BULL. AUSTRAL. MATH. SOC. 11B50, 11J70, 11L03
VOL. 68 (2003) [1–11]

A NOTE ON THE LEAST QUADRATIC NON-RESIDUE OF THE INTEGER-SEQUENCES

M.Z. GARAEV

In this paper we consider the problem of an upper bound estimate for the least quadratic non-residue modulo prime number on special arithmetic sequences such as $f(n) = [\alpha n]$ and $f(n) = [n^c]$.

1. INTRODUCTION.

Throughout the text p denotes a prime number. We also use the following notations: $A \underset{a,\dots,b}{\ll} B$ means that $|A| \leqslant cB$ for some positive number c which may depend only on $a, \dots, b$, (a/p) denotes the Legendre symbol, and d denotes the least positive quadratic non-residue $\pmod p$ that is, the least positive integer for which $(d/p) = -1$.

The problem of an upper bound estimate for d originates in the work of Vinogradov [**10**], where he gave the estimate

$$d \underset{\varepsilon}{\ll} p^{1/(2\sqrt{e})+\varepsilon}.$$

Vinogradov based his proof on the inequality

$$\sum_{1 \leqslant n \leqslant x} \left(\frac{n}{p}\right) = O(p^{1/2}\log p)$$

discovered by him and independently by Pólya [**6**]. Currently the best upper bound for d is due to Burgess [**1**] where he obtained the estimate

$$d \underset{\varepsilon}{\ll} p^{1/(4\sqrt{e})+\varepsilon}. \tag{1}$$

Such problems for special arithmetic sequences have been considered by Preobrazhenskii [**7, 8**].

DEFINITION: ([**8**].) Let f be a real-valued function on the natural numbers. The family of integers $\left[f(n)\right]$ is called the integer-sequence.

We denote by $n_{\min}(f)$ the least positive integer n such that the number $\left[f(n)\right]$ is a quadratic non-residue $\pmod p$.

Received 13th May, 2002

Theorem. ([8]) *Let $f(n) = \alpha n$ where α is a real irrational number and assume that the incomplete quotients of the continued fraction expansion of α are bounded. Then for any $\varepsilon > 0$ the estimate*

$$n_{\min}(f) \underset{\alpha,\varepsilon}{\ll} p^{1/(2\sqrt{e})+\varepsilon} \tag{2}$$

holds.

In other words if q_{k+1}/q_k are bounded then (2) holds, where by q_k we denote the denominators of the convergents of α, arranged in increasing order. It should be pointed out that the proof of the above Theorem is of use to obtain (2) also for α with $q_{k+1} < q_k^{1+\varepsilon}$ for large k. This holds for algebraic α in view of Roth theorem. But it is also true for almost all α in the sense of Lebesgue measure. The following statement is a consequence of [**3**, Theorem 32]:

Theorem. ([3]) *Let ε be any fixed positive number. Then for almost all α the inequality*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}$$

has at most a finite number of solutions for integers p and q ($q > 0$).

By taking $p/q = p_k/q_k$ where p_k/q_k is a convergent of α, and using

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k q_{k+1}}$$

we see that for almost all α and for all $k > k_0(\alpha, \varepsilon)$ we have $q_{k+1} < q_k^{1+\varepsilon}$. Therefore in view of the proof of the Theorem of [8] we conclude that estimate (2) in fact holds for all irrational algebraic as well as for almost all α.

2. Statement of the results

The following Theorems 1, 2 and 3 are the results of our note:

Theorem 1. *Let the integer-sequence $[f(n)]$ be such that*

$$1 \leqslant [f(n+1)] - [f(n)] < \phi(n)$$

where $\phi(n)$ is an increasing sequence and assume that there is a positive integer M such that $f(1) < \phi(M) < p - M$ and

$$M > 2^{\phi(M)+2}(\phi(M)+2)p^{1/2}\log p.$$

Then

$$n_{\min}(f) \leqslant M.$$

Using arithmetic properties of the sequence $[\alpha n]$ we can improve the estimate of Theorem 1 for this special case:

Theorem 2. *Let $f(n) = \alpha n$ where $\alpha > 0$. Then for any $\varepsilon > 0$ there exists $c(\varepsilon) > 0$ such that the estimate*

$$n_{\min}(f) \ll_{\varepsilon} \left(1 + \frac{1}{\alpha}\right) p^{(1/4)+(1/4\sqrt{e})+\varepsilon}$$

is valid for all primes $p, p > \left(\alpha^2 + (1/\alpha)\right)c(\varepsilon)$.

Our estimate is less precise than (2), however it is valid for all $\alpha > 0$.

Theorem 1 gives an upper bound for $n_{\min}(f)$ when $f(x)/x$ increases very slowly. For example if $f(n) = n(\log n)^{1-\delta}$ then for any small positive numbers ε, δ one has

$$n_{\min}(f) \ll_{\varepsilon,\delta} p^{1/2+\varepsilon}.$$

A corresponding question naturally arises for functions $f(n)$ which grow faster than $n \log n$, say for $f(n) = n^c$ with non-integer $c, c > 1$. In this regard we prove the following result:

Theorem 3. *Let $f(n) = n^c$ where $1 < c < (12/11)$, and $\varepsilon > 0$. Then*

$$n_{\min}(f) \ll_{\varepsilon,c} p^{3/(4(6-4c)\sqrt{e})+\varepsilon}$$

for all sufficiently large p.

3. Proof of Theorem 1

The following statement is a particular case of a general celebrated result of Weil [**12**] (see also [**11**, p. 11, Lemma 2C; p. 45, Theorem 2G]).

Lemma 1. *Let $h(x) = (x-a_1)\dots(x-a_k)$ where the integers $a_1, \dots, a_k$ are different* (mod p)*. Then*

$$\sum_{x=0}^{p-1}\left(\frac{h(x)}{p}\right)e^{(2\pi i a x)/p} \leqslant kp^{1/2}.$$

Lemma 2. *Let N, M be any integers $0 \leqslant M \leqslant p-1$. Then under the conditions of* Lemma 1 *we have*

$$\left|\sum_{x=N}^{N+M}\left(\frac{h(x)}{p}\right)\right| \leqslant 2kp^{1/2}\log p.$$

Proof: Since for integers x, δ one has

$$\frac{1}{p}\sum_{a=0}^{p-1} e^{2\pi i(a(x-\delta)/p)} = \begin{cases} 1, & \text{if } x \equiv \delta \pmod p \\ 0, & \text{if } x \not\equiv \delta \pmod p \end{cases}$$

https://doi.org/10.1017/S0004972700037369 Published online by Cambridge University Press

then

$$\sum_{x=N}^{N+M}\Big(\frac{h(x)}{p}\Big) = \frac{1}{p}\sum_{\delta=N}^{N+M}\sum_{x=0}^{p-1}\sum_{a=o}^{p-1}\Big(\frac{h(x)}{p}\Big)e^{2\pi i(a(x-\delta)/p)}$$

$$\Big|\sum_{x=N}^{N+M}\Big(\frac{h(x)}{p}\Big)\Big| \leqslant \frac{1}{p}\sum_{a=o}^{p-1}\Big|\sum_{\delta=N}^{N+M}e^{2\pi i(a\delta/p)}\Big|\Big|\sum_{x=0}^{p-1}\Big(\frac{h(x)}{p}\Big)e^{2\pi i(ax/p)}\Big|.$$

Applying Lemma 1 we have

$$\Big|\sum_{x=N}^{N+M}\Big(\frac{h(x)}{p}\Big)\Big| \leqslant kp^{-(1/2)}\sum_{a=o}^{p-1}\Big|\sum_{\delta=N}^{N+M}e^{2\pi i(a\delta/p)}\Big|.$$

Picking up the term corresponding to $a = 0$, and evaluating the sum over δ for $1 \leqslant a \leqslant p-1$ we obtain

$$\Big|\sum_{x=N}^{N+M}\Big(\frac{h(x)}{p}\Big)\Big| \leqslant k(M+1)p^{-(1/2)} + kp^{-(1/2)}\sum_{a=1}^{p-1}\Big|\sin\frac{\pi a}{p}\Big|^{-1}.$$

The latter sum is not greater than $p\log p$ (see for example [**4**, p. 109-110]). Therefore

$$\Big|\sum_{x=N}^{N+M}\Big(\frac{h(x)}{p}\Big)\Big| \leqslant 2kp^{1/2}\log p.$$

Let us now prove Theorem 1. Consider the function

$$H(x) = \prod_{n=1}^{[\phi(M)]+1} h_n(x)$$

where $h_n(x) = 1 - \big((x+n)/p\big)$. We have that

$$\Big|\sum_{x=1}^{M} F(x)\Big| \geqslant M - \Big|\sum_{x=1}^{M}\big(F(x)-1\big)\Big|.$$

The function $H(x) - 1$ is a sum of $2^{[\phi(M)]+1} - 1$ functions of the type $\pm\big(h(x)/p\big)$ with $h(x)$ subject to the conditions of Lemma 1 and 2 (the roots of $h(x)$ are distinct $\pmod p$ since $\phi(M) < p$). Therefore applying Lemma 2 each time with $N = 1$ we obtain

$$\Big|\sum_{x=1}^{M} F(x)\Big| \geqslant M - 2^{\phi(M)+2}\big(\phi(M)+1\big)p^{1/2}\log p > 0.$$

$\square$

Since $\Big|\sum_{x=1}^{M} F(x)\Big| > 0$ then $F(x) \neq 0$ for some $x, 1 \leqslant x \leqslant M$ and hence

$$\Big(\frac{x+1}{p}\Big) = \Big(\frac{x+2}{p}\Big) = \ldots \Big(\frac{x+[\phi(M)]+1}{p}\Big) = -1.$$

Theorem 1 now follows from the conditions

$$f(1) < \phi(M), \quad 1 \leqslant \big[f(n+1)\big] - \big[f(n)\big] < \phi(n).$$

4. Proof of Theorem 2

We need a well-known result of Burgess [**1**]:

Lemma 3. *Let δ, ε be any fixed positive numbers. Then for all sufficiently large p and any N, we have*

$$\left|\sum_{n=N+1}^{N+H}\left(\frac{n}{p}\right)\right| < \delta H$$

provided $H > p^{(1/4)+\varepsilon}$.

As we agreed before d denotes the least positive quadratic non-residue (mod p).

For the proof of Theorem 2 we distinguish 3 cases:

Case 1. α is an irrational, $\alpha > 1$.

Let

$$\alpha = a_1 + \frac{1}{a_2 + (1/a_3 + \dots)}$$

be an expansion of α into a continued fraction and denote by $p_1/q_1, p_2/q_2, \dots$ the convergents of α. If we set $p_0 = 1, q_0 = 0$ then we can write

$$p_1 = a_1 = [\alpha],\ q_1 = 1,\ p_{k+1} = a_{k+1}p_k + p_{k-1},\ q_{k+1} = a_{k+1}q_k + q_{k-1}.$$

There exists a number k such that $q_k \leqslant d < q_{k+1}$. From the properties of continued fraction we have

$$\alpha = \frac{p_k}{q_k} + \frac{\theta_k}{q_k q_{k+1}}$$

where $0 < \theta_k < 1$ for odd k, and $-1 < \theta_k < 0$ for even k.

If k is odd integer then from $q_{k+1} > d$ we have

$$[\alpha q_k] = p_k,\ [\alpha d q_k] = d p_k.$$

Since d is a non-residue (mod p), $p_k < \alpha d < p$ then one of the numbers p_k, dp_k is a quadratic non-residue (mod p). Now the required estimate follows from

$$dp_k \leqslant d^2 \underset{\varepsilon}{\ll} p^{1/(2\sqrt{e})+\varepsilon}$$

where we used (1).

Let k be an even integer. Consider 2 possibilities.

(a) $q_{k+1} \leqslant p^{(1/4)+\varepsilon}$. Then we can write

$$\alpha = \frac{p_{k+1}}{q_{k+1}} + \frac{\theta_{k+1}}{q_{k+1}q_{k+2}}$$

where $0 < \theta_{k+1} < 1$. We have as before

$$[\alpha q_{k+1}] = p_{k+1},\ [\alpha d q_{k+1}] = p_{k+1}d,\ p_{k+1} < \alpha p^{(1/4)+\varepsilon} < p.$$

Now the required estimate follows from

$$dq_{k+1} \underset{\varepsilon}{\ll} p^{(1/4)+(1/4\sqrt{e})+\varepsilon}.$$

(b) $q_{k+1} > p^{(1/4)+\varepsilon}$. Put $H = p^{(1/4)+\varepsilon}$ and let $n = xq_k$ where x runs through integers $1 \leqslant x \leqslant H$. Since $-1 < \theta_k < 0$ then $[\alpha n] = xp_k - 1$. Also note that $p_k < 2\alpha q_k < p$.

We make use of Lemma 3. Taking $\delta = 1/2$ we have that

$$\left|\sum_{x=1}^{H}\Big(\frac{xp_k - 1}{p}\Big)\right| = \left|\sum_{x=1}^{H}\Big(\frac{x - p_k^*}{p}\Big)\right| < \frac{H}{2}$$

where p_k^* is defined from $p_k p_k^* \equiv 1 \pmod p$. Hence among the numbers $xp_k - 1$ with $1 \leqslant x \leqslant p^{(1/4)+\varepsilon}$ there exists a quadratic non-residue $(\bmod\ p)$. Therefore

$$n_{\min}(f) \leqslant xq_k \underset{\varepsilon}{\ll} p^{(1/4)+1/4\sqrt{e}+\varepsilon}.$$

Case 1 is thus treated completely. ▯

CASE 2. α is rational, $\alpha > 1$.

In this case the number of convergents of α are finite. Let $p_1/q_1, \dots, p_r/q_r$ be all convergents of α. If $q_r \leqslant d$ then we prove Theorem 2 by taking $n = q_r$ or $n = dq_r$. If $q_r > d$ then from $q_1 = 1$ we deduce that $q_k \leqslant d < q_{k+1}$ for some $k < r$. The remainder of the proof is the same as in Case 1 and we omit it here.

CASE 3. $0 < \alpha \leqslant 1$.

The case $\alpha = 1$ is classical and the desired estimate follows from (1).

Let $0 < \alpha < 1$. Then for $n_0 = [d/\alpha] + 1$ we have

$$\alpha n_0 = \alpha[d/\alpha] + \alpha = d + \alpha\big(1 - \{d/\alpha\}\big),$$

when $[\alpha n_0] = d$. Therefore $n_{\min}(f) \leqslant n_0 \leqslant p^{1/4\sqrt{e}+\varepsilon}/\alpha$.

Theorem 2 is thus proved. ▯

5. Proof of Theorem 3

The following two Lemmas are well known and can be found for example in [2, p. 255]:

LEMMA 4. *For any real number t we have*

$$\varrho(t) = \sum_{1\leqslant|h|\leqslant H} \frac{e^{2\pi i h t}}{2\pi i h} + O\Big(\frac{1}{\sqrt{1 + H^2 \sin^2 \pi t}}\Big)$$

where $\varrho(t) = 1/2 - \{t\}$.

https://doi.org/10.1017/S0004972700037369 Published online by Cambridge University Press

Lemma 5. *Let $M = H\log H, H > 10$. Then*

$$\frac{1}{\sqrt{1+H^2\sin^2\pi t}} = \sum_{1\leqslant |h|\leqslant M} c_h e^{2\pi iht} + O\Big(\frac{\log H}{H}\Big)$$

where $|c_h| \ll (\log H/H)e^{-|h|/H}$.

Let $0 \leqslant \alpha < \beta < 1$, and $\sigma(t) = \sigma(\alpha,\beta,t)$ be a periodic function with period 1 defined as

(3)
$$\sigma(t) = \begin{cases} 1, & \text{if } \{t\} \in (\alpha,\beta] \\ 0, & \text{otherwise.} \end{cases}$$

Then

$$\sigma(t) = \beta - \alpha + \varrho(\beta - t) - \varrho(\alpha - t).$$

This equality together with Lemma 4 and 5 gives

Lemma 6. *Let $X > 10$, $H > 10$. Then for some $1 \leqslant N \leqslant H\log H$ and $m \in [N, 2N]$ we have*

$$\sum_{X/2<x\leqslant X} \sigma(g(x)) \geqslant \frac{\beta-\alpha}{2}X - R\log^2 H$$

where

$$R = O\Big(\frac{X}{H} + \Big|\sum_{X/2<x\leqslant X} e^{2\pi img(x)}\Big|\Big).$$

In fact, for any real γ we have

$$\sum_{X/2<x\leqslant X} \varrho(\gamma - g(x)) \ll \sum_{1\leqslant h\leqslant H} \frac{1}{h}\Big|\sum_{X/2<x\leqslant X} e^{2\pi ihg(x)}\Big| + \frac{\log H}{H}\sum_{1\leqslant h\leqslant H\log H}\Big|\sum_{X/2<x\leqslant X} e^{2\pi ihg(x)}\Big| + \frac{X\log H}{H}$$

which proves Lemma 6. ∎

Lemma 7. (Van der Korput). *Let k be a positive integer, $k \geqslant 2$. Suppose that $F(x)$ is a real-valued function with k continuous derivatives on $[X/2, X], X \geqslant 1$. Further suppose that*

$$0 < \lambda \leqslant F^{(k)} \leqslant h\lambda,\ K = 2^{k-1}.$$

Then

$$\Big|\sum_{X/2<x\leqslant X} e^{2\pi iF(x)}\Big| \ll Xh^{2/K}\lambda^{1/2K-2} + X^{1-(2/K)}\lambda^{-(1/2K-2)}$$

where the implied constant is absolute.

For the proof see [**5**, p. 378].

https://doi.org/10.1017/S0004972700037369 Published online by Cambridge University Press

Now we are ready to proceed to prove Theorem 3. Let ε_1 be a positive number which is considerably smaller than $\bigl((12/11)-c\bigr)\varepsilon$. For a large prime p we distinguish two cases depending on the value of d.

CASE 1. $d \geqslant p^{\varepsilon_1}$.

Put

$$X = d^{(7c-6)/(6-4c)+\varepsilon_1}. \tag{4}$$

Since $(7c-6/6-4c)+\varepsilon_1 < 1$ then all numbers of the form dx with $x \leqslant X$ are quadratic non-residue. Our aim is to find $x, (X/2) < x \leqslant X$ such that $[n^c] = dx$ for some n. It would then follow that

$$n_{\min}(f) \leqslant \bigl(d^{(3c/6-4c)+\varepsilon_1}\bigr)^{1/c}$$

which together with (1) proves Theorem 3.

The equation $[n^c] = dx$ is equivalent to the inequality

$$(dx)^{1/c} \leqslant n < (dx+1)^{1/c}.$$

This holds if

$$0 < \bigl\{(dx+1)^{1/c}\bigr\} \leqslant \frac{(dX)^{(1/c)-1}}{4}$$

since $\bigl((dX)^{(1/c)-1}\bigr)/4 < (dx+1)^{1/c} - (dx)^{1/c}$. Therefore it is enough to prove that

$$\sum_{X/2<x\leqslant X} \sigma\bigl((dx+1)^{1/c}\bigr) > 0$$

where $\sigma(t)$ is defined from (3) with $\alpha = 0, \beta = \bigl((dX)^{(1/c)-1}\bigr)/4$. Taking $g(x) = (dx+1)^{1/c}$ and applying Lemma 6 we obtain

$$\sum_{X/2<x\leqslant X} \sigma\bigl((dx+1)^{1/c}\bigr) > \frac{X^{1/c}d^{(1/c)-1}}{8} - R\log^2 H \tag{5}$$

where

$$R \ll \frac{X}{H} + \Biggl|\sum_{(X/2)<x\leqslant X} e^{2\pi i m(dx+1)^{1/c}}\Biggr|, \quad 1 \leqslant N \leqslant m \leqslant 2N \leqslant 2H\log H.$$

We can choose H as we please, provided $H > 10$.

In order to estimate R we make use of Lemma 7. Here we take $F(x) = m(dx+1)^{1/c}$ and $k = 3$. For $X/2 < x \leqslant X$ we have

$$F^{(3)}(x) \asymp N d^{1/c} X^{(1/c)-3}.$$

Therefore $\lambda \asymp N d^{1/c} X^{(1/c)-3}$. From $N \leqslant H\log H$ it follows that

$$R \ll_{\varepsilon,c} \Bigl(\frac{X}{H} + H^{1/6} d^{1/6c} X^{(1/2)+(1/6c)} + d^{-(1/6c)} X^{1-(1/6c)}\Bigr)\log H.$$

https://doi.org/10.1017/S0004972700037369 Published online by Cambridge University Press

We choose now $H = X^{3/7-(1/7c)}d^{-(1/7c)}$ and recall (4). Obviously we have $H > 10$ and

$$R \underset{\varepsilon,c}{\ll} \left(d^{(4c-3/6-4c)+((4c+1)\varepsilon_1)/7c} + d^{(14c-13)/(2(6-4c))+((6c-1)\varepsilon_1)/6c}\right) \log d.$$

From the other side

$$X^{1/c}d^{(1/c)-1} = d^{(4c-3)/(6-4c)+\varepsilon_1/c}.$$

Since

$$\frac{4c+1}{7c} < \frac{1}{c}, \quad \frac{14c-13}{2(6-4c)} < \frac{4c-3}{6-4c}$$

then by (5) we have the estimate

$$\sum_{X/2<x\leqslant X} \sigma\left((dx+1)^{1/c}\right) > 0.$$

which proves the Case 1 in Theorem 3. ∎

CASE 2. $2 \leqslant d < p^{\varepsilon_1}$.

Now our starting point is that dx^2 is a non-residue for all $x, x < p$. We suppose $X/2 < x \leqslant X$ and choose $X = p^{1/100}$.

The equation $[n^c] = dx^2$ is equivalent to the inequality

$$(dx^2)^{1/c} \leqslant n < (dx^2+1)^{1/c}.$$

This holds if

$$0 < \left\{(dx+1)^{1/c}\right\} \leqslant \frac{(dX^2)^{(1/c)-1}}{10}.$$

Therefore it is enough to prove that

$$\sum_{(X/2)<x\leqslant X} \sigma\left((dx^2+1)^{1/c}\right) > 0$$

where $\sigma(t)$ is defined from (3) with $\alpha = 0, \beta = \left((dX^2)^{(1/c)-1}\right)/10$. Analogously to Case 1 we apply Lemma 6 by taking $g(x) = (dx^2+1)^{1/c}$. We have

$$\sum_{(X/2)<x\leqslant X} \sigma\left((dx^2+1)^{1/c}\right) > \tfrac{X^{(2/c)-1}d^{(1/c)-1}}{20} - R\log^2 H, \tag{6}$$

$$R \ll \tfrac{X}{H} + \left|\sum_{(X/2)<x\leqslant X} e^{2\pi i m(dx^2+1)^{(1/c)}}\right|, \quad 1 \leqslant N \leqslant m \leqslant 2N \leqslant 2H\log H$$

where we can choose any $H, H > 10$.

In order to estimate R we apply Lemma 7 for $F(x) = m(dx^2+1)^{1/c}$ and $k = 3$. It is easy to see that for $X/2 < x \leqslant X$ we have

$$F^{(3)}(x) \asymp Nd^{1/c}X^{(2/c)-3}.$$

https://doi.org/10.1017/S0004972700037369 Published online by Cambridge University Press

Therefore we can take $\lambda \asymp N d^{1/c} X^{(2/c)-3}$. Then using $N \leqslant H \log H$ we have

$$R \underset{\varepsilon,c}{\ll} \Big(\frac{X}{H} + H^{1/6} d^{1/6c} X^{1/2+1/3c} + d^{-(1/6c)} X^{1-(1/3c)}\Big) \log X.$$

We choose now $H = X^{3/7-2/7c} d^{-1/7c}$ and recall that $X = p^{1/100}$. Obviously we have $H > 10$ and

$$R \underset{\varepsilon,c}{\ll} \big(X^{(4/7)+(2/7c)} d^{1/7c} + X^{1-(1/3c)} d^{-(1/6c)}\big) \log H.$$

From $c < 12/11$ it follows

$$\frac{4}{7} + \frac{2}{7c} < \frac{2}{c} - 1,\ 1 - \frac{1}{3c} < \frac{2}{c} - 1.$$

Now the estimate

$$\sum_{(X/2) < x \leqslant X} \sigma\big((dx^2+1)^{1/c}\big) > 0.$$

follows from (6) using $d < p^{\varepsilon_1}$.

Theorem 3 is proved. ∎

REMARK. Two kind of problems arise in connection with Theorem 3. One is further improvement on the range of $n_{\min}(f)$, and another one is improvement on the range of c. One is able to apply the method of exponential pairs. It would give after some consideration the following result:

Let (κ, λ) be an exponential pair. Then for any $c < 2/(1+\kappa+\lambda)$ we have

$$n_{\min}(f) \underset{\varepsilon,c}{\ll} p^{(1+\kappa-\lambda)/(4(1-\lambda c)\sqrt{e})+\varepsilon}.$$

In 1955 Rankin [9] proved that for some θ with

$$0.32902135684 \leqslant \theta < 0.32902135688$$

there exists an exponential pair $(\kappa, \lambda) = \big((\theta/2)+\varepsilon, 1/2+\theta/2+\varepsilon\big)$ for any small positive ε. Hence we have admissible range for c as

$$c < \frac{12}{11} + 0.00257\ldots.$$

and

$$n_{\min(f)} \underset{\varepsilon,c}{\ll} p^{1/(8(1-\theta_2 c)\sqrt{e})+\varepsilon}$$

where $\theta_2 = 0.66451\ldots$. Both estimate are slightly better than that one of Theorem 3. However this improvement is not strong enough. One can expect that there is another way to treat the problem which would make considerably better improvement than we have just discussed.

References

[1] D.A. Burgess, 'The distribution of quadratic residues and non-residues', *Mathematika* **4** (1957), 106–112.

[2] S.B. Gashkov and V.N. Chubarikov, *Arithmetics. Algorithms. Complexity of computations*, (in Russian) (Visshaya Shkola, Moscow, 2000).

[3] A.Ya. Khintchine, *Continued fractions* (P. Noordhoff Ltd. Groningen, The Netherlands, 1963).

[4] A.A. Karatsuba, *Basic analytic number theory* (Springer-Verlag, Berlin, Heidelberg, New York, 1993).

[5] A.A. Karatsuba and S.M. Voronin, *The Riemann zeta-function* (Walter de Gruyter, Berlin, New York, 1992).

[6] G. Pólya, 'Über die Verteilung der quadratischen Reste und Nichtreste', *Göttinger Nachrichten* (1918), 21–29.

[7] S.N. Preobrazhenskii, 'The least quadratic non-residue in an arithmetic sequence', *Moscow Univ. Math. Bull.* **56** (2001), 44–46.

[8] S.N. Preobrazhenskii, 'Power non-residues modulo a prime number in a special entier-sequence', *Moscow Univ. Math. Bull.* **56** (2001), 41–42.

[9] R.A. Rankin, 'Van der Corput's method and the theory of exponent pairs', *Quart. J. Math. (Oxford)* **6** (1955), 147–153.

[10] I.M. Vinogradov, 'Sur la distribution des résidus et des non-résidus des puissances', *Journal Physico-Math. Soc. Univ. Perm* **1** (1918), 94–96.

[11] W.M. Schmidt, *Equations over finite fields*, Lecture Notes in Math. **536** (Springer-Verlag, Berlin, New York, 1976).

[12] A. Weil, 'On some exponential sums', *Proc. Nat. Acad. Sci. U.S.A.* **34** (1948), 204–207.

Instituto de Matemáticas UNAM
Campus Morelia
Apartado Postal 27-3 (Xangari)
C.P. 58089, Morelia
Michoacán
Mexico
e-mail: garaev@matmor.unam.mx