ACTA ARITHMETICA
124.1 (2006)

On the logarithmic factor in error term estimates in certain additive congruence problems

by

M. Z. Garaev (Morelia)

1. Introduction. In additive number theory an important topic is the problem of finding an asymptotic formula for the number of solutions of a given congruence. In many additive congruences the error term estimates of asymptotic formulas contain logarithmic factors. The aim of the present paper is to illustrate application of double exponential sums and a multidimensional smoothing argument in removing these factors for a class of additive problems.

Let g be a primitive root modulo an odd prime number p and let K, N and M be any integers with $1 \le K, N < p$. We start by recalling the well known formula of Montgomery [6]:

$$J = \frac{KN}{p} + O(p^{1/2} \log^2 p), \tag{1}$$

where J denotes the number of integers $x \in [H+1, H+K]$ such that $g^x \in [M+1, M+N]$. In this paper we establish the following statement.

Theorem 1. *The following estimate holds*:

$$J - \frac{KN}{p} \ll p^{1/2} \log^2(KNp^{-3/2} + 2). \tag{2}$$

We recall that the notations $A \ll B$ and $A = O(B)$ are both equivalent to $|A| \le cB$ for some absolute positive constant c.

Estimate (2) gives the asymptotic formula $J \sim KN/p$ in the range

$$KNp^{-3/2} \to \infty \quad \text{as } p \to \infty,$$

while formula (1) gives the same asymptotic formula when

$$KNp^{-3/2} \log^{-2} p \to \infty \quad \text{as } p \to \infty.$$

Moreover, if $KN \ll p^{3/2}$, then our estimate guarantees the bound $J \ll p^{1/2}$, while formula (1) provides the bound $J \ll p^{1/2} \log^2 p$. Also note that

2000 *Mathematics Subject Classification*: 11A07, 11L03.

estimate (2) improves (1) in the range $KN \le p^{3/2+o(1)}$ and coincides with (1) for larger values of KN.

The method that we use to prove Theorem 1 is applicable to a class of other well known additive problems. For a given integer $h \not\equiv 0 \pmod p$, denote by J_1 the number of solutions of the congruence

$$g^x - g^y \equiv h \pmod p, \qquad 1 \le x, y \le N.$$

In [7] (see also [10]) the asymptotic formula

$$J_1 = \frac{N^2}{p} + O(p^{1/2} \log^2 p) \tag{3}$$

has been established. In the present paper we prove

THEOREM 2. *The following estimate holds*:

$$J_1 - \frac{N^2}{p} \ll N^{2/3} \log^{2/3}(Np^{-3/4} + 2) + p^{1/2}.$$

We see that Theorem 2 provides the asymptotic formula $J_1 \sim N^2/p$ in the range

$$Np^{-3/4} \to \infty \qquad \text{as } p \to \infty,$$

while (3) gives the same asymptotic formula when

$$Np^{-3/4} \log^{-2} p \to \infty \qquad \text{as } p \to \infty.$$

We mention that in a series of recent works it has been proved that any residue class $h \pmod p$ is representable in the form

$$h \equiv g^x - g^y \pmod p, \qquad 1 \le x, y \le cp^{3/4},$$

for a suitably chosen constant c (see [2, 5, 9]). In [3] it is shown that one can take $c = 2^{5/4}$.

The following result has been obtained in [8]:

Let $\mathcal{U}, \mathcal{V} \subset \{0, 1, \ldots, p-1\}$ *with* u *and* v *elements respectively*, *and let* S *and* T *be any integers with* $1 \le T \le p$. *If* J_2 *denotes the number of solutions of the congruence*

$$xy \equiv z \pmod p, \qquad x \in \mathcal{U},\ y \in \mathcal{V},\ S+1 \le z \le S+T,$$

then

$$\left| J_2 - \frac{uvT}{p} \right| < 2(puv)^{1/2} \log p. \tag{4}$$

Our approach leads to

THEOREM 3. *The following estimate holds*:

$$J_2 - \frac{uvT}{p} \ll (puv)^{1/2} \log(uvT^2p^{-3} + 2).$$

From Theorem 3 we derive the asymptotic formula $J_2 \sim uvT/p$ under the condition

$$uvT^2p^{-3} \to \infty \qquad \text{as } p \to \infty,$$

while estimate (4) gives the same formula only when

$$uvT^2p^{-3}\log^{-2} p \to \infty \qquad \text{as } p \to \infty.$$

We remark that estimate (4) (even with constant 2 on the right hand side replaced by 1) is a consequence of the Vinogradov double exponential sum estimate (see Lemma 5 below) and the inequality

$$\sum_{a=1}^{p-1}\Big|\sum_{n=S+1}^{S+T} e^{2\pi ian/p}\Big| < p^{1/2}\log p$$

(see, for example, the proof of Lemma 5 in [4, p. 109]).

THEOREM 4. *Let $h \not\equiv 0 \pmod p$ and let J_3 denote the number of solutions of the congruence*

$$xy \equiv h \pmod p, \qquad 1 \le x, y \le N.$$

Then

$$J_3 - \frac{N^2}{p} \ll p^{1/2}\log^2(Np^{-3/4} + 2).$$

In particular, the asymptotic formula $J_3 \sim N^2/p$ holds when $Np^{-3/4} \to \infty$ as $p \to \infty$. In passing we remark that the argument of our paper can be used in a series of other related problems.

For more information on very recent results on distribution properties of special sequences related to our paper we refer the reader to [1]–[3], [5], [7], [9], [10] and references therein.

2. Lemmas

LEMMA 5. *Let m be a positive integer, and let a be an integer coprime to m. Then*

$$\Big|\sum_{x=0}^{m-1}\sum_{y=0}^{m-1} \nu(x)\varrho(y)e^{2\pi iaxy/m}\Big| \le \sqrt{mXY}$$

for any complex numbers $\nu(x), \varrho(y)$ with

$$\sum_{x=0}^{m-1} |\nu(x)|^2 = X, \qquad \sum_{y=0}^{m-1} |\varrho(y)|^2 = Y.$$

The proof of this lemma can be found in [11, p. 142].

LEMMA 6. *Let L_1, L_2, A, B and m be any integers, $1 \le A, B \le m$. Then*

$$W := \sum_{a=0}^{m-1} \Big| \sum_{x=L_1+1}^{L_1+A} e^{2\pi i a x/m} \Big| \Big| \sum_{y=L_2+1}^{L_2+B} e^{2\pi i a y/m} \Big| \ll mA \log(BA^{-1}+2).$$

Proof. If $A \ge B$, then applying the Cauchy inequality we obtain

$$W^2 \le \sum_{a=0}^{m-1} \Big| \sum_{x=L_1+1}^{L_1+A} e^{2\pi i a x/m} \Big|^2 \sum_{a=0}^{m-1} \Big| \sum_{y=L_2+1}^{L_2+B} e^{2\pi i a y/m} \Big|^2 = m^2 AB \le m^2 A^2,$$

whence the result.

Let $A < B$. Then

$$W \le 2W_1 + 2W_2 + 2W_3,$$

where

$$W_1 = \sum_{0 \le a \le m/B} \Big| \sum_{x=L_1+1}^{L_1+A} e^{2\pi i a x/m} \Big| \Big| \sum_{y=L_2+1}^{L_2+B} e^{2\pi i a y/m} \Big|,$$

$$W_2 = \sum_{m/B < a \le \min\{m/A, m/2\}} \Big| \sum_{x=L_1+1}^{L_1+A} e^{2\pi i a x/m} \Big| \Big| \sum_{y=L_2+1}^{L_2+B} e^{2\pi i a y/m} \Big|,$$

$$W_3 = \sum_{\min\{m/A, m/2\} < a \le m/2} \Big| \sum_{x=L_1+1}^{L_1+A} e^{2\pi i a x/m} \Big| \Big| \sum_{y=L_2+1}^{L_2+B} e^{2\pi i a y/m} \Big|.$$

The trivial estimate shows

$$W_1 \ll (m/B)AB \le mA.$$

To estimate W_2 we recall that for $1 \le a \le m/2$,

$$\Big| \sum_{y=L_2+1}^{L_2+B} e^{2\pi i a y/m} \Big| \ll \frac{m}{a}.$$

Then, estimating the sum over x trivially, we obtain

$$W_2 \ll A \sum_{m/B < a \le m/A} \frac{m}{a} \ll mA \log(BA^{-1}+2).$$

Finally, for W_3 we have

$$W_3 \ll \sum_{a > m/A} \frac{m^2}{a^2} \ll mA.$$

Therefore, $W \ll mA \log(BA^{-1}+2)$. ∎

LEMMA 7. *Let L_1, L_2, A, B be any integers with $1 \le A, B \le p-1$. Then for any integer a with $(a,p)=1$,*

$$I := \Big|\sum_{x=L_1+1}^{L_1+A}\sum_{y=L_2+1}^{L_2+B} e^{2\pi i a g^{x+y}/p}\Big| \ll p^{1/2} A \log(BA^{-1}+2).$$

The same estimate holds if in the exponent the function g^{x+y} is replaced by g^{x-y}.

Proof. Applying the smoothing argument, we obtain

$$\begin{aligned} I &= \frac{1}{p-1}\Big|\sum_{b=0}^{p-2}\sum_{x=L_1+1}^{L_1+A}\sum_{y=L_2+1}^{L_2+B}\sum_{z=1}^{p-1} e^{2\pi i a g^z/p} e^{2\pi i b(x+y-z)/(p-1)}\Big| \\ &\le \frac{1}{p-1}\sum_{b=0}^{p-2}\Big|\sum_{z=1}^{p-1} e^{2\pi i a g^z/p} e^{-2\pi i b z/(p-1)}\Big|\Big|\sum_{x=L_1+1}^{L_1+A}\sum_{y=L_2+1}^{L_2+B} e^{2\pi i b(x+y)/(p-1)}\Big|. \end{aligned}$$

The sum over z is a Gauss sum, so its absolute value is equal to $p^{1/2}$ for any integer $b \not\equiv 0 \pmod{(p-1)}$ and is equal to 1 for $b \equiv 0 \pmod{(p-1)}$. Thus,

$$\begin{aligned} I &\ll p^{-1/2}\sum_{b=0}^{p-2}\Big|\sum_{x=L_1+1}^{L_1+A} e^{2\pi i b x/(p-1)}\Big|\Big|\sum_{y=L_2+1}^{L_2+B} e^{2\pi i b y/(p-1)}\Big| \\ &\ll p^{1/2} A \log(BA^{-1}+2), \end{aligned}$$

where we have also used Lemma 6 with $m = p-1$.

The estimate of the sum with g^{x-y} in the exponent instead of g^{x+y} is completely analogous. ■

3. Proof of Theorem 1. If $N > p/2$ then J is equal to K minus the number of integers x for which

$$H+1 \le x \le H+K, \quad g^x \in [M+N+1, M+p] \pmod{p},$$

where now $p-N < p/2$. For this reason it is sufficient to consider the case $N < p/2$. By the same argument we may suppose that $K < p/2$. Also note that if $K \le 10$ or $N \le 10$, then the estimate becomes trivial, since in this case we have $J \le 10$. Therefore, we may assume that $10 \le K, N < p/2$.

Let K_1, N_1 be some positive integers with $K_1 < K$ and $N_1 < N$. Denote by J' the number of solutions of the congruence

$$g^{x+z} \equiv y + t \pmod{p}$$

subject to the conditions

$$\begin{aligned} H+1 &\le x \le H+(K-K_1), & 1 &\le z \le K_1, \\ M+1 &\le y \le M+(N-N_1), & 1 &\le t \le N_1. \end{aligned}$$

It is obvious that for fixed integers z and t the corresponding number of solutions of the above congruence (in variables x and y) is not greater than J. Therefore,

$$J \geq \frac{J'}{K_1 N_1}. \tag{5}$$

Similarly, let J'' be the number of solutions to the congruence

$$g^{x-z} \equiv y - t \pmod p$$

subject to the conditions

$$\begin{aligned} H+1 \leq x \leq H+K+K_1, &\qquad 1 \leq z \leq K_1, \\ M+1 \leq y \leq M+N+N_1, &\qquad 1 \leq t \leq N_1. \end{aligned}$$

Then we have

$$J \leq \frac{J''}{K_1 N_1}. \tag{6}$$

We claim that

$$\frac{J'}{K_1 N_1} - \frac{KN}{p} \ll p^{1/2} \log^2(KNp^{-3/2} + 2)$$

and

$$\frac{J''}{K_1 N_1} - \frac{KN}{p} \ll p^{1/2} \log^2(KNp^{-3/2} + 2)$$

for some K_1, N_1. To prove it we express J' by means of trigonometric sums:

$$J' = \frac{1}{p} \sum_{a=0}^{p-1} \sum_{x=H+1}^{H+K-K_1} \sum_{z=1}^{K_1} \sum_{y=M+1}^{M+N-N_1} \sum_{t=1}^{N_1} e^{2\pi i a (g^{x+z} - y - t)/p}.$$

Isolating the term corresponding to $a = 0$ we find

$$\begin{aligned} J' = & \frac{K_1 N_1 (K - K_1)(N - N_1)}{p} \\ & + \frac{1}{p} \sum_{a=1}^{p-1} \sum_{x=H+1}^{H+K-K_1} \sum_{z=1}^{K_1} \sum_{y=M+1}^{M+N-N_1} \sum_{t=1}^{N_1} e^{2\pi i a (g^{x+z} - y - t)/p}. \end{aligned}$$

For $1 \leq a \leq p-1$ we have, according to Lemma 7,

$$\Big| \sum_{x=H+1}^{H+K-K_1} \sum_{z=1}^{K_1} e^{2\pi i a g^{x+z}/p} \Big| \ll p^{1/2} K_1 \log(KK_1^{-1} + 2).$$

Therefore,

$$J' - \frac{K_1N_1(K-K_1)(N-N_1)}{p} \ll p^{-1/2}K_1\log(KK_1^{-1}+2)\sum_{a=1}^{p-1}\Big|\sum_{y=M+1}^{M+N-N_1} e^{2\pi iay/p}\Big|\,\Big|\sum_{t=1}^{N_1} e^{2\pi iat/p}\Big|.$$

According to Lemma 6 the sum over a is $\ll pN_1\log(NN_1^{-1}+2)$. Hence,

$$J' - \frac{K_1N_1(K-K_1)(N-N_1)}{p} \ll p^{1/2}K_1N_1\log(KK_1^{-1}+2)\log(NN_1^{-1}+2),$$

whence

$$\frac{J'}{K_1N_1} = \frac{(K-K_1)(N-N_1)}{p} + O(p^{1/2}\log(KK_1^{-1}+2)\log(NN_1^{-1}+2)). \tag{7}$$

If $KN < 100p^{3/2}$, then we choose $K_1 = [K/2]$, $N_1 = [N/2]$ and obtain

$$\frac{J'}{K_1N_1} = O(p^{1/2}) = \frac{KN}{p} + O(p^{1/2}\log^2(KNp^{-3/2}+2)).$$

If $KN > 100p^{3/2}$, then we put

$$V = KNp^{-3/2}\log^{-2}(KNp^{-3/2}),$$

and observe that $2<V\le\min\{K,N\}$. Thus, we can choose K_1 and N_1 to be

$$K_1 = [K/V], \qquad N_1 = [N/V].$$

Therefore, from (7) we obtain

$$\frac{J'}{K_1N_1} - \frac{KN}{p} \ll \frac{KN}{pV} + p^{1/2}\log^2 V \ll p^{1/2}\log^2(KNp^{-3/2}).$$

Thus, in both cases we have

$$\frac{J'}{K_1N_1} - \frac{KN}{p} \ll p^{1/2}\log^2(KNp^{-3/2}+2),$$

whence, in view of (5), we deduce the bound

$$J \ge \frac{KN}{p} + O(p^{1/2}\log^2(KNp^{-3/2}+2)). \tag{8}$$

The above argument applied to J'' leads to

$$\frac{J''}{K_1N_1} - \frac{KN}{p} \ll p^{1/2}\log^2(KNp^{-3/2}+2),$$

which, due to (6), implies

$$J \le \frac{KN}{p} + O(p^{1/2}\log^2(KNp^{-3/2}+2)). \tag{9}$$

The result now follows from (8) and (9). ∎

4. Proof of Theorem 2. We may suppose that $N > 10$ and also, due to (3) for example, that $N < p/2$.

Let N_1 be a positive integer to be chosen later, $N_1 \le N/4$. Denote by J_1' the number of solutions of the congruence

$$g^{x+z} - g^y \equiv hg^{-t} \pmod p$$

subject to the conditions

$$1 \le x \le N - 2N_1, \quad 1 \le z \le N_1, \quad 1 \le y \le N - N_1, \quad 1 \le t \le N_1.$$

Let J_1'' denote the number of solutions of the congruence

$$g^{x-z} - g^y \equiv hg^{t} \pmod p$$

subject to the conditions

$$1 \le x \le N + 2N_1, \quad 1 \le z \le N_1, \quad 1 \le y \le N + N_1, \quad 1 \le t \le N_1.$$

Then

$$\frac{J_1'}{N_1^2} \le J_1 \le \frac{J_1''}{N_1^2}. \tag{10}$$

We express J_1' in terms of trigonometric sums and obtain

$$J_1' = \frac{1}{p}\sum_{a=0}^{p-1}\sum_{x=1}^{N-2N_1}\sum_{z=1}^{N_1}\sum_{y=1}^{N-N_1}\sum_{t=1}^{N_1} e^{2\pi i a(g^{x+z} - g^y - hg^{-t})/p}.$$

Isolating the term corresponding to $a = 0$ and applying Lemma 7 to the sum over x and z, we deduce

$$\frac{J_1'}{N_1^2} - \frac{(N-2N_1)(N-N_1)}{p} \ll p^{-1/2}N_1^{-1}\log(NN_1^{-1}+2)\sum_{a=1}^{p-1}\Big|\sum_{y=1}^{N-N_1} e^{2\pi i a g^y/p}\Big|\Big|\sum_{t=1}^{N_1} e^{2\pi i a h g^{-t}/p}\Big|.$$

Application of the Cauchy inequality yields

$$\sum_{a=1}^{p-1}\Big|\sum_{y=1}^{N-N_1} e^{2\pi i a g^y/p}\Big|\Big|\sum_{t=1}^{N_1} e^{2\pi i a h g^{-t}/p}\Big| \ll \Big(\sum_{a=0}^{p-1}\Big|\sum_{y=1}^{N-N_1} e^{2\pi i a g^y/p}\Big|^2\Big)^{1/2}\Big(\sum_{a=0}^{p-1}\Big|\sum_{t=1}^{N_1} e^{2\pi i a h g^{-t}/p}\Big|^2\Big)^{1/2} \le pN^{1/2}N_1^{1/2}.$$

Hence,

$$\frac{J_1'}{N_1^2} - \frac{N^2}{p} \ll \frac{NN_1}{p} + p^{1/2}N^{1/2}N_1^{-1/2}\log(NN_1^{-1}+2). \tag{11}$$

If $N < 100p^{3/4}$ then we let $N_1 = [N/4]$ and obtain

$$\frac{J_1'}{N_1^2} = O(p^{1/2}) = \frac{N^2}{p} + O(N^{2/3}\log^{2/3}(Np^{-3/4}+2) + p^{1/2}).$$

If $N > 100p^{3/4}$, then we define

$$V = N^{4/3}p^{-1}\log^{-2/3}(Np^{-3/4})$$

and observe that $4 \le V \le N$. Now put $N_1 = [N/V]$ and observe that in this case from (11) we again have

$$\frac{J_1'}{N_1^2} = \frac{N^2}{p} + O(N^{2/3}\log^{2/3}(Np^{-3/4}+2) + p^{1/2}).$$

Thus, for the N_1 chosen the above asymptotic formula holds, and hence due to (10) we have

$$J_1 \ge \frac{N^2}{p} + O(N^{2/3}\log^{2/3}(Np^{-3/4}+2) + p^{1/2}).$$

Analogously,

$$\frac{J_1''}{N_1^2} = \frac{N^2}{p} + O(N^{2/3}\log^{2/3}(Np^{-3/4}+2) + p^{1/2}),$$

whence, in view of (10),

$$J_1 \le \frac{N^2}{p} + O(N^{2/3}\log^{2/3}(Np^{-3/4}+2) + p^{1/2}).$$

Therefore,

$$J_1 = \frac{N^2}{p} + O(N^{2/3}\log^{2/3}(Np^{-3/4}+2) + p^{1/2})$$

and the result follows. ∎

5. Proof of Theorem 3. We remark that if $T \le 10$, then the statement follows from the trivial estimates $J_2 \le 10u,\ J_2 \le 10v$ and the fact that the error term in this case dominates. Furthermore, without loss of generality we may assume that $T < p/2$.

Let $T_1 \le T/2$ be an integer to be chosen later. Denote by J_2' the number of solutions of the congruence

$$xy \equiv z + t \pmod{p}$$

subject to the conditions

$$x \in \mathcal{U}, \quad y \in \mathcal{V}, \quad S+1 \le z \le S+T-T_1, \quad 1 \le t \le T_1.$$

Let J_2'' denote the number of solutions of the congruence

$$xy \equiv z - t \pmod{p}$$

subject to the conditions

$$x \in \mathcal{U}, \quad y \in \mathcal{V}, \quad S+1 \le z \le S+T+T_1, \quad 1 \le t \le T_1.$$

Then

$$\frac{J_2'}{T_1} \le J_2 \le \frac{J_2''}{T_1}. \tag{12}$$

Expressing J_2' via trigonometric sums, isolating the main term, applying Lemma 5 to the double sum over $x \in \mathcal{U}$, $y \in \mathcal{V}$, and Lemma 6 to the double sum over z and t, and following exactly the same lines of the proofs of Theorems 1 and 2, we obtain

$$\frac{J_2'}{T_1} - \frac{uvT}{p} \ll \frac{uvT_1}{p} + (puv)^{1/2} \log(TT_1^{-1} + 2).$$

If $T^2uv < 10000p^3$, then we put $T_1 = [T/2]$, and in this case obtain

$$\frac{J_2'}{T_1} = O((puv)^{1/2}) = \frac{uvT}{p} + O((puv)^{1/2} \log(uvT^2p^{-3} + 2)).$$

If $T^2uv > 10000p^3$, then define

$$V = (uvT^2p^{-3})^{1/2} \log^{-1}(uvT^2p^{-3}).$$

Observe that $2 \le V \le T$. Let $T_1 = [T/V]$. Then we immediately obtain

$$\frac{J_2'}{T_1} - \frac{uvT}{p} \ll (puv)^{1/2} \log(uvT^2p^{-3} + 2). \tag{13}$$

Analogously,

$$\frac{J_2''}{T_1} - \frac{uvT}{p} \ll (puv)^{1/2} \log(uvT^2p^{-3} + 2). \tag{14}$$

Putting (12)–(14) together, we deduce Theorem 3. ∎

6. Proof of Theorem 4. For $N \le 10$ the statement is trivial. Furthermore, we have the well known asymptotic formula

$$J_3 = \frac{N^2}{p} + O(p^{1/2} \log^2 p).$$

Therefore, to prove Theorem 4 we may assume that $10 < N < p/2$.

Let J_3' be the number of solutions of the congruence

$$(x+u)(y+v) \equiv h \pmod{p}, \quad 1 \le x, y \le N-K, \ 1 \le u, v \le K,$$

where $K < N$ is a positive integer to be chosen later. By the same argument that we have used in the previous sections, we have the inequality

$$J_3 \ge \frac{J_3'}{K^2}.$$

Next, we express J_3' in terms of trigonometric sums:

$$J_3' = \frac{1}{p}\sum_{a=0}^{p-1}\sum_{x=1}^{N-K}\sum_{y=1}^{N-K}\sum_{u=1}^{K}\sum_{v=1}^{K} e^{2\pi i a(x+u-h(y+v)^{-1})/p}.$$

Using the standard technique, we obtain

$$J_3' = \frac{1}{p^2}\sum_{a=0}^{p-1}\sum_{b=0}^{p-1}\sum_{z=1}^{p-1}\sum_{x=1}^{N-K}\sum_{y=1}^{N-K}\sum_{u=1}^{K}\sum_{v=1}^{K} e^{2\pi i(a(x+u-hz^{-1})+b(z-y-v))/p}. \tag{15}$$

From the classical Weil estimate of Kloosterman sums we have

$$\Big|\sum_{z=1}^{p-1} e^{2\pi i(bz-ahz^{-1})/p}\Big| \le 2p^{1/2} \tag{16}$$

for any $a \not\equiv 0 \pmod p$. This also holds if $a \equiv 0 \pmod p$ and $b \not\equiv 0 \pmod p$ (even with the right hand side replaced by 1). Therefore, (16) holds if at least one of the numbers a and b is not divisible by p. Hence, in (15) isolating the term corresponding to $a = b = 0$ and using (16) for other values of a and b, we obtain

$$J_3' = \frac{(N-K)^2K^2(p-1)}{p^2} + 2\theta p^{1/2}\bigg(\frac{1}{p}\sum_{a=0}^{p-1}\Big|\sum_{x=1}^{N-K} e^{2\pi i ax/p}\Big|\Big|\sum_{u=1}^{K} e^{2\pi i au/p}\Big|\bigg)^2,$$

where $|\theta| \le 1$. We use Lemma 6 to bound the sum over a. This yields

$$J_3' - \frac{(N-K)^2K^2}{p} \ll p^{1/2}K^2\log^2(NK^{-1}+2).$$

Hence,

$$\frac{J_3'}{K^2} - \frac{N^2}{p} \ll \frac{KN}{p} + p^{1/2}\log^2(NK^{-1}+2). \tag{17}$$

If $N < 100p^{3/4}$, then define $K = N-1$ and deduce that in this case

$$\frac{J_3'}{K^2} - \frac{N^2}{p} \ll p^{1/2} \ll p^{1/2}\log^2(Np^{-3/4}+2).$$

Let $N > 100p^{3/4}$. Choose

$$V = N^2p^{-3/2}\log^{-2}(Np^{-3/4})$$

and note that $2 \le V \le N$. Now define $K = [N/V]$ and observe that in this case as well from (17) we have

$$\frac{J_3'}{K^2} - \frac{N^2}{p} \ll p^{1/2}\log^2(Np^{-3/4}+2).$$

Hence,

$$J_3 \ge \frac{N^2}{p} + O(p^{1/2}\log^2(Np^{-3/4}+2)). \tag{18}$$

To obtain a similar upper bound for J_3, define J_3'' to be the number of solutions of the congruence

$$(x-u)(y-v) \equiv h \pmod p, \quad 1 \le x, y \le N+K,\ 1 \le u, v \le K.$$

Then $J_3 \le K^{-2} J_3''$ and

$$J_3'' = \frac{1}{p^2} \sum_{a=0}^{p-1} \sum_{b=0}^{p-1} \sum_{z=1}^{p-1} \sum_{x=1}^{N+K} \sum_{y=1}^{N+K} \sum_{u=1}^{K} \sum_{v=1}^{K} e^{2\pi i (a(x-u-hz^{-1})+b(z-y+v))/p}.$$

The argument used to obtain lower bounds for J_3' and J_3 leads to the upper bound

$$J_3 \le \frac{N^2}{p} + O(p^{1/2} \log^2(Np^{-3/4}+2)).$$

Combining this with (18), we conclude that

$$J_3 - \frac{N^2}{p} \ll p^{1/2} \log^2(Np^{-3/4}+2).$$

Acknowledgements. The author is highly thankful to the anonymous referee for very useful suggestions which has led to Lemma 6. In particular, this has allowed the author to exploit the method of the paper to a much wider extent than in the first version.

This work was supported by Project PAPIIT-IN105605 from the UNAM.

References

[1] C. I. Cobeli, S. M. Gonek and A. Zaharescu, *On the distribution of small powers of a primitive root*, J. Number Theory 88 (2001), 49–58.

[2] M. Z. Garaev and K. L. Kueh, *Distribution of special sequences modulo a large prime*, Int. J. Math. Math. Sci. 50 (2003), 3189–3194.

[3] V. C. García, *A note on an additive problem with powers of a primitive root*, Bol. Soc. Mat. Mexicana 11 (2005), 1–4.

[4] A. A. Karatsuba, *Basic Analytic Number Theory*, Springer, Berlin, 1993.

[5] S. V. Konyagin, *Bounds of exponential sums over subgroups and Gauss sums*, in: Proc. 4th Intern. Conf. Modern Problems of Number Theory and Its Applications, Moscow Lomonosov State Univ., Moscow, 2002, 86–114 (in Russian).

[6] H. L. Montgomery, *Distribution of small powers of a primitive root*, in: Advances in Number Theory (Kingston, ON, 1991), Oxford Sci. Publ., Oxford Univ. Press, New York, 1993, 137–149.

[7] Z. Rudnik and A. Zaharescu, *The distribution of spacings between small powers of a primitive root*, Israel J. Math. 120 (2000), 271–287.

[8] A. Sárközy, *On the distribution of residues of product of integers*, Acta Math. Hungar. 49 (1987), 397–401.

[9] I. D. Shkredov, *On some additive problems associated with the exponential function*, Uspekhi Mat. Nauk 58 (2003), no. 4 (352), 165–166 (in Russian); English transl.: Russian Math. Surveys 58 (2003), no. 4, 798–799.

[10] M. Vâjâitu and A. Zaharescu, *Differences between powers of a primitive root*, Int. J. Math. Math. Sci. 29 (2002), 325–331.
[11] I. M. Vinogradov, *An Introduction to the Theory of Numbers*, Pergamon Press, London, 1955.

Instituto de Matemáticas, UNAM
Campus Morelia, Ap. Postal 61-3 (Xangari)
C.P. 58089, Morelia, Michoacán, México
E-mail: garaev@matmor.unam.mx

Received on 29.3.2005
and in revised form on 16.3.2006 (4967)