arXiv:1003.1997v1 [math.NT] 9 Mar 2010

On the Number of Solutions of Exponential Congruences

Antal Balog
Alfréd Rényi Institute of Mathematics
Hungarian Academy of Sciences
H-1364 Budapest, P.O. Box: 127, Hungary
balog@renyi.hu

Kevin A. Broughan
Department of Mathematics
University of Waikato
Private Bag 3105, Hamilton, New Zealand
kab@waikato.ac.nz

Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
igor@comp.mq.edu.au

March 11, 2010

Abstract

For a prime p and an integer $a \in \mathbb{Z}$ we obtain nontrivial upper bounds on the number of solutions to the congruence $x^x \equiv a \pmod p$, $1 \le x \le p-1$. We use these estimates to estimate the number of solutions to the congruence $x^x \equiv y^y \pmod p$, $1 \le x, y \le p-1$, which is of cryptographic relevance.

1 Introduction

For a prime p and an integer $a \in \mathbb{Z}$ we denote by $N(p;a)$ the number of solutions to the congruence

$$x^x \equiv a \pmod p, \qquad 1 \le x \le p-1. \tag{1}$$

Obviously only the case of $\gcd(a,p)=1$ is of interest.

We note that other than the result Crocker [3] showing that there are at least $\lfloor \sqrt{(p-1)/2} \rfloor$ incongruent values of $x^x \pmod p$ when $1 \le x \le p-1$ and our estimates, little appears to be known about the solutions to (1). The function $x \mapsto x^x \pmod p$, is also used in some cryptographic protocols (see [9, Sections 11.70 and 11.71]), so certainly deserves further investigation, see also [8] for various conjectures concerning this function.

Here we suggest several approaches to studying this congruence and derive some upper bounds for $N(p;a)$.

Our first bound is nontrivial if a is of small multiplicative order, which in the particular case when $a=1$, takes the form $N(p;a) \le p^{1/3+o(1)}$ as $p \to \infty$. The second bound is nontrivial if a is of large multiplicative order, which in the particular case when a is a primitive root modulo p, takes the form $N(p;a) \le p^{11/12+o(1)}$ as $p \to \infty$.

Furthermore, both bounds combined imply that as $p \to \infty$, we have the uniform estimate

$$N(p;a) \le p^{12/13+o(1)}. \tag{2}$$

Finally, we estimate the number of solutions $M(p)$ to the symmetric congruence

$$x^x \equiv y^y \pmod p, \qquad 1 \le x, y \le p-1, \tag{3}$$

which has been considered by Holden & Moree [8] in their study of short cycles in the iterations of the discrete logarithm modulo p, see also [6, 7]. However, no nontrivial estimate of $M(p)$ has been known prior to this work. Clearly

$$M(p) = \sum_{a=1}^{p-1} N(p;a)^2. \tag{4}$$

Thus using the bound (2) and the identity

$$\sum_{a=1}^{p-1} N(p;a) = p-1, \tag{5}$$

we immediately derive

$$M(p) \le p^{25/13+o(1)}. \tag{6}$$

However here we obtain a slightly stronger bound, namely

$$M(p) \le p^{48/25+o(1)}.$$

Surprisingly enough, besides elementary number theory arguments, the bounds derived here rely on some results and arguments from additive combinatorics, in particular on results of Garaev [4].

For an integer $m \ge 1$ we use $\mathbb{Z}_m$ to denote the residue ring modulo m and we use $\mathbb{Z}_m^*$ to denote the unit group of $\mathbb{Z}_m$.

Note that without the condition $1 \le x \le p-1$ (needed in the cryptographic application) there are always many solutions. Let g be a primitive root modulo p. For any element $a \in \mathbb{Z}_p^*$ (and so for any integer $a \not\equiv 0 \pmod p$) we use $\operatorname{ind} a$ for its discrete logarithm modulo p, that is, the unique residue class $v \pmod{p-1}$ with

$$g^v \equiv a \pmod p.$$

Now, if for a primitive root g we have

$$x \equiv p \operatorname{ind} a - (p-1)g \pmod{p(p-1)},$$

then

$$x^x \equiv g^{p \operatorname{ind} a-(p-1)g} \equiv (g^p)^{\operatorname{ind} a} \cdot (g^{-g})^{p-1} \equiv a \pmod p.$$

2 Elements of Small Order

We need to recall some notions and results from additive combinatorics.

For a prime p and a set $\mathcal{A} \subseteq \mathbb{Z}_p^*$ we define the sets

$$\mathcal{A}+\mathcal{A} = \{a_1+a_2 \ : \ a_1, a_2 \in \mathcal{A}\}, \quad \mathcal{A}\cdot\mathcal{A} = \{a_1a_2 \ : \ a_1, a_2 \in \mathcal{A}\}.$$

Our bound on $N(p,a)$ makes use of the following estimate of Garaev [4, Theorem 1].

Lemma 1 *For any set $\mathcal{A} \subseteq \mathbb{Z}_p^*$,*

$$\#(\mathcal{A}+\mathcal{A}) \cdot \#(\mathcal{A}\cdot\mathcal{A}) \gg \min\left\{p\#\mathcal{A}, \frac{(\#\mathcal{A})^4}{p}\right\}.$$

Let $\operatorname{ord} a$ denote the multiplicative order of $a \in \mathbb{Z}_p^*$.

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

$$\sum_{\substack{a \in \mathbb{Z}_p^* \\ \operatorname{ord} a \mid t}} N(p;a) \le \max\{t, p^{1/2}t^{1/4}\} p^{o(1)}.$$

Proof. Fix a primitive root g mod p. The union of non-zero residue classes a with $\operatorname{ord} a \mid t$ of all the solutions to (1) is precisely the set of solutions to

$$x^{tx} \equiv 1 \pmod p, \qquad 1 \le x \le p-1. \tag{7}$$

This congruence is equivalent to

$$tx \operatorname{ind} x \equiv 0 \pmod{p-1},$$

or if we put

$$T = \frac{p-1}{t}$$

to

$$x \operatorname{ind} x \equiv 0 \pmod T,$$

or after fixing $d \mid T$ and considering only the solutions to (7) with

$$\gcd(x, T) = d,$$

they can be written as $x = dy$ and satisfy

$$\operatorname{ind}(dy) \equiv 0 \pmod{T_d}, \qquad 1 \le y \le D, \qquad \gcd(y, T_d) = 1. \tag{8}$$

where

$$T_d = \frac{T}{d} \qquad \text{and} \qquad D = \frac{p-1}{d}.$$

Let us denote by $\mathcal{Y}_d$ the set of integers y satisfying (8), and by $\mathcal{W}_d$ the set of the residue classes mod p represented by the elements of $\mathcal{Y}_d$. Obviously $\#\mathcal{Y}_d = \#\mathcal{W}_d$, and we have

$$\sum_{\substack{a \in \mathbb{Z}_p^* \\ \operatorname{ord} a \mid t}} N(p;a) = \sum_{d \mid T} \#\mathcal{Y}_d = \sum_{d \mid T} \#\mathcal{W}_d. \tag{9}$$

First note that

$$\#\left(\mathcal{W}_d + \mathcal{W}_d\right) \le \#\left(\mathcal{Y}_d + \mathcal{Y}_d\right) \le 2D \tag{10}$$

from the second condition in (8).

Furthermore, the product set of $\mathcal{W}_d$ is contained in

$$\{w \in \mathbb{Z}_p^* : \operatorname{ind}(d^2 w) \equiv 0 \pmod{T_d}\},$$

and so

$$\#\left(\mathcal{W}_d \cdot \mathcal{W}_d\right) \le \frac{p-1}{T_d} = dt. \tag{11}$$

Hence, applying Lemma 1 and using the bounds (10) and (11) we see that

$$\min\left\{p\#\mathcal{W}_d, \frac{(\#\mathcal{W}_d)^4}{p}\right\} \ll pt.$$

Hence

$$\#\mathcal{W}_d \ll \max\{t, p^{1/2}t^{1/4}\}. \tag{12}$$

Recalling the bound on the divisor function $\tau(k)$

$$\tau(k) = \sum_{d|k} 1 = k^{o(1)}, \tag{13}$$

see [5, Theorem 315], and using (12) in (9), we conclude the proof. □

Corollary 3 *Uniformly over $t \mid p-1$ and all integers a with $\gcd(a,p) = 1$ of multiplicative order $\operatorname{ord} a = t$, we have, as $p \to \infty$,*

$$N(p;a) \le \max\{t, p^{1/2}t^{1/4}\}p^{o(1)}.$$

Next we show that if t is very small then the bound of Theorem 2 can be improved. For example, this applies to the most interesting special case of the congruence (1), namely the case $a = 1$.

Theorem 4 *Uniformly over $t \mid p-1$, we have, as $p \to \infty$,*

$$\sum_{\substack{a \in \mathbb{Z}_p^* \\ \operatorname{ord} a | t}} N(p;a) \le p^{1/3+o(1)}t^{2/3}.$$

Proof. We follow the proof of Theorem 2 up to (11), but finish the argument in a different way to derive a new bound for $\#\mathcal{Y}_d$. Let us define

$$s(b) = \#\{(y_1, y_2) \ : \ y_1, y_2 \in \mathcal{Y}_d, \ y_1 y_2 \equiv b \pmod p\}.$$

First note that $s(b) > 0$ only when $b \in \mathcal{W}_d \cdot \mathcal{W}_d$, and so

$$(\#\mathcal{Y}_d)^2 = \sum_{b \in \mathbb{Z}_p} s(b) \le \# (\mathcal{W}_d \cdot \mathcal{W}_d) \max_{b \in \mathbb{Z}_p} s(b). \qquad (14)$$

If (y_1, y_2) is counted in $s(b)$ then on the one hand $y_1 y_2 \equiv b \pmod p$, on the other hand $1 \le y_1 y_2 \le D^2$ (where as before $D = (p-1)/d$), therefore $y_1 y_2 = b + kp$, where $0 \le k < \frac{p}{d^2}$. Thus the product $y_1 y_2$ can take at most $p/d^2 + 1$ possible values $y_1 y_2 = z$ and once z is fixed, there are $\tau(z) = z^{o(1)} = p^{o(1)}$ possibilities for the pair (y_1, y_2), see (13). Thus

$$s(b) \le (p/d^2 + 1) p^{o(1)},$$

which after inserting in (14) and recalling (11) yields

$$\#\mathcal{Y}_d \le \left((pt/d)^{1/2} + (td)^{1/2}\right) p^{o(1)}. \qquad (15)$$

For $d \le p^{1/3} t^{-1/3}$ we use $\#\mathcal{Y}_d \le dt$ from the first condition of (8) and for $d \ge p^{2/3} t^{-1/3}$ we use $\#\mathcal{Y}_d \le D$ from the second condition of (8). Therefore we obtain

$$\#\mathcal{Y}_d \ll p^{1/3} t^{2/3} \qquad \text{and} \qquad \#\mathcal{Y}_d \ll p^{1/3} t^{1/3},$$

respectively.

Finally, for $p^{1/3} t^{-1/3} \le d \le p^{2/3} t^{-1/3}$ we use (15) to derive

$$\#\mathcal{Y}_d \le \left(p^{1/3} t^{2/3} + p^{1/3} t^{1/3}\right) p^{o(1)} = p^{1/3 + o(1)} t^{2/3}.$$

Using these bounds with (13) in (9) we conclude the proof. □

Corollary 5 *Uniformly over $t \mid p-1$ and all integers a with $\gcd(a,p) = 1$ of multiplicative order $\operatorname{ord} a = t$, we have, as $p \to \infty$,*

$$N(p; a) \le p^{1/3 + o(1)} t^{2/3}.$$

3 Elements of Large Order

Here we use a different argument, which is similar to the one used in [1], and a bound of [2], on the number of solutions of an exponential congruence, plays the crucial role. However, this approach is effective only for values of a of sufficiently large order.

We recall the following estimate, given in [2, Lemma 7], on the number of zeros of sparse polynomials over a finite field $\mathbb{F}_q$ of q elements.

Lemma 6 *For $n \geq 2$ given elements $a_1, \ldots, a_n \in \mathbb{F}_q^*$ and integers $k_1, \ldots, k_n$ in $\mathbb{Z}$ let us denote by Q the number of solutions of the equation*

$$\sum_{i=1}^{n} a_i X^{k_i} = 0, \qquad X \in \mathbb{F}_q^*.$$

Then

$$Q \leq 2q^{1-1/(n-1)}\Delta^{1/(n-1)} + O\left(q^{1-2/(n-1)}\Delta^{2/(n-1)}\right),$$

where

$$\Delta = \min_{1\leq i\leq n} \max_{j\neq i} \gcd(k_j - k_i, q-1).$$

We are now ready to prove the main result of this section.

Theorem 7 *Uniformly over $t \mid p-1$ and all integers a with $\gcd(a,p) = 1$ of multiplicative order $\operatorname{ord} a = t$, we have, as $p \to \infty$,*

$$N(p;a) \leq p^{1+o(1)} t^{-1/12}.$$

Proof. Let a be a non-zero residue class modulo p of multiplicative order $t \mid p-1$. As before, we put

$$T = \frac{p-1}{t}$$

Clearly, there is a primitive root g modulo p with $a \equiv g^T \pmod p$. Using the discrete logarithm to base g, the congruence (1) is equivalent to

$$x \operatorname{ind} x \equiv T \pmod{p-1}.$$

Note the condition $\gcd(x, p-1) \mid T$. After fixing $d \mid T$ and considering only the solutions to (1) with $\gcd(x, p-1) = d$, they can be written as $x = dy$ and satisfy

$$y \operatorname{ind}(dy) \equiv T_d \pmod D, \quad 1 \leq y \leq D, \quad \gcd(y, D) = 1,$$

where, as before,

$$T_d = \frac{T}{d} \qquad \text{and} \qquad D = \frac{p-1}{d}.$$

Note that $t \mid D$. The congruence $yz \equiv 1 \pmod D$ defines a one–to–one correspondence between the integers $\{1 \le y \le D \ : \ \gcd(y, D) = 1\}$ and $z \in \mathbb{Z}_D^*$.

Furthermore, the relation $yz \equiv 1 \pmod D$ defines a one–to–M_d correspondence between the set $\{1 \le y \le D \ : \ \gcd(y, D) = 1\}$ and $z \in \mathbb{Z}_{p-1}^*$, where M_d is the number of residue classes in $\mathbb{Z}_{p-1}^*$ in the form $z + kD$. These residue classes are automatically coprime to D, but we have to ensure that they are coprime to d as well (and thus belong to $\mathbb{Z}_{p-1}^*$). Thus using $\mu(k)$ to denote the Möbius function, by [5, Theorem 263] (which is essentially the inclusion-exclusion principle) we obtain

$$\begin{aligned} M_d &= \sum_{k=1}^{d} \sum_{f \mid \gcd(z+kD,d)} \mu(f) = \sum_{f \mid d} \mu(f) \sum_{\substack{k=1 \\ z+kD \equiv 0 \pmod f}}^{d} 1 \\ &= \sum_{\substack{f \mid d \\ \gcd(f,D)=1}} \mu(f) \frac{d}{f} = d\,\frac{\varphi(m)}{m}, \end{aligned}$$

where $\varphi(k)$ is the Euler function and m is the product of primes q with $q \mid d$ and $q \nmid D$, see [5, Equation (16.3.1)]. In particular $m \le d \le p$ and recalling the well-known estimate on the Euler function, see [5, Theorem 328] we obtain

$$M_d = dp^{o(1)}.$$

From now on the integer $1 \le y \le D$ and the residue class $z \in \mathbb{Z}_{p-1}^*$ with or without subscripts are always connected by $yz \equiv 1 \pmod D$, even if this is not explicitly stated.

Let us define

$$\mathcal{Z}_d = \{z \in \mathbb{Z}_{p-1}^* \ : \ \mathrm{ind}\,(dy) \equiv Dz/t \pmod D, \ 1 \le y \le D\}.$$

(we recall our convention that we always have $yz \equiv 1 \pmod D$). We have

$$N(p, a) = \sum_{d \mid T} \frac{1}{M_d} \# \mathcal{Z}_d \le p^{o(1)} \sum_{d \mid T} \frac{1}{d} \# \mathcal{Z}_d. \tag{16}$$

The congruence $\operatorname{ind}(dy) \equiv Dz/t \pmod D$ is equivalent to

$$dy \equiv \rho g^{Dz/t} \pmod p,$$

for some $\rho \in \mathbb{Z}_p^*$ with $\rho^d \equiv 1 \pmod p$. Thus we split $\mathcal{Z}_d$ into subsets $\mathcal{Z}_{d,\rho}$ getting

$$\#\mathcal{Z}_d = \sum_{\rho^d \equiv 1 \pmod p} \#\mathcal{Z}_{d,\rho}, \tag{17}$$

where

$$\mathcal{Z}_{d,\rho} = \{z \in \mathbb{Z}_{p-1}^* \ : \ dy \equiv \rho g^{Dz/t} \pmod p, \ 1 \le y \le D\}$$

(and again we recall our convention that $yz \equiv 1 \pmod D$).

Clearly,

$$(\#\mathcal{Z}_{d,\rho})^2 = \#\{z_1, z_2 \in \mathbb{Z}_{p-1}^* \ : \ dy_j \equiv \rho g^{Dz_j/t} \pmod p, \ j = 1, 2\}.$$

We have by adding the two congruences that

$$\begin{aligned}(\#\mathcal{Z}_{d,\rho})^2 & \\ \le \#\{z_1, z_2 \in \mathbb{Z}_{p-1}^* \ &: \ d(y_1+y_2) \equiv \rho\left(g^{Dz_1/t} + g^{Dz_2/t}\right) \pmod p\} \\ = \sum_{v \in \mathbb{Z}} \#\{z_1, z_2 \in \mathbb{Z}_{p-1}^* \ &: \ d(y_1+y_2) = v, \\ & \rho\left(g^{Dz_1/t} + g^{Dz_2/t}\right) \equiv v \pmod p\}.\end{aligned}$$

The sum over $v \in \mathbb{Z}$ is empty unless $v = dw$, where $2 \le w \le 2D$ and we get by the Cauchy–Schwarz inequality that

$$\begin{aligned}(\#\mathcal{Z}_{d,\rho})^4 \le 2D\#\{z_1, z_2, z_3, z_4 \in \mathbb{Z}_{p-1}^* \ &: \ d(y_1+y_2) = d(y_3+y_4) \\ \equiv \rho\left(g^{Dz_1/t} + g^{Dz_2/t}\right) &\equiv \rho\left(g^{Dz_3/t} + g^{Dz_4/t}\right) \pmod p\}.\end{aligned}$$

Clearly, when $z_1, z_2, z_3, z_4 \in \mathbb{Z}_{p-1}^*$ are fixed, then the condition

$$\begin{aligned}d(y_1+y_2) &= d(y_3+y_4) \\ &\equiv \rho\left(g^{Dz_1/t} + g^{Dz_2/t}\right) \equiv \rho\left(g^{Dz_3/t} + g^{Dz_4/t}\right) \pmod p\end{aligned}$$

defines ρ uniquely. Hence

$$\begin{aligned}\sum_{\rho^d \equiv 1 \pmod p} (\#\mathcal{Z}_{d,\rho})^4 & \\ \le 2D\#\{z_1, z_2, z_3, z_4 \in \mathbb{Z}_{p-1}^* \ &: \ y_1 + y_2 = y_3 + y_4, \\ & g^{Dz_1/t} + g^{Dz_2/t} \equiv g^{Dz_3/t} + g^{Dz_4/t} \pmod p\}.\end{aligned}$$

Relaxing the condition $y_1+y_2=y_3+y_4$ to $y_1+y_2\equiv y_3+y_4 \pmod D$ only increases the number of solution (but allows us to think about y_j as a residue class modulo D defined by $y_jz_j\equiv 1 \pmod D$, $j=1,2,3,4$). Thus

$$\sum_{\rho^d\equiv 1 \pmod p} (\#\mathcal{Z}_{d,\rho})^4 \le 2D\#\{z_1,z_2,z_3,z_4\in \mathbb{Z}_{p-1}^* \ :\ y_1+y_2\equiv y_3+y_4 \pmod D,\ g^{Dz_1/t}+g^{Dz_2/t}\equiv g^{Dz_3/t}+g^{Dz_4/t} \pmod p\}.$$

Finally, after the substitution $z_j\to wz_j$ for $w\in\mathbb{Z}_{p-1}^*$ (and thus $y_j\to w^{-1}y_j$), $j=1,2,3,4$, where w^{-1} is defined modulo D, we obtain that any solution is computed with $\varphi(p-1)$ multiplicity, that is

$$\sum_{\rho^d\equiv 1 \pmod p} (\#\mathcal{Z}_{d,\rho})^4 \le \frac{2D}{\varphi(p-1)}\#\{z_1,z_2,z_3,z_4,w\in \mathbb{Z}_{p-1}^* \ :\ y_1+y_2\equiv y_3+y_4 \pmod D,\ (g^w)^{Dz_1/t}+(g^w)^{Dz_2/t}\equiv (g^w)^{Dz_3/t}+(g^w)^{Dz_4/t} \pmod p\}. \qquad (18)$$

Writing $X\equiv g^w \pmod p$ and $k_j=Dz_j/t=(p-1)z_j/dt=T_dz_j$, after fixing z_1,z_2,z_3,z_4, the number of $w\in\mathbb{Z}_{p-1}^*$ satisfying the congruence in (18) is bounded by the number of solutions to the congruence $X^{k_1}+X^{k_2}\equiv X^{k_3}+X^{k_4} \pmod p$, and this is bounded in Lemma 6, applied with $n=4$, by $O\left(p^{2/3}\Delta^{1/3}\right)$, where

$$\Delta = \min_{1\le i<j\le 4}\gcd\left(T_d(z_i-z_j),p-1\right) = T_d\min_{1\le i<j\le 4}\gcd\left(z_i-z_j,dt\right).$$

For every fixed i,j, $1\le i<j\le 4$ and $\delta\mid dt$ there are $(p-1)^2/\delta$ choices for (z_i,z_j) with

$$\gcd(z_i-z_j,dt)=\delta.$$

When z_i and z_j are fixed the congruence $y_1+y_2\equiv y_3+y_4 \pmod D$ implies that there are $dp^{1+o(1)}$ choices for the remaining two variables. (Recall that each y determines $M_d=dp^{o(1)}$ different choices of z.) Thus, putting everything together in (18) and recalling (13), we obtain

$$\sum_{\rho^d\equiv 1 \pmod p} (\#\mathcal{Z}_{d,\rho})^4 \le \frac{2D}{\varphi(p-1)}\sum_{\delta\mid dt} p^{2/3}(T_d\delta)^{1/3}\frac{(p-1)^2}{\delta}dp^{1+o(1)}$$
$$= dDp^{8/3+o(1)}T_d^{1/3}\sum_{\delta\mid dt}\delta^{-2/3} = p^{11/3+o(1)}T_d^{1/3} = \frac{p^{4+o(1)}}{(dt)^{1/3}}.$$

Putting this to (17), we get by the Hölder inequality

$$\#\mathcal{Z}_d \le d^{3/4}\left(\sum_{\rho^d\equiv 1 \pmod p} (\#\mathcal{Z}_{d,\rho})^4\right)^{1/4} \le \frac{p^{1+o(1)}}{t^{1/12}}\, d^{2/3}.$$

Finally (16) and (13) gives

$$N(p,a) \le \sum_{d|(p-1)/t} \frac{p^{1+o(1)}}{t^{1/12}d^{1/3}} \le \frac{p^{1+o(1)}}{t^{1/12}},$$

and we conclude the proof. □

4 Symmetric Congruence

We now improve the bound (6) on the number of solutions to the symmetric congruence (3).

Theorem 8 *We have, as $p \to \infty$.*

$$M(p) \le p^{48/25+o(1)}.$$

Proof. From (4) we obtain

$$M(p) \le \sum_{t|p-1} \sum_{\substack{a\in\mathbb{Z}_p^* \\ \mathrm{ord}\, a=t}} N(p;a)^2.$$

We fix some parameter ϑ and for $t \le \vartheta$ we use Theorem 2 to estimate

$$\begin{aligned}\sum_{\substack{a\in\mathbb{Z}_p^* \\ \mathrm{ord}\, a=t}} N(p;a)^2 &\le \left(\sum_{\substack{a\in\mathbb{Z}_p^* \\ \mathrm{ord}\, a=t}} N(p;a)\right)^2 \\ &\le \max\{t^2p^{o(1)}, p^{1+o(1)}t^{1/2}\} \le \max\{\vartheta^2p^{o(1)}, p^{1+o(1)}\vartheta^{1/2}\}.\end{aligned}$$

For $t \ge \vartheta$ we use Theorem 7 together with (5) to estimate

$$\sum_{\substack{a\in\mathbb{Z}_p^* \\ \mathrm{ord}\, a=t}} N(p;a)^2 \le p^{1+o(1)}t^{-1/12} \sum_{\substack{a\in\mathbb{Z}_p^* \\ \mathrm{ord}\, a=t}} N(p;a) \le p^{2+o(1)}\vartheta^{-1/12}.$$

Taking

$$\vartheta = p^{24/25}$$

to balance the above estimates, we obtain the bound

$$\sum_{\substack{a \in \mathbb{Z}_p^* \\ \mathrm{ord}\, a = t}} N(p;a)^2 \le p^{48/25+o(1)}$$

and using (13), we conclude the proof. □

5 Concluding Remarks

Clearly Theorem 2 is nontrivial provided that $t \le p^{1-\varepsilon}$ for some $\varepsilon > 0$, while Theorem 7 is nontrivial provided $t \ge p^{\varepsilon}$, for an arbitrary $\varepsilon > 0$ and a sufficiently large p. In particular, using Corollary 3 for $t \le p^{12/13}$ and Theorem 7 for $t > p^{12/13}$, we derive (2).

It is also easy to see that all but $o(p)$ elements $a \in \mathbb{Z}_p^*$ are of multiplicative order $t = p^{1+o(1)}$. Thus for almost all $a \in \mathbb{Z}_p^*$ we have $N(p;a) \le p^{11/12+o(1)}$ by Theorem 7.

Similar results can also be established for several other congruences. For example, the same arguments as those used in the proof of Theorem 4 imply that the congruence

$$x^{x-1} \equiv 1 \pmod p, \qquad 1 \le x \le p-1,$$

has $O\left(p^{1/3+o(1)}\right)$ solutions. This means that the function $x \mapsto x^x \pmod p$ has $O(p^{1/3+o(1)})$ fixed points in the interval $1 \le x \le p-1$.

Acknowledgements

Research of A. B. was supported in part by Hungarian National Science Foundation Grants K72731 and K81658 and that of I. S. was supported in part by Australia Research Council Grants DP0556431 and DP0881473.

References

[1] J. Bourgain and I. E. Shparlinski, 'Distribution of consecutive modular roots of an integer', *Acta Arith.*, **134** (2008), 83–91.

[2] R. Canetti, J. B. Friedlander, S. V. Konyagin, M. Larsen, D. Lieman and I. E. Shparlinski, 'On the statistical properties of Diffie–Hellman distributions', *Israel J. Math.*, **120** (2000), 23–46.

[3] R. Crocker, 'On residues of n^n', *Amer. Math. Monthly*, **76** (1969), 1028–1029.

[4] M. Z. Garaev, 'The sum-product estimate for large subsets of prime fields', *Proc. Amerc. Math. Soc.*, **136** (2008), 2735–2739.

[5] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Oxford, 1979.

[6] J. Holden, 'Fixed points and two cycles of the discrete logarithm', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2369** (2002), 405–416.

[7] J. Holden and P. Moree, 'New conjectures and results for small cycles of the discrete logarithm', *High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams*, Fields Institute Communications, vol.41, Amer. Math. Soc., 2004, 245–254.

[8] J. Holden and P. Moree, 'Some heuristics and and results for small cycles of the discrete logarithm', *Math. Comp.*, **75** (2006), 419–449.

[9] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of applied cryptography*, CRC Press, Boca Raton, FL, 1996.