# QUADRATIC NON-RESIDUES IN SHORT INTERVALS

SERGEI V. KONYAGIN AND IGOR E. SHPARLINSKI

Abstract. We use the Burgess bound and combinatorial sieve to obtain an upper bound on the number of primes $p$ in a dyadic interval $[Q, 2Q]$ for which a given interval $[u+1, u+\psi(Q)]$ does not contain a quadratic non-residue modulo $p$. The bound is nontrivial for any function $\psi(Q) \to \infty$ as $Q \to \infty$. This is an analogue of the well known estimates on the smallest quadratic non-residue modulo $p$ on average over primes $p$, which corresponds to the choice $u = 0$.

## 1. Introduction

### 1.1. Motivation and background.

For a prime $p \geq 3$ we denote by $n(p)$ the smallest quadratic non-residue modulo $p$. The best known upper bound $n(p) \leq p^{1/4e^{1/2}+o(1)}$ is due to Burgess [1], while it is expected that $n(p) = p^{o(1)}$, which is widely known as a *Conjecture of Vinogradov*.

Bound of this type, and in fact much more precise, are also known. For example, conditionally on the Generalised Riemann Conjecture, we have $n(p) = O(\log^2 p)$ for any prime $p$, see [8, Theorem 13.11].

Furthermore, unconditionally, using the large sieve method, Erdős [3] has established that

$$\frac{1}{\pi(x)} \sum_{p \leq x} n(p) \to \sum_{k=1}^{\infty} \frac{p_k}{2^k}, \qquad x \to \infty,$$

where, as usual $\pi(x)$ denotes the number of primes $p \leq x$ and $p_k$ denotes the $k$th prime. This instantly implies that the inequality $n(p) \leq \psi(p)$ holds for almost all primes $p$ (that is, for all but $o(x/\log x)$ primes $p \leq x$, as $x \to \infty$), where $\psi$ is an arbitrary function with $\psi(z) \to \infty$ as $z \to \infty$.

On the other hand, by a result of Graham and Ringrose [6], there is an absolute constant $C > 0$ such that for infinitely many primes $p$ all nonnegative integers $z \leq C \log p \log\log\log p$ are quadratic residues modulo $p$.

2010 *Mathematics Subject Classification.* 11A15, 11L40.

*Key words and phrases.* Quadratic non-residues, character sums.

Another *Conjecture of Vinogradov* is the bound $d(p) = p^{o(1)}$, where $d(p)$ is the longest sequence of consecutive quadratic residues modulo $p$. It seems that this conjecture received less attention than the one about the smallest quadratic non-residue. In particular, the only known result about $d(p)$ is the bound $d(p) \le p^{1/4+o(1)}$, which is due to Burgess [1] as well. It is still unknown whether the Generalised Riemann Conjecture or the large sieve method (or any other standard methods and conjectures) can lead to a better estimate on $d(p)$ for at least almost all primes. This naturally leads to the following:

**Problem 1.** *Assuming the Generalised Riemann Conjecture, show that for some constant $\gamma < 1/4$ the bound $d(p) < p^{\gamma}$ holds for almost all primes $p$.*

In fact, it is still unknown whether $d(p) = o(p^{1/4})$ for an infinite sequence of primes.

Our main goal here is to attract more attention to the function $d(p)$ and also make a modest step towards better understanding the distribution of quadratic non-residues.

We also denote by $n_k(p)$ the $k$th quadratic non-residue modulo $p$, and consider the gaps $\Delta_k(p) = n_{k+1}(p) - n_k(p)$, $k = 1, \ldots, (p-3)/2$.

It is shown in [2, Lemma 2] that for any fixed $\varepsilon > 0$ and $h \ge p^{\varepsilon}$

$$\#\{k = 1, \ldots, (p-3)/2 \ : \ \Delta_k(p) \ge h\} \le p^{1/2+o(1)} h^{-2}.$$

which, via partial summation, leads to the estimate

$$S(h,p) = \sum_{\substack{j=1\\ \Delta_k(p) \ge h}}^{(p-3)/2} \Delta_k(p) \le p^{1/2+o(1)} h^{-1}.$$

We also note that a result of Garaev, Konyagin and Malykhin [5, Theorem 2], in particular, gives an asymptotic formula for the average values of the $\gamma$-powers of gaps between quadratic residues modulo $p$ for $0 < \gamma < 4$. This can easily be extended to the same estimate for the gaps between quadratic non-residues modulo $p$.

1.2. **Main result.** Let $d_u(p)$ be smallest $h$ such that there exist a quadratic non-residue in the interval $\mathcal{I} = [u+1, u+h]$. Clearly

$$n(p) = d_u(p) \qquad \text{and} \qquad d(p) = \max_{u \in \mathbb{Z}} d_u(p).$$

So estimating $d_u(p)$ for a given $u$ can be considered as an intermediate question between estimating $n(p)$ and $d(p)$.

Here we estimate $d_u(p)$, uniformly over $u$, for almost all primes $p$. It is more convenient to work with primes from dyadic intervals $[Q, 2Q]$.

**Theorem 2.** *Let $\psi$ be an arbitrary function with $\psi(z) \to \infty$ as $z \to \infty$. For any sufficiently large real positive $Q$, for any integer $u \le 2Q$, for the set $\mathcal{E}_u(\psi, Q)$ of primes $p \in [Q, 2Q]$ with*

$$d_u(p) > \psi(p)$$

*we have $\mathcal{E}_u(\psi, Q) = o(Q/\log Q)$ uniformly in $u$.*

## 2. Preliminaries

2.1. **General notation.** Throughout the paper, the implied constants in the symbols "$O$", "$\ll$" and "$\gg$" may occasionally, where obvious, depend on the real positive parameters $\varepsilon$ and $\eta$ and are absolute otherwise. We recall that the expressions $A = O(B)$, $A \ll B$ and $B \gg A$ are each equivalent to the statement that $|A| \le cB$ for some constant $c$.

We always use the letter $p$, with or without subscripts, to denote a prime number, while $k$, $m$, $n$ and $q$ always denote positive integer numbers.

As usual, we use $\varphi(k)$ is the Euler function.

2.2. **Burgess bound.** We now recall the Burgess bound for some of multiplicative characters modulo arbitrary integers, see [7, Theorems 12.5 and 12.6]. In fact we only need it for sums of Jacobi symbols.

**Lemma 3.** *For any integers $q \ge M \ge 1$, where $q \ge 2$ is not a perfect square, we have*

$$\left| \sum_{m \le M} \left( \frac{m}{q} \right) \right| \le M^{1-1/\nu} q^{(\nu+1)/4\nu^2 + o(1)},$$

*with $\nu = 1, 2, 3$.*

In particular, Lemma 3 implies:

**Corollary 4.** *For any $\varepsilon > 0$ there exists some $\delta > 0$ such that for any integers $M \ge q^{1/3+\varepsilon}$, where $q \ge 2$ is not a perfect square, we have*

$$\left| \sum_{m \le M} \left( \frac{m}{q} \right) \right| \le M^{1-\delta}$$

2.3. **Integers with a prescribed multiplicative structure.** Now given some $\eta > 0$ we denote by $\mathcal{P}(\eta, M)$ the set of positive integers $m \le M$ which do not have prime divisors $p \le M^\eta$. It is well known that for any fixed $\eta > 0$ we have

$$|\mathcal{P}(\eta, M)| \le c_0 \frac{M}{\eta \log M} \qquad (1)$$

for some absolute constants $c_0 > 0$, see, for example, [9, Section III.6.2, Theorem 3].

We now recall the so-called *fundamental lemma of the combinatorial sieve*, see, for example, [9, Section I.4.2, Theorem 3].

For a finite set of integers $\mathcal{A}$ and a set of primes $\mathcal{P}$ we denote

$$P(y) = \prod_{\substack{p \in \mathcal{P} \\ p \le y}} p$$

and

$$S(\mathcal{A}, \mathcal{P}, y) = \#\{a \in \mathcal{A} \ : \ \gcd(a, P(y)) = 1\}.$$

**Lemma 5.** *Assume that for a finite set of integers $\mathcal{A}$ and a set of primes $\mathcal{P}$ there exist a non-negative multiplicative function $\omega(d)$, a real $X$ and positive constants $\alpha$ and $A$ such that:*

- *for any $d \mid P(y)$, we have*

$$\#\{a \in \mathcal{A} \ : \ a \equiv 0 \pmod d\} = X\frac{\omega(d)}{d} + R_d;$$

- *for any real $v > w \ge 2$ we have*

$$\prod_{w \le p \le v} \left(1 - \frac{\omega(p)}{p}\right) < \left(\frac{\log v}{\log w}\right)^{\alpha} \left(1 + \frac{A}{\log w}\right).$$

*Then uniformly for $\mathcal{A}$, $X$, $y$ and $u \ge 1$*

$$S(\mathcal{A}, \mathcal{P}, y) = X \prod_{p \mid P(y)} \left(1 - \frac{\omega(p)}{p}\right) \left(1 + O(u^{-u/2})\right) + O\left(\sum_{\substack{d \mid P(y) \\ d \le y^u}} |R_d|\right).$$

We also need the following well-known statement which follows from the standard inclusion-exclusion argument and the classical bound on the number of integer divisors of $q$.

**Lemma 6.** *For any integers $q \ge M \ge 1$, we have*

$$\#\{1 \le m \le M \ : \ \gcd(m, q) = 1\} = \frac{\varphi(q)}{q} M + O(q^{o(1)}).$$

The following asymptotic formula for the number of square-free integers in a short interval is a very special case of a much more general result of Tolev [10, Theorem 1.3] (which we apply with $r = 2$, $l_1 = 1$, $l_2 = 2$), which in turn extends and generalises a result of Filaseta and Trifonov [4].

**Lemma 7.** *For any fixed $\varepsilon > 0$ and real $h \ge u^{1/5+\varepsilon}$, the interval $[u+1, u+h]$ contains $(A+o(1))\,h$ square-free integers $n$ for which $n+1$ is also square-free, where*

$$A = \prod_{p \ \text{prime}} \left(1 - \frac{2}{p^2}\right).$$

**Corollary 8.** *For any fixed $\varepsilon > 0$ and real $u \ge h \ge u^{1/5+\varepsilon}$, the interval $[u+1, u+h]$ contains at least $(A+o(1))\,h$ odd square-free integers $n$.*

Note, that Corollary 8 is much stronger than what we actually need. Namely, any result with $\alpha < 1/2$ instead of $1/5$ and arbitrary $A > 0$ is sufficient for our purposes.

2.4. **Character sums with integers from $\mathcal{P}(\eta, M)$.** We now consider the sets

$$\mathcal{P}_{\pm}(\eta, M, q) = \left\{ m \in \mathcal{P}(\eta, M) \ : \ \left(\frac{m}{q}\right) = \pm 1 \right\}.$$

**Lemma 9.** *For any $\varepsilon > 0$ there exists some $\eta_0 > 0$ such that for any positive $\eta < \eta_0$ and integers $M \ge q^{1/3+\varepsilon}$, where $q \ge 2$ is not a perfect square, we have*

$$\left| \mathcal{P}_{\pm}(\eta, M, q) - \frac{1}{2} M \prod_{p \le M^{\eta}} \left(1 - \frac{1}{p}\right) \right| \le C \eta^{\eta^{-1/2}/4 - 1} \frac{M}{\log M} + O\left(M^{1-\eta}\right),$$

*where $C$ is an absolute constant.*

*Proof.* We see from Corollary 4 and Lemma 6 that for any positive integer $d < q^{\varepsilon/2}$ with $\gcd(d, q) = 1$ we have

$$\#\left\{ 1 \le m \le M \ : \ d \mid m \text{ and } \left(\frac{m}{q}\right) = \pm 1 \right\} = \frac{\varphi(q)}{2dq} M + R(q, M, d), \tag{2}$$

where

$$R(q, M, d) = O((M/d)^{-\delta}) \tag{3}$$

for some $\delta > 0$ depending only on $\varepsilon$.

We now set $\eta_0 = \delta^2/4$ and apply Lemma 5 with $u = \eta^{-1/2}$, $y = M^{\eta}$ and

$$\omega(d) = \begin{cases} 1, & \text{if } \gcd(d, q) = 1; \\ 0, & \text{if } \gcd(d, q) > 1. \end{cases}$$

We also assume that $\eta$ is small enough so that

$$y^u = M^{\eta^{1/2}} \le q^{\varepsilon/2}$$

so (2) applies to all positive integers $d \le y^u$. This implies,

$$\left| \mathcal{P}_\pm(\eta, M, q) - \frac{\varphi(q)}{2q} M \prod_{\substack{p \le M^\eta \\ p \nmid q}} \left(1 - \frac{1}{p}\right) \right| \le \Delta_1 + \Delta_2, \tag{4}$$

where

$$\Delta_1 = C u^{-u/2} \frac{\varphi(q)}{q} M \prod_{\substack{p \le M^\eta \\ p \nmid q}} \left(1 - \frac{1}{p}\right)$$

for some absolute constant $C$, and

$$\Delta_2 \ll \sum_{d \le y^u} |R(q, M, d)|$$

with $R(q, M, d)$ defined by (2).

For $\Delta_1$, recalling the choice of $u$ and $y$, we derive

$$\Delta_1 \le C \eta^{\eta^{-1/2}/4} \frac{\varphi(q)}{q} M \prod_{\substack{p \le M^\eta \\ p \nmid q}} \left(1 - \frac{1}{p}\right). \tag{5}$$

For $\Delta_2$, using (3) and assuming that $\eta \le \delta/2$, we obtain

$$\Delta_2 \ll \sum_{d \le y^u} (M/d)^{1-\delta} \ll M^{1-\delta/2} \le M^{1-\eta}. \tag{6}$$

We also note that

$$\begin{aligned} \frac{\varphi(q)}{q} \prod_{\substack{p \le M^\eta \\ p \nmid q}} \left(1 - \frac{1}{p}\right) &= \prod_{p \le M^\eta} \left(1 - \frac{1}{p}\right) \prod_{\substack{p > M^\eta \\ p \mid q}} \left(1 - \frac{1}{p}\right) \\ &= \left(1 + O(M^{-\eta})\right) \prod_{p \le M^\eta} \left(1 - \frac{1}{p}\right). \end{aligned} \tag{7}$$

Thus substituting (5), (6) and (7) in (4) and recalling that by the Mertens formula, see [9, Section I.1.6, Theorem 11], we have

$$\prod_{p \le M^\eta} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma} + o(1)}{\eta \log M},$$

where $\gamma = 0.57721\ldots$ is the Euler constant, we conclude the proof. □

**Corollary 10.** *For any $\varepsilon > 0$ there exists some $\eta_0 > 0$ such that for any positive $\eta < \eta_0$, integers $M \ge q^{1/3+\varepsilon}$, where $q \ge 2$ is not a perfect* *square, we have*

$$\left|\sum_{m\in\mathcal{P}(\eta,M)}\left(\frac{m}{q}\right)\right| \le C_0\eta^{\eta^{-1/2}/4-1}\frac{M}{\log M} + O\left(M^{1-\eta}\right),$$

*where $C_0$ is an absolute constant.*

## 3. Proof of Theorem 2

Let

$$h = \min_{z\in[Q,2Q]} \psi(z).$$

We consider the interval $\mathcal{I} = [u+1, u+h]$. Without loss of generality we can assume that, say, $\psi(z) \le \log z$, so that $h = o(Q)$.

Let us fix some arbitrary $\kappa > 0$, we show that for all but at most $\kappa Q/\log Q$ primes $p \in [Q, 2Q]$ there is a quadratic non-residue in $\mathcal{I}$.

Let $\mathcal{N}$ be an arbitrary set of integers $n \in \mathcal{I}$ with either $n \equiv 1 \pmod 4$ or $n \equiv 3 \pmod 4$. So we observe that

$$n_1n_2 \equiv 1 \pmod 4, \qquad n_1, n_2 \in \mathcal{N}. \tag{8}$$

Consider the sum

$$S = \sum_{p\in[Q,2Q]}\left|\sum_{n\in\mathcal{N}}\left(\frac{n}{p}\right)\right|^2$$

of Legendre symbols. Clearly, if $\mathcal{N}$ consists of only quadratic residues (or zeros) modulo $p$ then

$$\sum_{n\in\mathcal{N}}\left(\frac{n}{p}\right) \ge \#\mathcal{N} - 1.$$

Thus

$$\#\{p \in [Q, 2Q] \ : \ d_u(p) \ge h\} \le \frac{S}{(\#\mathcal{N}-1)^2}. \tag{9}$$

We now choose yet another real parameter $\eta > 0$.

Expanding the summation from primes $p \in [Q, 2Q]$, squaring and extending the summation to all integers $m \in \mathcal{P}(\eta, M)$, we obtain

$$S \le \sum_{m\in\mathcal{P}(\eta,M)}\left|\sum_{n\in\mathcal{N}}\left(\frac{n}{m}\right)\right|^2.$$

Squaring and changing the order of summation, we obtain

$$S \le \sum_{n_1,n_2\in\mathcal{N}}\ \sum_{m\in\mathcal{P}(\eta,M)}\left(\frac{n_1n_2}{m}\right).$$

Finally, using (8), we derive

$$S \le \sum_{n_1,n_2\in\mathcal{N}} \sum_{m\in\mathcal{P}(\eta,M)} \left(\frac{m}{n_1n_2}\right).$$

If $n_1n_2$ is not a perfect square, we apply Corollary 10 with

$$q = n_1n_2 \le (u+h)^2 \le 5Q^2$$

(provided that $Q$ is large enough) to estimate the inner sum. Otherwise, that is, when $n_1n_2$ is a perfect square, we use the trivial bound $\#\mathcal{P}(\eta, M)$ for the inner sum, getting

$$S \le T\#\mathcal{P}(\eta,2Q) + h^2\left(C_0\eta^{\eta^{-1/2}/4-1}\frac{Q}{\log(2Q)} + O\left(Q^{1-\eta}\right)\right),$$

where $T$ is the number of products $n_1n_2$ with $n_1, n_2 \in \mathcal{N}$ that are perfect squares. Thus using (1), we see from we see from (9) that

$$\begin{aligned}
&\#\{p\in[Q,2Q] \ : \ d_u(p)\ge h\}\\
&\qquad \le c_0\frac{QT}{\eta(\#\mathcal{N}-1)^2\log Q}\\
&\qquad\quad + \frac{h^2}{(\#\mathcal{N}-1)^2}\left(C_0\eta^{\eta^{-1/2}/4-1}\frac{Q}{\log(2Q)} + O\left(Q^{1-\eta}\right)\right),
\end{aligned} \tag{10}$$

We now consider two different choices of the set $\mathcal{N}$ depending on the relative size of $u$ and $h$.

If $h \ge u^{1/2}/\log u$, we consider the sets of $\mathcal{N}_1$ and $\mathcal{N}_3$ of square-free integers $n \in \mathcal{I}$ with $n \equiv 1 \pmod 4$ and $n \equiv 3 \pmod 4$ respectively. We now define $\mathcal{N}$ as the largest set out of $\mathcal{N}_1$ and $\mathcal{N}_3$. We see from Corollary 8 that there are

$$\#\mathcal{N}_1 + \#\mathcal{N}_3 \ge (A + o(1))h.$$

Hence $\#\mathcal{N} \ge (A/2+o(1))h$. Clearly for two square-free integers $n_1$ and $n_2$ their product is a perfect square only if $n_1 = n_2$. Hence, $T = \#\mathcal{N}$ and we see from (9) and (10) that in this case

$$\begin{aligned}
&\#\{p\in[Q,2Q] \ : \ d_u(p)\ge h\}\\
&\qquad \le C_1\eta^{-1}\frac{Q}{h\log Q} + C_2\eta^{\eta^{-1/2}/4-1}\frac{Q}{\log Q} + C_3Q^{1-\eta}
\end{aligned} \tag{11}$$

for some absolute constants $C_1$, $C_2$, $C_3$.

We now assume that $h < u^{1/2}/\log u$. If $n_1n_2 = m^2$ for an integer $m$ then, writing $n_1 = k_1d$, $n_2 = k_2d$, with $d = \gcd(n_1, n_2)$, we see that

$$k_1 = m_1^2 \qquad \text{and} \qquad k_2 = m_2^2$$

for some integers $m_1, m_2$. Assume $m_1 < m_2$. Thus

$$u/d \le m_1^2 < m_2^2 \le u/d + h/d.$$

Therefore

$$(u/d)^{1/2} \ll h/d$$

or

$$h \gg (du)^{1/2} \ge u^{1/2},$$

which contradicts our choice of $h$. So taking $\mathcal{N}$ as the set of all integer $n \in \mathcal{I}$ with $n \equiv 1 \pmod 4$ we see that $T = \#\mathcal{N}$ and we obtain (11) again.

We not choose $\eta$ small enough to satisfy

$$C_2 \eta^{\eta^{-1/2}/4-1} \le \frac{1}{3}\kappa$$

then we choose $Q$ large enough to satisfy

$$C_1 \eta^{-1} h^{-1} \le \frac{1}{3}\kappa \qquad \text{and} \qquad C_3 Q^{1-\eta} \le \frac{1}{3}\kappa.$$

With these parameters, we derive from (11) that

$$\#\{p \in [Q, 2Q] \ : \ d_u(p) \ge h\} \le \kappa \frac{Q}{\log Q}.$$

Since $\kappa > 0$ is arbitrary, the result now follows.

## 4. Comments

Note that the inequality $u \le 2Q$ in Theorem 2 is a natural restriction with respect to primes $p \in [Q, 2Q]$. On the other hand, it is also interesting to remove this condition. It is easy to see that the limit $u \le 2Q$ in Theorem 2 can be increased a little if one uses the full power of the Burgess bound. In fact it is easy to see that for quadratic characters only the square-free part of the modulus $q$ matters so one can actually use Lemma 3 with any integer $\nu \ge 1$, see [7, Theorem 12.6]. However for large $u$ one needs some new ideas.

Furthermore, obtaining a version of Theorem 2 with an unlimited $u$ is essentially equivalent to estimating $d(p)$ for almost all primes $p$. Indeed, assume there are $N$ "exceptional" primes $\ell_1, \ldots, \ell_N \in [Q, 2Q]$ with $d(\ell_i) \ge \psi(\ell_i)$, $i = 1, \ldots, N$, for some function $\psi(z)$. This means that there are integers $u_i$ with

$$d_{u_i}(\ell_i) \ge \psi(\ell_i), \qquad i = 1, \ldots, N.$$

Let us choose an integer $u$ satisfying

$$u \equiv u_i \pmod{\ell_i}, \qquad i = 1, \ldots, N.$$

Then we have

$$d_u(\ell_i) = d_{u_i}(\ell_i) \geq \psi(\ell_i), \qquad i = 1, \ldots, N.$$

So a version of Theorem 2 with an unlimited $u$ immediately implies an upper bound on $N$.

Similar questions are also interesting to study for the gaps between primitive roots modulo $p$.

## Acknowledgements

The first author was supported in part by the Russian Fund for Basic Research, Grant N. 14-01-00332, and by the Program Supporting Leading Scientific Schools, Grant Nsh-3082.2014.1.

The second author would like to thank the Max Planck Institute for Mathematics, Bonn, for support and hospitality during his work on this project. The second author was also supported in part by Australian Research Council, Grants DP110100628 and DP130100237

## References

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

[2] R. Dietmann, C. Elsholtz and I. E. Shparlinski, 'On gaps between quadratic non-residues in the Euclidean and Hamming metrics', *Indagationes Mathematicae*, **24** (2013), 930–938.

[3] P. Erdős, 'Remarks on number theory. I', *Mat. Lapok*, **12** (1961), 10–17.

[4] M. Filaseta and O. Trifonov, 'On gaps between squarefree numbers II', *J. London Math. Soc.*, **45** (1992), 215–221.

[5] M. Z. Garaev, S. V. Konyagin, and Y. V. Malykhin, 'Asymptotics for the sum of powers of distances between power residues modulo a prime', *Proc. Steklov Math. Inst.*, vol. 276, 2012, 83–95.

[6] S. W. Graham and C. J. Ringrose, 'Lower bounds for least quadratic non-residues', *Analytic number theory (Allerton Park, IL, 1989)*, Birkhäuser, Boston, MA, 1990, 269–309.

[7] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[8] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory I: Classical theory*, Cambridge Univ. Press, Cambridge, 2006.

[9] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge University Press, 1995.

[10] D. I. Tolev, 'On the distribution of r-tuples of squarefree numbers in short intervals', *Intern J. Number Theory*, **2** (2006), 225–234.

Steklov Mathematical Institute, 8, Gubkin Street, Moscow, 119991, Russia
*E-mail address*: konyagin@mi.ras.ru

Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia
*E-mail address*: igor.shparlinski@unsw.edu.au