International Journal of Mathematics and
Computer Science, **17**(2022), no. 1, 309–315

On the square-free and square-full solutions of polynomial congruences

Watcharapon Pimsert, Thorranin Thansri

Department of Mathematics
Faculty of Science
Kasetsart University
Bangkok, Thailand

email: fsciwcrp@ku.ac.th, fscitnt@ku.ac.th

(Received July 21, 2021, Accepted August 23, 2021)

Abstract

We study the distribution of the square-free and square-full roots (if they exist) of the congruence

$$x^d \equiv a \pmod q$$

with $\gcd(a, q) = 1$. Moreover, we obtain the smallest solution of these roots.

1 Introduction and results

Polynomial congruences have been studied by several authors (see, for example, chapter 13 of [2]). Murty [4] investigated an estimate of the smallest solution of the polynomial congruence

$$x^d \equiv a \ (\text{mod} p),$$

where p is a prime, d is a divisor of $p-1$ and $a^{(p-1)/d} \equiv 1 \ (\bmod p)$ and proved that the smallest solution x_0 satisfies $|x_0| \ll p^{3/2}(\log p)/q$. In the same year,

Key words and phrases: Character sums, polynomial congruences, square-free numbers, square-full numbers
AMS (MOS) Subject Classifications: 11T06, 11L40, 11T24.
ISSN 1814-0432, 2022, http://ijmcs.future-in-tech.net

Gun [1] studied an estimate of solutions of the polynomial congruences of the type

$$x^d \equiv a \ (\mathrm{mod} q), \tag{1.1}$$

where q is not necessarily prime and proved that the smallest solution x_0 satisfies

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

where $n(d)$ is the number of elements in $(\mathbb{Z}/q\mathbb{Z})^*$ whose order divides d.

It would be interesting to consider the special class of the solution of the polynomial congruences. In this paper, we investigate the bound solutions of (1.1) which are of special classes of integers, say, square-free and square-full numbers. A positive integer n is called square-free if it is not divisible by the square of any prime and a positive integer n is said to be square-full numbers if each of its prime factors appears to the power at least 2.

We obtain the following theorems.

Theorem 1.1. *Let q and d be positive integers such that $d \mid \phi(q)$. Suppose that the polynomial congruence (1.1) has a solution that is square-free. Then the smallest solution x_0 satisfies*

$$|x_0| \ll \frac{q^{3/8}\phi^2(q)\log^2 q}{(n(d))^2}\prod_{p|q}(1+p^{-1})^2.$$

Theorem 1.2. *Let q and d be positive integers such that $d \mid \phi(q)$. Suppose that the polynomial congruence (1.1) has a solution that is square-full. Then the smallest solution x_0 satisfies*

$$|x_0| \ll \frac{q^3\log^6 q}{A^6(q)},$$

where

$$A(q) = \frac{n(d)}{\phi(q)}\frac{\zeta(3/2)}{\zeta(3)}\prod_{p|q}\left(\frac{1-p^{-1}}{1+p^{-3/2}}\right) + \frac{1}{\phi(q)}\sum_{\substack{\chi^{2d}=\chi_0\\ \chi\neq\chi_0}}\overline{\chi(a)}\frac{L(3/2,\chi^d)}{\zeta(3)}\prod_{p|q}\left(1+\frac{1}{p}+\frac{1}{p^2}\right)^{-1}.$$

2 Lemmas

In this section, we collect several auxiliary results that will be used in our proofs of the theorems. Here are estimates of character sums over square-free numbers:

Lemma 2.1. *([3]) Let χ be non-trivial characters mod q. Then*

$$\Big|\sum_{n\le x}\mu^2(n)\chi(n)\Big| \ll \begin{cases} x^{1/2}q^{1/4}(\log q)^{1/2}, \\ x^{1/2}(\log x)q^{3/16+\varepsilon}. \end{cases}$$

Lemma 2.2. *([3]) Let q be an integer ≥ 2, we have*

$$\sum_{\substack{n\le x\\ \gcd(n,q)=1}} \mu^2(n) = \frac{x}{\zeta(2)}\prod_{p|q}\left(1+\frac{1}{p}\right)^{-1} + O(x^{1/2}\tau(q)),$$

where $\tau(n)$ denotes the number of positive divisors of n, and the product runs over primes $p \mid q$.

For any character χ mod q, we define

$$Q_2(x;\chi) := \sum_{n\le x}\alpha(n)\chi(n); \qquad \alpha(n) := \begin{cases} 1 & \text{if } n \text{ is a square-full integer;} \\ 0 & \text{otherwise,} \end{cases}$$

which is the character sum of square-full integers not exceeding x. Then we obtain the following estimates of character sums over square-full numbers.

Lemma 2.3. *([3]) Let $q > 3$ be an integer, χ a Dirichlet character mod q, and χ_0 the trivial character mod q. Then*

$$Q_2(x;\chi_0) = \frac{\zeta(3/2)}{\zeta(3)}\prod_{p|q}\left(\frac{1-p^{-1}}{1+p^{-3/2}}\right)x^{1/2} + \frac{\zeta(2/3)}{\zeta(2)}\prod_{p|q}\left(\frac{1-p^{-2/3}}{1+p^{-1}}\right)x^{1/3} + O\Big(x^{1/6+\varepsilon}q^{\varepsilon}\Big). \tag{2.2}$$

If χ is a quadratic character, then

$$Q_2(x;\chi) = \frac{L(3/2,\chi)}{\zeta(3)}\prod_{p|q}\left(1+\frac{1}{p}+\frac{1}{p^2}\right)^{-1}x^{1/2} + O\Big(x^{1/4}(\log x)^{1/2}q^{3/32+\varepsilon}\Big), \tag{2.3}$$

and if $\chi^2 \ne \chi_0$ and $\chi \ne \chi_0$, then

$$Q_2(x;\chi) = O\Big(x^{1/3}q^{1/2}\log q\Big). \tag{2.4}$$

Proof. We only give the proof of (2.4). If $\chi^2 \neq \chi_0$ and $\chi \neq \chi_0$, then using Burgess inequality on character sum, we have

$$\begin{aligned} Q_2(x;\chi) &= \sum_{a^2b^3} \mu^2(b)\chi(a^2b^3) \\ &= \sum_{b\leq x^{1/3}} \mu^2(b)\chi(b^3) \sum_{a\leq x^{1/2}b^{-3/2}} \chi(a^2) \\ &\ll q^{1/2}\log q \sum_{b\leq x^{1/3}} 1 \\ &= O\Big(x^{1/3}q^{1/2}\log q\Big). \end{aligned}$$

□

3 Proofs of Theorems

Proof of Theorem 1.1. For a positive integer N, let us define the following function

$$T(N) = \frac{1}{\phi(q)} \sum_{\substack{n\leq N \\ \text{n is square-free}}} \sum_{\chi} \overline{\chi(a)}\chi(n^d), \tag{3.5}$$

where the inner sum run over all characters modulo q. Indeed, $T(N)$ is the number of solutions that are square-free of (1.1) and do not exceed N. The behavior of the inner sum differs with χ^d. Thus we write (3.5) as

$$\begin{aligned} T(N) &= \frac{1}{\phi(q)} \sum_{\chi} \overline{\chi(a)} \sum_{n\leq N} \mu^2(n)\chi(n^d) \\ &= \frac{1}{\phi(q)} \sum_{\substack{\chi \\ \chi^d=\chi_0}} \overline{\chi(a)} \sum_{n\leq N} \mu^2(n)\chi(n^d) + \frac{1}{\phi(q)} \sum_{\substack{\chi \\ \chi^d\neq\chi_0}} \overline{\chi(a)} \sum_{n\leq N} \mu^2(n)\chi(n^d) \\ &= \frac{1}{\phi(q)} \sum_{\substack{\chi \\ \chi^d=\chi_0}} \overline{\chi(a)} \sum_{\substack{n\leq N \\ \gcd(n,q)=1}} \mu^2(n) + \frac{1}{\phi(q)} \sum_{\substack{\chi \\ \chi^d\neq\chi_0}} \overline{\chi(a)} \sum_{n\leq N} \mu^2(n)\chi(n^d). \end{aligned}$$

In view of Lemmas 2.1 and 2.2, we have

$$\begin{aligned} T(N) &= \frac{1}{\phi(q)} \sum_{\substack{\chi \\ \chi^d=\chi_0}} \overline{\chi(a)} \Big(\frac{N}{\zeta(2)} \prod_{p|q} \left(1+\frac{1}{p}\right)^{-1} + O(N^{1/2}\tau(q))\Big) + O(N^{1/2}(\log N)q^{3/16+\varepsilon}) \\ &= \frac{n(d)}{\phi(q)} \frac{N}{\zeta(2)} \prod_{p|q} \left(1+\frac{1}{p}\right)^{-1} + O(N^{1/2}(\log N)q^{3/16+\varepsilon}), \end{aligned}$$

which completes the proof. □

Proof of Theorem 1.2. Let

$$Q(N) = \frac{1}{\phi(q)} \sum_{\substack{n \le N \\ \text{n is square-full}}} \sum_{\chi} \overline{\chi(a)} \chi(n^d). \tag{3.6}$$

where the inner sum is over all characters modulo q. The function $Q(N)$ counts the number of solutions that are square-full of (1.1) up to N. Here, the behavior of the inner sum will be different depending on whether χ^d is principal character, quadratic, cubic character or none of this. Thus we write (3.6) as

$$\begin{aligned}
Q(N) &= \frac{1}{\phi(q)} \sum_{\chi} \overline{\chi(a)} \sum_{n \le N} \alpha(n) \chi(n^d) \\
&= \frac{1}{\phi(q)} \sum_{\substack{\chi \\ \chi^d = \chi_0}} \overline{\chi(a)} \sum_{n \le N} \alpha(n) \chi(n^d) + \frac{1}{\phi(q)} \sum_{\substack{\chi \\ \chi^d \neq \chi_0}} \overline{\chi(a)} \sum_{n \le N} \alpha(n) \chi(n^d) \\
&= \frac{1}{\phi(q)} \sum_{\substack{\chi \\ \chi^d = \chi_0}} \overline{\chi(a)} \sum_{\substack{n \le N \\ \gcd(n,q)=1}} \alpha(n) + \frac{1}{\phi(q)} \sum_{\substack{\chi \\ \chi^d \neq \chi_0}} \overline{\chi(a)} \sum_{n \le N} \alpha(n) \chi(n^d) \\
&=: \frac{1}{\phi(q)} \sum_{\substack{\chi \\ \chi^d = \chi_0}} \overline{\chi(a)} Q_1(N, \chi) + \frac{1}{\phi(q)} \sum_{\substack{\chi \\ \chi^d \neq \chi_0}} \overline{\chi(a)} Q_2(N, \chi).
\end{aligned} \tag{3.7}$$

By (2.2) in Lemma 2.3, we have

$$\begin{aligned}
&\frac{1}{\phi(q)} \sum_{\substack{\chi \\ \chi^d = \chi_0}} \overline{\chi(a)} Q_1(N, \chi) = \frac{1}{\phi(q)} \sum_{\substack{\chi \\ \chi^d = \chi_0}} \overline{\chi(a)} \Big(\frac{\zeta(3/2)}{\zeta(3)} \prod_{p|q} \left(\frac{1 - p^{-1}}{1 + p^{-3/2}} \right) N^{1/2} \\
&+ \frac{\zeta(2/3)}{\zeta(2)} \prod_{p|q} \left(\frac{1 - p^{-2/3}}{1 + p^{-1}} \right) N^{1/3} \Big) + O\Big(\frac{n(d)}{\phi(q)} N^{1/6+\varepsilon} q^{\varepsilon} \Big) \\
&= \frac{n(d)}{\phi(q)} \frac{\zeta(3/2)}{\zeta(3)} \prod_{p|q} \left(\frac{1 - p^{-1}}{1 + p^{-3/2}} \right) N^{1/2} + \frac{n(d)}{\phi(q)} \frac{\zeta(2/3)}{\zeta(2)} \prod_{p|q} \left(\frac{1 - p^{-2/3}}{1 + p^{-1}} \right) N^{1/3} \\
&+ O\Big(\frac{n(d)}{\phi(q)} N^{1/6+\varepsilon} q^{\varepsilon} \Big).
\end{aligned} \tag{3.8}$$

For the second sum in (3.7), with (2.3) and (2.4) in Lemma 2.3, we have

$$Q_2(N,\chi^d) = \begin{cases} \frac{L(3/2,\chi^d)}{\zeta(3)} \prod_{p|q} \left(1+\frac{1}{p}+\frac{1}{p^2}\right)^{-1} N^{1/2} + O\Big(N^{1/4}(\log N)^{1/2} q^{3/32+\varepsilon}\Big) & \text{if } \chi^d = \chi_0, \\ O\Big(N^{1/3} q^{1/2} \log q\Big) & \text{if } \chi^{2d} \neq \chi_0. \end{cases} \tag{3.9}$$

Inserting (3.8) and (3.9) into (3.7), we get

$$\begin{aligned} Q(N) = \Big(&\frac{n(d)}{\phi(q)} \frac{\zeta(3/2)}{\zeta(3)} \prod_{p|q} \left(\frac{1-p^{-1}}{1+p^{-3/2}}\right) \\ &+ \frac{1}{\phi(q)} \sum_{\substack{\chi^{2d}=\chi_0 \\ \chi\neq\chi_0}} \overline{\chi(a)} \frac{L(3/2,\chi^d)}{\zeta(3)} \prod_{p|q} \left(1+\frac{1}{p}+\frac{1}{p^2}\right)^{-1} \Big) N^{1/2} \\ &+ O\Big(N^{1/3} q^{1/2} (\log q)\Big). \end{aligned}$$

The assertion holds by comparing the error term with the main term. □

Acknowledgment. The first author gratefully acknowledges the financial support under the Basic Research Fund (BRF) provided by the Faculty of Science, Kasetsart University.

References

[1] S. Gun, *On solutions of polynomial congruences*, Acta. Arith., **144,** no. 2, (2010), 151–158,

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

[3] M. Munsch, *Character sums over squarefree and squarefull numbers*, Arch. Math., **102,** no. 6, (2014), 555–563.

[4] M. R. Murty, *Small solutions of polynomial congruences*, Indian. J. Pure. Appl. Math., **41,** no. 1, (2010), 15–23.