $\mathrm{M} \ge 1$. Consider the subgroup

$$\mathrm{H} = \{n \in (\mathbb{Z}/d\mathbb{Z})^* \mid n^q \equiv 1 \pmod{d}\}$$

of $(\mathbb{Z}/d\mathbb{Z})^*$. Note that all roots of (7) lie in a coset $b\mathrm{H}$ with $b^q \equiv a \pmod{d}$ of H. Hence by the theorem of Bourgain (Theorem 2.6), we have

$$\bigg|\sum_{i\le n(q)} e\bigg(\frac{mr_i}{d}\bigg)\bigg| = \bigg|\sum_{h\in\mathrm{H}} e\bigg(\frac{mbh}{d}\bigg)\bigg| \ll n(q)d^{-\varepsilon'(\delta)}.$$

Hence by choosing $\mathrm{M} \gg d^{\varepsilon'(\delta)}$, we see that

$$\#\{r_i \mid r_i^q \equiv a \pmod{d}, 0 < r_i < \alpha d, 1 \le i \le n(q)\}$$
$$= N(n(q),\alpha) = n(q)\alpha + O(n(q)d^{-\varepsilon(\delta)}).$$

Acknowledgements. It is my pleasure to thank Ram Murty for sending me his paper [9] which initiated this work and also for many valuable suggestions. I would also like to thank Purusottam Rath and the referee for their valuable comments.

References

[1] J. Bourgain, *Exponential sum estimates over subgroups of $\mathbb{Z}_q^*$, q arbitrary*, J. Anal. Math. 97 (2005), 317–355.

[2] D. A. Burgess, *On Dirichlet characters of polynomials*, Proc. London Math. Soc. (3) 13 (1963), 537–548.

[3] A. Cojocaru and M. R. Murty, *An Introduction to Sieve Methods and Their Applications*, Cambridge Univ. Press, Cambridge, 2006.

[4] H. Davenport, *On the distribution of the lth power residues mod p*, J. London Math. Soc. 7 (1932), 117–121.

[5] S. Gun, F. Luca, P. Rath, B. Sahu and R. Thangadurai, *Distribution of residues modulo p*, Acta Arith. 129 (2007), 325–333.

[6] M. Hudson, *On the least non-residue of a polynomial*, J. London Math. Soc. 41 (1966), 745–749.

[7] C. Mauduit, J. Rivat and A. Sárközy, *On the pseudo-random properties of n^c*, Illinois J. Math. 46 (2002), 185–197.

[8] H. Montgomery, *Ten Lectures on the Interface between Analytic Number Theory and Harmonic Analysis*, CBMS Reg. Conf. Ser. Math. 84, Amer. Math. Soc., 1994.

[9] M. R. Murty, *Small solutions of polynomial congruences*, Indian J. Pure Appl. Math. 41 (2010), 15–23.

[10] W. Schmidt, *Equations over Finite Fields. An Elementary Approach*, Lecture Notes in Math. 536, Springer, Berlin, 1976.

[11] A. Weil, *On the Riemann hypothesis in function fields*, Proc. Nat. Acad. Sci. U.S.A. 27 (1941), 345–347.
[12] —, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind. 1041, Publ. Inst. Math. Univ. Strasbourg 7 (1945), Hermann, Paris, 1948.
[13] —, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. 34 (1948), 204–207.

Sanoli Gun
Institute of Mathematical Sciences
C.I.T. campus
Taramani, Chennai 600 113, India
E-mail: sanoli@imsc.res.in

Received on 13.6.2009
and in revised form on 20.1.2010 (6057)