PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 144, Number 6, June 2016, Pages 2411–2418
http://dx.doi.org/10.1090/proc/12919
Article electronically published on October 21, 2015

THE CONGRUENCE $x^x \equiv \lambda \pmod p$

J. CILLERUELO AND M. Z. GARAEV

(Communicated by Ken Ono)

Abstract. In the present paper we obtain several new results related to the problem of upper bound estimates for the number of solutions of the congruence

$$x^x \equiv \lambda \pmod p; \quad x \in \mathbb{N}, \quad x \le p-1,$$

where p is a large prime number and λ is an integer coprime to p. Our arguments are based on recent estimates of trigonometric sums over subgroups due to Shkredov and Shteinikov.

1. Introduction

For a prime p and an integer λ let $J(p;\lambda)$ be the number of solutions of the congruence

$$x^x \equiv \lambda \pmod p; \quad x \in \mathbb{N}, \quad x \le p-1. \tag{1}$$

Note that the period of the function x^x modulo p is $p(p-1)$, which is larger than the range in congruence (1).

From the works of Crocker [4] and Somer [8] it is known that there are at least $\lfloor (p-1)/2 \rfloor$ and at most $3p/4 + p^{1/2+o(1)}$ incongruent values of $x^x \pmod p$ when $1 \le x \le p-1$. There are several conjectures in [5] related to this function.

New approaches to study $J(p;\lambda)$ were given by Balog, Broughan and Shparlinski; see [1] and [2]. In the special case $\lambda = 1$ it was shown in [1] that $J(p;1) < p^{1/3+o(1)}$. This estimate was slightly improved in our work [3] to the bound $J(p;1) \ll p^{1/3-c}$ for some absolute constant $c > 0$. Note that the method of [3] applies to more general exponential congruences, however, the constant c there becomes too small. In the present paper we use a different approach and prove the following results.

Theorem 1. *The number $J(p;1)$ of solutions of the congruence*

$$x^x \equiv 1 \pmod p; \quad x \in \mathbb{N}, \quad x \le p-1, \tag{2}$$

satisfies $J(p;1) \lesssim p^{27/82}$.

Here and below we use the notation $A \lesssim B$ to denote that $A < Bp^{o(1)}$; that is, for any $\varepsilon > 0$ there exists $c = c(\varepsilon) > 0$ such that $A < cBp^{\varepsilon}$. As usual, $\operatorname{ord}\lambda$ denotes the multiplicative order of λ, that is, the smallest positive integer t such that $\lambda^t \equiv 1 \pmod p$. We recall that $\operatorname{ord}\lambda | p-1$.

Received by the editors March 23, 2015 and, in revised form, July 31, 2015.
2010 *Mathematics Subject Classification.* Primary 11A07.

Theorem 2. *Uniformly over $t|p-1$, we have, as $p \to \infty$,*

$$\sum_{\substack{1\le\lambda\le p-1\\ \operatorname{ord}\lambda=t}} J(p;\lambda) \lesssim t + p^{1/3}t^{1/2}. \tag{3}$$

In the range $t < p^{1/3}$ our Theorem 2 improves some results of the aforementioned works [1] and [2]. Note that in the case $t = 1$ the estimate of Theorem 1 is stronger. In fact, following the argument that we use in the proof of Theorem 1 it is possible to improve Theorem 2 in specific small ranges of t.

Now let $I(p)$ denote the number of solutions of the congruence

$$x^x \equiv y^y \pmod p; \quad x \in \mathbb{N}, \quad y \in \mathbb{N}, \quad x \le p-1, \quad y \le p-1.$$

There is the following relationship between $I(p)$ and $J(p;\lambda)$:

$$I(p) = \sum_{\lambda=1}^{p-1} J(p;\lambda)^2.$$

We modify one of the arguments of [1] and obtain the following refinement on [1, Theorem 8].

Theorem 3. *We have, as $p \to \infty$,*

$$I(p) \lesssim p^{23/12}. \tag{4}$$

In order to prove our results, we first reduce the problem to estimates of exponential sums over subgroups. In the proof of Theorem 1 we use Shteinikov's result from [7], while in the proof of Theorem 2 we use Shkredov's result from [6] (see Lemma 2 and Lemma 3 below).

In what follows, $\mathbb{F}_p$ is the field of residue classes modulo p. The elements of $\mathbb{F}_p$ we associate with their concrete representatives from $\{0, 1, \dots, p-1\}$. For an integer m coprime to p by m^* we denote the smallest positive integer such that $m^*m \equiv 1 \pmod p$. We also use the abbreviation

$$e_p(z) = e^{2\pi i z/p}.$$

2. Lemmas

Lemma 1. *Let*

$$\lambda \not\equiv 0 \pmod p, \quad n \in \mathbb{N}, \quad 1 \le M \le p.$$

Then for any fixed constant $k \in \mathbb{N}$ the number J of solutions of the congruence

$$x^n \equiv \lambda \pmod p, \quad x \in \mathbb{N}, \quad x \le M,$$

satisfies

$$J \lesssim \Big(1 + \frac{M}{p^{1/k}}\Big) n^{1/k}.$$

In particular, if $n = dt < p$ and $M = p/d$, then we have the bound

$$J \lesssim \Big(d^{1/k} + \Big(\frac{p}{d}\Big)^{1-1/k}\Big) t^{1/k}.$$

Proof. We have

$$J^k \lesssim \#\{(x_1, \ldots, x_k) \in \mathbb{N}^k \cap [1, M]^k; \quad (x_1 \ldots x_k)^n \equiv \lambda^k \pmod p\}.$$

Since for a given integer μ the congruence

$$X^n \equiv \mu \pmod p, \quad X \in \mathbb{N}, \quad X \le p,$$

has at most n solutions, there exists a positive integer $\lambda_0 < p$ such that

$$J^k \lesssim nJ_1,$$

where J_1 is the number of solutions of the congruence

$$x_1 \ldots x_k \equiv \lambda_0 \pmod p; \quad (x_1, \ldots, x_k) \in \mathbb{N}^k \cap [1, M]^k.$$

It follows that

$$x_1 \ldots x_k = \lambda_0 + py; \quad (x_1, \ldots, x_k) \in \mathbb{N}^k \cap [1, M]^k, \quad y \in \mathbb{Z}.$$

Since the left-hand side of this equation does not exceed M^k, we get that $|y| \le M^k/p$. Hence, for some fixed y_0 we have

$$J_1 \lesssim \Big(1 + \frac{M^k}{p}\Big) J_2,$$

where J_2 is the number of solutions of the equation

$$x_1 \ldots x_k = \lambda_0 + py_0; \quad (x_1, \ldots, x_k) \in \mathbb{N}^k \cap [1, M]^k.$$

Hence, from the bound for the divisor function it follows that $J_2 \lesssim 1$. Thus,

$$J^k \lesssim \Big(1 + \frac{M^k}{p}\Big) n,$$

and the result follows. □

Let H_d be the subgroup of $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ of order d. From the classical estimates for exponential sums over subgroups it is known that

$$\Big| \sum_{h \in H_d} e_p(ah) \Big| \le p^{1/2}.$$

For a wide range of d this bound has been improved in a series of works. Here, we need some results due to Shteinikov [7] (see Lemma 2 below) and Shkredov [6] (see Lemma 3 below). They will be used in the proof of Theorem 1 and Theorem 2, respectively.

Lemma 2. *Let H_d be the subgroup of $\mathbb{F}_p^*$ of order $d < p^{1/2}$. Then for any integer $a \not\equiv 0 \pmod p$ the following bound holds:*

$$\Big| \sum_{h \in H_d} e_p(ah) \Big| \lesssim p^{1/18} d^{101/126}.$$

Lemma 3. *Let H_d be the subgroup of $\mathbb{F}_p^*$ of order $d < p^{2/3}$. Then for any integer $a \not\equiv 0 \pmod p$ the following bound holds:*

$$\Big| \sum_{h \in H_d} e_p(ah) \Big| \lesssim p^{1/6} d^{1/2}.$$

The following two results are due to Balog, Broughan and Shparlinski [1, 2].

Lemma 4. *Uniformly over $t|p-1$, we have, as $p \to \infty$,*

$$\sum_{\substack{1\le\lambda\le p-1\\ \operatorname{ord}\lambda=t}} J(p;\lambda) \lesssim t + p^{1/2}.$$

Lemma 5. *Uniformly over $t|p-1$ and all integers λ with $\gcd(\lambda,p)=1$ and $\operatorname{ord}\lambda = t$, we have, as $p \to \infty$,*

$$J(p;\lambda) \lesssim pt^{-1/12}.$$

We also need the following lemma.

Lemma 6. *Let a, x be positive integers satisfying $a^x \equiv 1 \pmod p$. Then $a^d \equiv 1 \pmod p$ for $d = \gcd(x, p-1)$.*

This lemma is well known and the proof is simple. Indeed, we can write $d = kx + \ell(p-1)$ with k, ℓ integers. It then follows that

$$a^d \equiv a^{\ell(p-1)} \equiv 1 \pmod p$$

by Fermat's little theorem.

The following lemma is also well known; see, for example, the exercises and solution to chapter 3 in Vinogradov's book [9].

Lemma 7. *For any integers U and $V > U$ the following bound holds:*

$$\sum_{a=1}^{p-1}\Big|\sum_{z=U}^{V} e_p(az)\Big| \lesssim p.$$

3. Proof of Theorem 1

We have

$$J(p;1) = \sum_{d|p-1} J'_d,$$

where J'_d is the number of solutions of (2) with $\gcd(x, p-1) = d$. It then follows by Lemma 6 that

$$J(p;1) \le \sum_{d|p-1} J_d,$$

where J_d is the number of solutions of the congruence

$$z^d \equiv (d^d)^* \pmod p; \quad z \in \mathbb{N}, \quad z \le (p-1)/d.$$

We have, therefore,

$$J(p;1) \le R_1 + R_2 + R_3 + \sum_{\substack{d|p-1\\ d<p^{3/7}}} J_d,$$

where

$$R_1 = \sum_{\substack{d|p-1\\ d>p^{5/7}}} J_d; \quad R_2 = \sum_{\substack{d|p-1\\ p^{4/7}<d<p^{5/7}}} J_d; \quad R_3 = \sum_{\substack{d|p-1\\ p^{3/7}<d\le p^{4/7}}} J_d.$$

The trivial estimate $J_d \le p/d$ implies that

$$R_1 \lesssim \sum_{\substack{d|p-1\\ d>p^{5/7}}} \frac{p}{d} \lesssim \sum_{d|p-1} p^{2/7} \lesssim p^{2/7}.$$

To estimate R_2 we use Lemma 1 with $k = 3$ and get

$$R_2 = \sum_{\substack{d|p-1 \\ p^{4/7}<d<p^{5/7}}} J_d \lesssim \sum_{\substack{d|p-1 \\ p^{4/7}<d<p^{5/7}}} (d^{1/3} + (p/d)^{2/3}) \lesssim \sum_{d|p-1} p^{2/7} \lesssim p^{2/7}.$$

To estimate R_3 we use Lemma 1 with $k = 2$ and get

$$R_3 = \sum_{\substack{d|p-1 \\ p^{3/7}<d<p^{4/7}}} J_d \lesssim \sum_{\substack{d|p-1 \\ p^{3/7}<d<p^{4/7}}} (d^{1/2} + (p/d)^{1/2}) \lesssim \sum_{d|p-1} p^{2/7} \lesssim p^{2/7}.$$

Thus,

$$J(p; 1) \lesssim p^{2/7} + \sum_{\substack{d|p-1 \\ d<p^{3/7}}} J_d.$$

Hence, there exists $d|p - 1$ with $d < p^{3/7}$ such that

$$J(p; 1) \lesssim p^{2/7} + J_d. \tag{5}$$

Applying Lemma 1 with $k = 2$, we get

$$J_d \lesssim d^{1/2} + (p/d)^{1/2} \lesssim (p/d)^{1/2}. \tag{6}$$

Now let H_d be the subgroup of $\mathbb{F}_p^*$ of order d. We recall that J_d is the number of solutions of the congruence

$$(dz)^d \equiv 1 \pmod p; \quad z \in \mathbb{N}, \quad z \le (p-1)/d.$$

Therefore,

$$J_d = \#\{z \in \mathbb{N}; \quad z \le (p-1)/d, \quad dz \pmod p \in H_d\}.$$

It then follows that

$$J_d = \frac{1}{p} \sum_{a=0}^{p-1} \sum_{1 \le z \le (p-1)/d} \sum_{h \in H_d} e_p(a(dz - h)).$$

Separating the term corresponding to $a = 0$ and using Lemma 2 for $a \ne 0$, we get

$$J_d \le 1 + p^{1/18} d^{101/126} \Big(\frac{1}{p} \sum_{a=1}^{p-1} \Big| \sum_{1 \le z \le (p-1)/d} e_p(adz) \Big| \Big) \lesssim p^{1/18} d^{101/126}.$$

Using Lemma 7, we get the following bound for the latter double sum:

$$\sum_{a=1}^{p-1} \Big| \sum_{1 \le z \le (p-1)/d} e_p(adz) \Big| = \sum_{b=1}^{p-1} \Big| \sum_{1 \le z \le (p-1)/d} e_p(bz) \Big| \lesssim p.$$

Therefore

$$J_d \lesssim p^{1/18} d^{101/126}.$$

Comparing this estimate with (6) we obtain

$$J_d \lesssim p^{27/82}.$$

Incorporating this in (5), we get the desired result.

4. Proof of Theorem 2

In view of Lemma 4, it suffices to deal with the case $t < p^{1/3}$.

Since $\lambda^t \equiv 1 \pmod p$, it follows from (1) that

$$\sum_{\substack{1\le\lambda\le p-1\\ \mathrm{ord}\,\lambda=t}} J(p;\lambda) \le \#\{x\in\mathbb{N};\quad x^{tx}\equiv 1 \pmod p,\quad x\le p-1\}.$$

Hence, denoting $d=\gcd(x,(p-1)/t)$ and using Lemma 6 we obtain that

$$\sum_{\substack{1\le\lambda\le p-1\\ \mathrm{ord}\,\lambda=t}} J(p;\lambda) \le \sum_{d|(p-1)/t} T_d,$$

where T_d is the number of solutions of the congruence

$$z^{dt}\equiv (d^{dt})^* \pmod p;\quad z\in\mathbb{N},\quad z\le (p-1)/d.$$

By the trivial estimate $T_d\le p/d$ we have

$$\sum_{\substack{d|p-1\\ d>p^{2/3}}} T_d \le \sum_{d|p-1} p^{1/3} \lesssim p^{1/3}.$$

Furthermore, applying Lemma 1 with $k=2$, we get

$$\sum_{\substack{d|p-1\\ p^{1/3}<d<p^{2/3}}} T_d \le \sum_{\substack{d|p-1\\ p^{1/3}<d<p^{2/3}}} \Big(d^{1/2}+(p/d)^{1/2}\Big)t^{1/2} \lesssim p^{1/3}t^{1/2}.$$

Therefore,

$$\sum_{\substack{1\le\lambda\le p-1\\ \mathrm{ord}\,\lambda=t}} J(p;\lambda) \le p^{1/3}t^{1/2} + \sum_{\substack{d|(p-1)/t\\ d<p^{1/3}}} T_d. \tag{7}$$

Recall that $t<p^{1/3}$; thus $dt|p-1$ and $dt<p^{2/3}$.

Let H_{dt} be the subgroup of $\mathbb{F}_p^*$ of order dt. Since T_d is the number of solutions of the congruence

$$(dz)^{dt}\equiv 1 \pmod p;\quad z\in\mathbb{N},\quad z\le (p-1)/d,$$

it follows that

$$T_d = \#\{z\in\mathbb{N};\quad z\le (p-1)/d,\quad dz \pmod p \in H_{dt}\}.$$

Therefore,

$$T_d = \frac{1}{p}\sum_{a=0}^{p-1}\sum_{1\le z\le (p-1)/d}\sum_{h\in H_{dt}} e_p(a(dz-h)).$$

Separating the term corresponding to $a=0$ and using Lemma 3 for $a\ne 0$ (with d replaced by dt), we get

$$T_d \le t + p^{1/6}d^{1/2}t^{1/2}\Big(\frac{1}{p}\sum_{a=1}^{p-1}\Big|\sum_{1\le z\le (p-1)/d} e_p(adz)\Big|\Big).$$

Applying Lemma 7 to the double sum, as in the proof of Theorem 1, we obtain for $d<p^{1/3}$ the bound

$$T_d \lesssim t + p^{1/6}d^{1/2}t^{1/2} \lesssim t + p^{1/3}t^{1/2}.$$

Thus,

$$\sum_{\substack{d|(p-1)/t \\ d<p^{1/3}}} T_d \le \sum_{d|p-1} (t + p^{1/3}t^{1/2}) \lesssim t + p^{1/3}t^{1/2}.$$

Putting this into (7), we conclude the proof.

5. Proof of Theorem 3

We follow the arguments of [1] with some modifications. We have

$$I(p) = \sum_{\lambda=1}^{p-1} J(p;\lambda)^2 = \sum_{t|p-1} \sum_{\substack{1\le\lambda\le p-1 \\ \operatorname{ord}\lambda=t}} J(p;\lambda)^2.$$

It then follows that for some fixed order $t|p-1$ we have

$$I(p) \lesssim \sum_{\substack{1\le\lambda\le p-1 \\ \operatorname{ord}\lambda=t}} J(p;\lambda)^2.$$

We can split the range of $J(p;\lambda)$ into $O(\log p)$ dyadic intervals. Then, for some $1 \le M \le p$, we have

$$I(p) \lesssim |\mathcal{A}|M^2, \tag{8}$$

where $|\mathcal{A}|$ is the cardinality of the set

$$\mathcal{A} = \{1 \le \lambda \le p-1; \quad \operatorname{ord}\lambda = t, \quad M \le J(p;\lambda) < 2M\}.$$

From Lemma 5 we have

$$M \lesssim pt^{-1/12}. \tag{9}$$

On the other hand, by Lemma 4 we also have

$$|\mathcal{A}|M \lesssim \sum_{\lambda\in\mathcal{A}} J(p;\lambda) \lesssim \sum_{\substack{1\le\lambda\le p-1 \\ \operatorname{ord}\lambda=t}} J(p;\lambda) \lesssim t + p^{1/2}.$$

If $t < p^{1/2}$, then using (8) we get

$$I(p) \lesssim |\mathcal{A}|M^2 \lesssim (|\mathcal{A}|M)^2 \lesssim p,$$

and the result follows. If $t > p^{1/2}$, then we get $|\mathcal{A}|M \lesssim t$. Therefore, using (8) and (9) we get

$$I(p) \lesssim |\mathcal{A}|M^2 \lesssim t(pt^{-1/12}) = pt^{11/12} \lesssim p^{23/12}.$$

This proves Theorem 3.

Acknowledgement

The first author was supported by the grants MTM2014-56350-P of MINECO and ICMAT Severo Ochoa project SEV-2011-0087. The second author was supported by the sabbatical grant from PASPA-DGAPA-UNAM.

References

[1] Antal Balog, Kevin A. Broughan, and Igor E. Shparlinski, *On the number of solutions of exponential congruences*, Acta Arith. **148** (2011), no. 1, 93–103, DOI 10.4064/aa148-1-7. MR2784012 (2012f:11071)

[2] Antal Balog, Kevin A. Broughan, and Igor E. Shparlinski, *Sum-products estimates with several sets and applications*, Integers **12** (2012), no. 5, 895–906, DOI 10.1515/integers-2012-0012. MR2988554

[3] J. Cilleruelo and M. Z. Garaev, *Congruences involving product of intervals and sets with small multiplicative doubling modulo a prime and applications*, Preprint (2014).

[4] Roger Crocker, *On residues of n^n*, Amer. Math. Monthly **76** (1969), 1028–1029. MR0248072 (40 #1326)

[5] Joshua Holden and Pieter Moree, *Some heuristics and results for small cycles of the discrete logarithm*, Math. Comp. **75** (2006), no. 253, 419–449 (electronic), DOI 10.1090/S0025-5718-05-01768-0. MR2176407 (2006i:11145)

[6] I. D. Shkredov, *On exponential sums over multiplicative subgroups of medium size*, Finite Fields Appl. **30** (2014), 72–87, DOI 10.1016/j.ffa.2014.06.002. MR3249821

[7] Yu. N. Shteinikov, *Estimates of trigonometric sums modulo a prime*, Preprint, 2014.

[8] Lawrence Somer, *The residues of n^n modulo p*, Fibonacci Quart. **19** (1981), no. 2, 110–117. MR614045 (82g:10007)

[9] I. M. Vinogradov, *Elements of number theory.* Translated by S. Kravetz. Dover Publications, Inc., New York, 1954. MR0062138 (15,933e)

Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM) and Departamento de Matemáticas, Universidad Autónoma de Madrid, Madrid-28049, Spain
E-mail address: `franciscojavier.cilleruelo@uam.es`

Centro de Ciencias Matemáticas, Universidad Nacional Autónoma de México, C.P. 58089, Morelia, Michoacán, México
E-mail address: `garaev@matmor.unam.mx`