ACTA ARITHMETICA
148.1 (2011)

On the number of solutions of exponential congruences

by

Antal Balog (Budapest), Kevin A. Broughan (Hamilton) and
Igor E. Shparlinski (Sydney)

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 results of Crocker [3] and Somer [10] showing that there are at least $\lfloor\sqrt{(p-1)/2}\rfloor$ and at most $3p/4 + O(p^{1/2+o(1)})$, respectively, incongruent values of $x^x \pmod{p}$ when $1 \le x \le p-1$, little has been 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. We note that the function x^x is periodic modulo p with period $p(p-1)$, which is much larger than the range of x in the congruence (1) and which explains why it is so difficult to study.

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

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

2010 *Mathematics Subject Classification*: Primary 11B50.
Key words and phrases: congruences, sum-product problem.

DOI: 10.4064/aa148-1-7

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 modulo $p-1$ 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

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

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 the nonzero residue classes x satisfying (1) with $\operatorname{ord} a \mid t$ is precisely the set of solutions to

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

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 seen to satisfy

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

where

$$T_d = \frac{T}{d}, \quad D = \frac{p-1}{d}.$$

Let us denote by $\mathcal{Y}_d$ the set of integers y satisfying (8), and by $\mathcal{W}_d$ the set of residue classes modulo 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

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

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

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

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

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

Therefore

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

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

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

(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* $p \to \infty$,

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

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

$$s(b) = \#\{(y_1,y_2) : y_1, y_2 \in \mathcal{Y}_d,\ y_1y_2 \equiv b \pmod{p}\}.$$

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

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

If (y_1,y_2) is counted in $s(b)$ then on the one hand $y_1y_2 \equiv b \pmod{p}$, on the other hand $1 \le y_1y_2 \le D^2$ (where as before $D = (p-1)/d$), therefore $y_1y_2 = b + kp$, where $0 \le k < p/d^2$. Thus the product y_1y_2 can take at most p/d^2+1 possible values $y_1y_2 = z$ 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

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

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

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

respectively.

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

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

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 $n \ge 2$ given elements $a_1, \dots, a_n \in \mathbb{F}_q^*$ and integers $k_1, \dots, k_n$ 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

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

where

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

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 $p \to \infty$,*

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

Proof. Let a be a nonzero 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

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

where, as before,

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

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 $\mathbb{Z}_{p-1}^*$ of 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

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

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

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

The congruence $\mathrm{ind}(dy) \equiv Dz/t \pmod D$ 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 deduce by adding the two congruences that

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

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

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

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

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

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 solutions (but allows us to think about y_j as a residue class modulo D defined by $y_j z_j \equiv 1 \pmod D$, $j = 1, 2, 3, 4$). Thus

$$\sum_{\rho^d \equiv 1 \pmod p} (\#\mathcal{Z}_{d,\rho})^4 \le 2DT$$

where

$$T = \#\{z_1, z_2, z_3, z_4 \in \mathbb{Z}_{p-1}^* : y_1 + y_2 \equiv y_3 + y_4 \pmod D,\\ g^{Dz_1/t} + g^{Dz_2/t} \equiv g^{Dz_3/t} + g^{Dz_4/t} \pmod p\}.$$

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

$$\sum_{\rho^d \equiv 1 \pmod p} (\#\mathcal{Z}_{d,\rho})^4 \le \frac{2D}{\varphi(p-1)} \widetilde{T} \tag{18}$$

where

$$\widetilde{T} = \#\{z_1, z_2, z_3, z_4, w \in \mathbb{Z}_{p-1}^* : y_1 + y_2 \equiv y_3 + y_4 \pmod D,\\ (g^w)^{Dz_1/t} + (g^w)^{Dz_2/t} \equiv (g^w)^{Dz_3/t} + (g^w)^{Dz_4/t} \pmod p\}.$$

Writing $X \equiv g^w \pmod p$ and $k_j = Dz_j/t = (p-1)z_j/dt = T_d z_j$, 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 $O(p^{2/3}\Delta^{1/3})$, where

$$\begin{aligned}\Delta &= \min_{1\le i\le 4} \max_{\substack{1\le j\le 4\\ j\ne i}} \gcd(T_d(z_i - z_j), p-1)\\ &= T_d \min_{1\le i<j\le 4} \max_{\substack{1\le j\le 4\\ j\ne i}} \gcd(z_i - z_j, dt).\end{aligned}$$

For every fixed $i \ne j$, $1 \le i, j \le 4$ 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

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

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

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

Finally (16) and (13) give

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

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

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

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

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

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

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

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 $O(p^{1/3+o(1)})$ 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. Amer. Math. Soc. 136 (2008), 2735–2739.

[5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford Univ. Press, Oxford, 1979.

[6] J. Holden, *Fixed points and two-cycles of the discrete logarithm*, in: Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci. 2369, Springer, Berlin, 2002, 405–415.

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

[8] —, —, *Some heuristics 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, 1997.

[10] L. Somer, *The residues of n^n modulo p*, Fibonacci Quart. 19 (1981), 110–117.

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

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

Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
E-mail: igor.shparlinski@mq.edu.au

Received on 10.6.2010
and in revised form on 17.11.2010 (6415)