On the least quadratic non-residue
†
Y.-K. Lau & J. Wu

Abstract. We prove that for almost all real primitive characters \( \chi_d \) of modulus \(|d|\), the least positive integer \( n_{\chi_d} \) at which \( \chi_d \) takes a value not equal to 0 and 1 satisfies
\[
n_{\chi_d} \ll \log |d|,
\]
and give a quite precise estimate on the size of the exceptional set. Also, we generalize Burgess' bound for \( n_{\chi_d'} \) (with \( p' \) being a prime up to \( \pm \) sign) to composite modulus \(|d|\) and improve Garaev's upper bound for the least quadratic non-residue in Pajtechi-Šapiro's sequence.

§ 1. Introduction

Let \( q \geq 2 \) be an integer and \( \chi \) a non principal Dirichlet character modulo \( q \). Here the evaluation of the least integer \( n_{\chi} \) among all positive integers \( n \) for which \( \chi(n) \neq 0,1 \) is referred as Linnik’s problem. In case \( \chi \) coincides with the Legendre symbol, \( n_{\chi} \) is a least quadratic non-residue. Concerning the size of \( n_{\chi} \), Pólya-Vinogradov’s inequality
\[
\max_{x \geq 1} \left| \sum_{n \leq x} \chi(n) \right| \ll q^{1/2} \log q
\]
implies trivially \( n_{\chi} \ll q^{1/2} \log q \). But for prime \( q \), Vinogradov [24] proved the better bound
\[
n_{\chi} \ll q^{1/2(\sqrt{7})} (\log q)^2
\]
by combining a simple argument with (1.1). He also conjectured that \( n_{\chi} \ll \varepsilon q^\varepsilon \) for all integers \( q \geq 2 \) and any \( \varepsilon > 0 \). Under the Generalized Riemann Hypothesis (GRH), Linnik [18] settled this conjecture, and later Ankeny [1] gave a sharper estimate
\[
n_{\chi} \ll (\log q)^2
\]
(still assuming GRH). Burgess ([3], [4], [5]) wrote a series of important papers on sharpening (1.1). His well known estimate on character sums is as follows: For any \( \varepsilon > 0 \), there is \( \delta(\varepsilon) > 0 \) such that
\[
\left| \sum_{n \leq x} \chi(n) \right| \ll \varepsilon xq^{-\delta(\varepsilon)}
\]
provided \( x \geq q^{1/3+\varepsilon} \). The last condition can be improved to \( x \geq q^{1/4+\varepsilon} \) if \( q \) is cubefree. When \( q \) is prime, he deduced, via (1.4) and Vinogradov’s argument,

\[
(1.5) \quad n_\chi \ll \varepsilon q^{1/(4\sqrt{e})+\varepsilon}.
\]

Since Burgess’ estimate (1.4) on character sums holds for composite modulus, one expects a bound analogous to (1.5) for \( n_\chi \) in general cases, but this seems not available in literature. Our first result is to propose such a generalisation, by modifying Vinogradov’s argument.

**Theorem 1.** Let \( \varepsilon \) be an arbitrarily small positive number. For all integers \( q \geq 2 \) and \( \chi \) non principal characters \((\text{mod } q)\), we have

\[
(1.5) \quad n_\chi \ll \varepsilon \begin{cases} 
q^{1/(4\sqrt{e})+\varepsilon} & \text{if } q \text{ is cubefree,} \\
q^{1/(3\sqrt{e})+\varepsilon} & \text{otherwise.}
\end{cases}
\]

The proof of Theorem 1 will be given in the Section 2.

Let us now focus on real primitive characters. Denote \( \mathcal{D} \) (resp. \( \mathcal{D}(Q) \)) to be the set of fundamental discriminants \( d \) (resp. with \(|d| \leq Q\)), that is, the set of non-zero integers \( d \) which are products of coprime factors of the form \(-4, 8, -8, p' \) where \( p' := (-1)^{(p-1)/2}p \) (\( p \) odd prime). Also, we write \( \mathcal{K} \) (resp. \( \mathcal{K}(Q) \)) for the set of real primitive characters (resp. with modulus \( q \leq Q \)). Then there is a bijection between \( \mathcal{D} \) and \( \mathcal{K} \) given by

\[
d \mapsto \chi_d \left( \frac{d}{\cdot} \right)_K,
\]

where \( \left( \frac{d}{\cdot} \right)_K \) is the Kronecker symbol. Note that the modulus of \( \chi_d \) equals \(|d|\) and

\[
(1.6) \quad |\mathcal{D}(Q)| = |\mathcal{K}(Q)| = \frac{6}{\pi}Q + O(Q^{1/2}).
\]

In the opposite direction of (1.2), Fridlender [12], Salié [23] and Chowla & Turán (see [10]) independently showed that there are infinitely many primes \( p \) for which

\[
(1.7) \quad n_{\chi_{p'}} \gg \log p,
\]

or in other words, \( n_{\chi_{p'}} = \Omega(\log p) \). Under GRH, Montgomery [20] gave a stronger result \( n_{\chi_{p'}} = \Omega(\log p \log_2 p) \), where \( \log_k \) denotes the \( k \)-fold iterated logarithm. Without any assumption Graham & Ringrose [14] obtained \( n_{\chi_{p'}} = \Omega(\log p \log_3 p) \). In view of these results, it is natural to wonder what is the size of the majority of \( n_{\chi_{p'}} \), or more generally \( n_{\chi_d} \). Indeed the density of \( p' \) for which \( n_{\chi_{p'}} \) satisfies (1.7) is low. This can be seen from Erdős’ result [11],

\[
(1.8) \quad \lim_{x \to \infty} \frac{1}{\pi(x)} \sum_{p \leq x} n_{\chi_{p'}} = \text{constant},
\]

where \( \pi(x) \) denotes the number of primes up to \( x \). This result is extended and refined by Elliott in [7] and [8]. Using (1.8) or its refinement in [7], it follows, for any fixed constant \( \delta > 0 \), that

\[
(1.9) \quad \sum_{p \leq x, n_{\chi_{p'}} \geq \delta \log p} 1 \ll_{\delta} \frac{x}{(\log x)^2}.
\]
In [6], Duke & Kowalski indicated: Let $\alpha > 1$ be given. Denote by $N(Q, \alpha)$ the number of primitive characters $\chi$ (not necessarily real) of modulus $q \leq Q$ such that $\chi(n) = 1$ for all $n \leq (\log Q)^\alpha$ and $(n, q) = 1$. Then one has

$$N(Q, \alpha) \ll \varepsilon Q^{2/\alpha + \varepsilon}$$

for all $\varepsilon > 0$. Therefore

$$|\{d \leq Q : n_{\chi_d} \geq (\log Q)^\alpha\}| \ll \varepsilon Q^{2/\alpha + \varepsilon}.$$

However, in view of (1.6) this result is non-trivial only when $\alpha > 2$ and it tells that $n_{\chi_d} \geq (\log |d|)^{2 + \varepsilon}$ for almost all fundamental discriminants $d$. Very recently Baier [2] improved $2 + \varepsilon$ to $1 + \varepsilon$ by using the large sieve inequality of Heath-Brown [15] for real primitive characters. However, the argument is unable to cover the case $\alpha = 1$ or to provide information on the sparsity of the primes $p$ with $n_{\chi_p} \gg \log p$ as in (1.9).

Our second result is to supplement the case $\alpha = 1$, using the large sieve inequality of Elliott-Montgomery-Vaughan (see [9] and [21]). We obtain an almost all result, which is strong enough to yield a tighter estimate on the low density of exceptional non-residues than in (1.9).

**Theorem 2.** For $2 \leq P \leq Q$, define

$$E(Q, P) := \{d \in \mathcal{D}(Q) : \chi_d(p) = 1 \text{ for } P < p \leq 2P \text{ and } p \nmid |d|\}.$$

Then there are two absolute positive constants $C$ and $c$ such that

$$|E(Q, P)| \ll Qe^{-c(\log Q)/\log_2 Q}$$

holds uniformly for $Q \geq 10$ and $C \log Q \leq P \leq (\log Q)^2$. In particular we have

$$n_{\chi_d} \ll \log |d|$$

for all but except $O(Qe^{-c(\log Q)/\log_2 Q})$ characters $\chi_d \in K(Q)$.

Sections 3 and 4 are devoted to the proof of Theorem 2.

Theorem 3 (essentially due to Graham & Ringrose [14]) shows that the upper bound for exceptional real primitive characters set is optimal. Graham & Ringrose considered a problem of the quasi-random graphs (Paley graphs) which leads to study the lower bound for the sum of the right-hand side of (6.5) below. This will also be the essential part of our proof of Theorem 3. We shall provide the salient points along the line of arguments in [14] to prove Theorem 3, see Sections 5 and 6.

**Theorem 3.** For any fixed constant $\delta > 0$, there are a sequence of positive real numbers $\{Q_n\}_{n=1}^\infty$ with $Q_n \to \infty$ and a positive constant $c$ such that

$$\sum_{Q_n^{1/2} < p \leq Q_n \atop n_{\chi_p} \geq \delta \log p} 1 \gg_\delta Q_ne^{-c(\log Q_n)/\log_2 Q_n}.$$ 

Further if we assume that both $L_1(s, P)$ and $L_4(s, P)$ defined in (5.3) below have no exceptional zeros in the region (5.4), then (1.12) holds for all $Q \geq 10$.

Finally we consider the least quadratic non-residue problem in Pajtechi-Šapiro’s sequence $\{[n^c]\}_{n=1}^\infty$, where $c > 1$ is a constant and $[t]$ denotes the integral part of $t \in \mathbb{R}$. Denote by $n_{\chi_p, c}$
the least positive integer \( n \) such that \([n^c]\) is a quadratic non-residue \((\mod p)\). Garaev \cite{Gar13} proved that for \(1 < c < \frac{12}{11}\) and any \( \varepsilon > 0 \), one has

\[
n_{\chi_p',c} \ll_{c,\varepsilon} p^{3/8(3-2c)\sqrt{e}+\varepsilon}
\]

for all primes \( p \). He pointed out also that by the method of exponential pairs the range of \( c \) and the exponent of \( p \) can be improved to \(1 < c < \frac{12}{11} + 0.00257 \cdots\) and \(1/(8(1-\theta_2 c)\sqrt{e})\), respectively, where \( \theta_2 = 0.66451 \cdots \). Here we propose a further improvement by applying a recent result of Robert & Sargos \cite{RS22}, and give an almost result based on Theorem 2.

**Theorem 4.** Let \(1 < c < \frac{32}{29}\). Then for all primes \( p \) and any \( \varepsilon > 0 \), we have

\[
n_{\chi_p',c} \ll_{c,\varepsilon} p^{9/((64 - 40c)\sqrt{e})+\varepsilon}.
\]

For all but except \( O\left(Qe^{-c(\log Q)/\log_2 Q}\right) \) primes \( p \) with \( p \leq Q \), we have

\[
n_{\chi_p',c} \ll_{c,\varepsilon} (\log p)^{9/(16-10c)+\varepsilon}.
\]

We prove Theorem 4 in Section 7.

Our range of \( c \) is larger than \(\frac{12}{11} + 0.01253 \cdots\) \((\frac{32}{29} = \frac{12}{11} + 0.019794 \cdots)\) and our exponent is definitely better than (1.13) but is smaller than \(1/((64-40c)\sqrt{e})\) only when \( c > 1/(9\theta_2 - 5) = 1/0.019794 \cdots \). It is possible to give a slightly better result with Huxley’s estimates for exponential sums \cite[§ 18.5]{Hux66}. We can also generalize Theorem 4 to composite modulus \(|d|\) as in Theorem 1, but with smaller range of \( c \) and larger exponent of \(|d|\).

\[\section{2. Vinogradov’s argument and proof of Theorem 1}

Without loss of generality we assume \( n_\chi \geq q^{1/(4\sqrt{e})} \) (otherwise there is nothing to prove). Let \( x \) be a number specified later but satisfy

\[q > x \geq \begin{cases} \frac{1}{4+\varepsilon} q & \text{if } q \text{ is cubefree}, \\ \frac{1}{3+\varepsilon} q & \text{otherwise} \end{cases}\]

By Burgess’ well known estimate (1.4) on character sums, for any \( \varepsilon > 0 \) there are two positive constants \( C_\varepsilon \) and \( \delta(\varepsilon) > 0 \) such that

\[
C_\varepsilon q x^{3/4(\theta-\varepsilon)} \geq \left| \sum_{n \leq x} \chi(n) \right| \geq \sum_{n \leq x} \left( 1 - 2 \sum_{\substack{n \leq x \\{n,q\}=1 \}} 1 \right) \geq \sum_{\substack{n \leq x \\{n,q\}=1 \}} \left( 1 - 2 \sum_{\substack{n \chi < p \leq x \\{m,q\}=1 \}} 1 \right).
\]

As usual we denote by \( \varphi(n) \) the Euler function, \( \mu(n) \) the Möbius function and \( \omega(n) \) the number of distinct prime factors of \( n \). With the Möbius inversion formula, we have, for some \(|\theta| \leq 1\),

\[
\sum_{n \leq x} 1 = \sum_{d | q} \mu(d) \sum_{m \leq x/d} 1 = \frac{\varphi(q)}{q} x + \theta 2^{c(q)}.
\]
To estimate the last double sum on the right-hand side of (2.1), we divide the sum over \( p \) into two parts according as \( n_x < p \leq x/2^{\omega(q)} \) or \( x/2^{\omega(q)} < p \leq x \). By (2.2), the first part contributes at most

\[
(2.3) \sum_{n_x < p \leq x/2^{\omega(q)}} \left( \frac{\varphi(q)}{q} \frac{x}{p} + 2^{\omega(q)} \right) \leq \frac{\varphi(q)}{q} x \left\{ \log \left( \frac{\log x}{\log n_x} \right) + O \left( e^{-\sqrt{\log n_x}} \right) \right\} + \frac{(1 + \varepsilon)x}{\log(x/2^{\omega(q)})} \leq \frac{\varphi(q)}{q} x \log \left( \frac{\log x}{\log n_x} \right) + (1 + 2\varepsilon) \frac{x}{\log x}.
\]

Note that \( 2^{\omega(q)} \ll x^{\varepsilon} \) and \( n_x \geq q^{1/(4\sqrt{n})} \). For the second part, we interchange the summations and apply the Rankin trick,

\[
\sum_{x/2^{\omega(q)} < p \leq x} \sum_{m \leq x/p} 1 \leq \sum_{1 \leq m \leq x/2^{\omega(q)}} \sum_{p \leq x/m} \frac{1}{m} \ll \frac{x}{\log x} \prod_{p \leq x/2^{\omega(q)}} \left( \frac{1 - 1/p}{p} \right)^{-1} \leq \frac{\varphi(q)}{q} \frac{x}{\log x} \prod_{p \mid m} \left( \frac{1 - 1/p}{p} \right)^{-1} \times \prod_{p \leq x/2^{\omega(q)}} \left( 1 - \frac{1}{p} \right)^{-1}.
\]

In virtue of the simple estimates

\[
\prod_{p > x/2^{\omega(q)}} \left( 1 - \frac{1}{p} \right)^{-1} \ll \exp \left\{ \sum_{p > x/2^{\omega(q)}} \frac{1}{p} \right\} \ll \exp \left\{ \frac{\omega(q)}{2^{\omega(q)}} \right\} \ll 1,
\]

\[
\prod_{p \leq x/2^{\omega(q)}} \left( 1 - \frac{1}{p} \right)^{-1} \ll \exp \left\{ \sum_{p \leq x/2^{\omega(q)}} \frac{1}{p} \right\} \ll \omega(q),
\]

it follows immediately that

\[
(2.4) \sum_{x/2^{\omega(q)} < p \leq x} \sum_{m \leq x/p} \frac{1}{m} \ll \frac{\varphi(q)}{q} \frac{\omega(q)}{\log x}.
\]

Inserting (2.2), (2.3) and (2.4) into (2.1), we conclude

\[
C_x x^{q^{-\delta(c)}} \geq \frac{\varphi(q)}{q} x \left\{ 1 - 2 \log \left( \frac{\log x}{\log n_x} \right) \right\} - 2^{\omega(q)} - (1 + 2\varepsilon) \frac{x}{\log x} - C_x \frac{\varphi(q)}{q} \frac{\omega(q)}{\log x}.
\]

¿From this we deduce that

\[
\log \left( \frac{\log x}{\log n_x} \right) \geq \frac{1}{2} - C_x q^{1-\delta(c)} \varphi(q) - \frac{(1/2 + \varepsilon)q}{\varphi(q) \log x} - \frac{C_x \omega(q)}{2 \log x} \geq \frac{1}{2} - C_x \left( \frac{q}{\varphi(q) \log x} + \frac{\omega(q)}{\log x} \right)
\]
provided \( q \geq q_0(\varepsilon) \). Since \( q/\varphi(q) \log x + \omega(q)/\log x \ll (\log_2 q)^{-1} \), the preceeding inequality implies

\[
 n_x \ll x^{1/\sqrt{x}} \exp \left\{ Q \left( \frac{q}{\varphi(q)} + \omega(q) \right) \right\},
\]

which gives the required result, by taking

\[
 x = \begin{cases} 
 q^{1/4 + \varepsilon} & \text{if } q \text{ is cubefree}, \\
 q^{1/3 + \varepsilon} & \text{otherwise}.
\end{cases}
\]

This completes the proof of Theorem 1. \( \square \)

§ 3. A large sieve inequality of Montgomery-Vaughan

Our key tool for proving Theorem 2 is a large sieve inequality of Montgomery & Vaughan in [21, page 1050] following from [21, Lemma 2]. Here we state a slightly refined version. Their original statement absorbs the factors \((6/\log P)^{j} \) and \((6/(\log P)^2)^j \) in the implied constant. We reproduce here their proof with a minuscule modification.

**Lemma 1.** We have

\[
(3.1) \quad \sum_{d \in \mathcal{D}(Q)} \left| \sum_{P < p \leq 2P} \frac{\chi_d(p)}{p} \right|^{2j} \ll Q \left( \frac{6j}{P \log P} \right)^j + \left( \frac{6P}{(\log P)^2} \right)^j
\]

uniformly for \( 2 \leq P \leq Q \) and \( j \geq 1 \). The implied constant is absolute.

**Proof.** Since \( \chi_d(n) \) is completely multiplicative on \( n \), we can write

\[
 \left( \sum_{P < p \leq 2P} \frac{\chi_d(p)}{p} \right)^j = \sum_{P | m \leq (2P)^j} \frac{a_j(m)}{m} \chi_d(m),
\]

where

\[
 a_j(m) := |\{(p_1, \ldots, p_j) : p_1 \cdots p_j = m, \ P < p_i \leq 2P\}|.
\]

By Lemma 2 of [21] with the choice of parameters

\[
 X = P^j, \quad Y = (2P)^j \quad \text{and} \quad a_m = a_j(m)/m,
\]

it follows that as \( a_j(m_1) a_j(m_2) \leq a_{2j}(n^2) \) for \( n^2 = m_1 m_2 \),

\[
 (3.2) \quad \sum_{d \in \mathcal{D}(Q)} \left| \sum_{P < p \leq 2P} \frac{\chi_d(p)}{p} \right|^{2j} \ll Q \sum_{P | n \leq (2P)^j} \frac{a_{2j}(n^2)}{n^2} + \left( \sum_{P < p \leq 2P} \frac{1}{p^{3/2}} \right)^j.
\]

Writing \( n = p_1^{\nu_1} \cdots p_i^{\nu_i} \) with \( \nu_1 + \cdots + \nu_i = j \), we have

\[
 a_{2j}(n^2) = \frac{(2j)!}{(2\nu_1)! \cdots (2\nu_i)!} \left( \frac{2j!}{(2\nu_1)!} \frac{\nu_1!}{(2\nu_1)!} \cdots \frac{\nu_i!}{(2\nu_i)!} \right) a_j(n).
\]
From this, it is easy to see \( a_{2j}(n^2) \leq j^2 a_j(n) \), and thus
\[
\sum_{P^j < n \leq (2P)^j} \frac{a_{2j}(n^2)}{n^2} \leq j^2 \sum_{P^j < n \leq (2P)^j} \frac{a_j(n)}{n^2} = \left( j \sum_{P < p \leq 2P} \frac{1}{P^2} \right)^j \leq \left( \frac{6j}{P \log P} \right)^j.
\]
Inserting this into (3.2) and using the estimate
\[
\sum_{P < p \leq 2P} \frac{1}{p^{1/2}} \leq \frac{6P^{1/2}}{\log P},
\]
we obtain the required result (3.1).

§ 4. Proof of Theorem 2

Define
\[
\mathcal{E}^*(Q, P) := \{ d \in \mathcal{D}(Q) : Q^{1/2} \leq |d| \leq Q \text{ and } \chi_d(p) = 1 \ (P < p \leq 2P, \ p \nmid |d|) \}.
\]
Let \( C \log Q \leq P \leq (\log Q)^2 \). For \( d \in \mathcal{E}^*(Q, P) \), we invoke the prime number theorem to deduce
\[
\sum_{P < p \leq 2P} \frac{\chi_d(p)}{p} = \sum_{P < p \leq 2P} \frac{1}{p} - \sum_{P < p \leq 2P, p \nmid |d|} \frac{1}{p} \geq \frac{\log 2 + o(1)}{\log P} - \frac{(1 + o(1)) \log Q}{P \log_2 Q} \geq \frac{\log 2 - 2/C + o(1)}{\log P} > \frac{1}{2 \log P},
\]
provided \( C \) is sufficiently large. It is apparent from (3.1) that
\[
\left| \mathcal{E}^*(Q, P) \right| \leq \sum_{d \in \mathcal{D}(Q)} \left| \sum_{P < p \leq 2P} \frac{\chi_d(p)}{p} \right|^{2j} \leq Q \left( \frac{6j}{P \log P} \right)^j + \left( \frac{6P}{(\log P)^2} \right)^j.
\]
Hence we obtain
\[
\left| \mathcal{E}^*(Q, P) \right| \ll Q(12j \log P/P)^j + (12P)^j
\]
uniformly for \( C \log Q \leq P \leq (\log Q)^2 \) and \( j \geq 1 \). Taking
\[
j = \left\lceil \frac{\log Q}{48 \log P} \right\rceil + 1,
\]
a simple calculation shows that
\[ |\mathcal{E}^*(Q, P)| \ll Q e^{-c \log Q / \log_2 Q} \]
with \( c = (\log 2) / 48 \). This implies (1.10).

Finally let
\[ \mathcal{E}^*(Q) := \{ d \in \mathcal{D}(Q) : d \leq Q^{1/2} \} \cup \mathcal{E}^*(Q, C \log Q). \]
Then by (1.10), we have
\[ |\mathcal{E}^*(Q)| \ll Q e^{-c \log Q / \log_2 Q}; \]
and for any \( d \in \mathcal{D}(Q) \setminus \mathcal{E}^*(Q) \) there is a prime number \( p = \log Q \approx \log |d| \) such that \( \chi_d(p) \neq 1 \), which implies (1.11). The proof is complete.

\[ \text{§ 5. Graham-Ringrose’s method} \]

In this section, we shall state and extend the main results of ([14], Theorems 2, 3 and 4) for our purposes. For characters of certain moduli, Graham & Ringrose [14] obtained a wide zero-free region and good zero density estimates for the corresponding Dirichlet \( L \)-functions. The main ingredient of their method is an \( q \)-analogue of van der Corput’s result, which can be stated as follows: Suppose that \( q = 2^s r \), where \( 0 \leq \nu \leq 3 \) and \( r \) is an odd squarefree integer, and that \( \chi \) is a non-principal character mod \( q \). Let \( p \) be the largest prime factor of \( q \). Suppose that \( k \) is a non-negative integer, and \( K = 2^k \). Finally, assume that \( N \leq M \). Then
\[ \sum_{M < n \leq M + N} \chi(n) \ll M^{1 - \frac{k+1}{8K} - \frac{3}{2k} + \frac{1}{2k} + \frac{1}{4k} + \frac{1}{8K} + \frac{1}{16K} - \frac{1}{64K}} (\log q)^{\frac{k+1}{8K} - 1} \sigma^{-1}(q), \]
where \( \sigma(q) := \sum_{d | q} d^\nu \) and \( d(q) := \sigma_0(q) \). The implied constant is absolute.

Recall that for any odd prime \( p \),
\[ \chi_s(p) = \left( \frac{2}{p} \right), \quad \chi_{q'}(p) = \left( \frac{q}{p} \right), \quad \chi_{q'}(p) = \left( \frac{q}{p} \right) (q \text{ odd prime, } q' := (-1)^{(q-1)/2}) \]
by definition. For squarefree \( m \geq 2 \), the character \( \chi_m := \prod_{p | m} \chi_{p} \) for odd \( m \) or \( \chi_m := \chi_8 \chi_{m'} \) for \( m = 2m' \) is a real primitive of modulus \( m \) or \( 4m \), respectively. By convention, we set \( \chi_1 \equiv 1 \). Moreover, if \( \chi_4 \) is the real primitive character mod 4, i.e. \( \chi_4(n) = (-1)^{(n-1)/2} \) for odd \( n \), then \( \chi_{4m} := \chi_4 \chi_m \) is also a real primitive character of modulus \( 4m \).

Let
\[ P_y := \prod_{p \leq y} p = e^{(1 + o(1)) y} \quad (y \to \infty), \]
and define for \( \ell = 1 \) or 4,
\[ L_\ell(s, P_y) := \prod_{m | P_y} L(s, \chi_{\ell m}), \]
where \( L(s, \chi_{\ell m}) \) is the Dirichlet \( L \)-function associated to \( \chi_{\ell m} \). Denote by \( N_\ell(\alpha) \) the number of zeros of \( L_\ell(s, P_y) \) in the rectangle
\[ \alpha \leq \sigma \leq 1 \quad \text{and} \quad |\tau| \leq \log P_y. \]
Here and in the sequel we implicitly define the real numbers \( \sigma \) and \( \tau \) by the relation \( s = \sigma + i \tau \).

The next lemmas 2, 3 and 4 are trivial extensions of Theorems 2, 3 and 4 of [14], respectively.
Lemma 2. Let \( y \geq 100 \). Then there is an absolute positive constant \( C_1 \) such that the \( L \)-function \( \prod_{\ell=1,4} L_\ell(s, P_y) \) has at most one zero in the region

\[
\sigma \geq 1 - \frac{C_1 (\log_2 P_y)^{1/2}}{\log P_y} \quad \text{and} \quad |\tau| \leq \log P_y.
\]

The exceptional zero, if exists, is real.

Proof. As the crucial estimate (5.1) holds for all non-principal primitive characters of modulus \( q = 2^\nu r \geq 2 \) with \( 0 \leq \nu \leq 3 \) and \( r \) being odd squarefree. Consider the case \( \nu = 0 \) or 3, and \( \nu = 2 \) or 3, respectively. We see that (5.1) applies to \( \chi_m \) and \( \chi_{4m} \) for any \( m | P_y \). It follows that [14, Lemma 6.1] is valid for these characters. Proceeding with the same argument, we have [14, Lemma 6.2] for our \( L \)-function \( \prod_{\ell=1,4} L_\ell(s, P_y) \) in place of \( L(s, P_y) \) there. Then the same proof of [14, Theorem 2] will give the desired result. (Note that the value of \( \phi \) suffers a negligible change when \( P_y \) is replaced by \( 4P_y \) or \( 8P_y \).) The exceptional zero must be real, for otherwise, its conjugate is another zero in the specified region. \( \square \)

Lemma 3. Let \( C_1 \) be as in Lemma 2. There is a sequence of positive real numbers \( \{y_n\}_{n=1}^\infty \) with \( y_n \to \infty \) such that both \( L_1(s, P_{y_n}) \) and \( L_4(s, P_{y_n}) \) have no zeros in the region

\[
\sigma \geq 1 - \eta(y_n) \quad \text{and} \quad |\tau| \leq \log P_{y_n},
\]

where

\[
\eta(y) := \frac{C_1 (\log_2 P_y)^{1/2}}{2 \log P_y}.
\]

Proof. Similar to [14, Theorem 3], our proof is also based on an interesting argument attributed to Maier [19]. Suppose that for some \( y \), the product \( L_1(s, P_y)L_4(s, P_y) \) has an exceptional zero in the region (5.4). That is, it has a real zero \( \beta > 1 - 2\eta(y) \). In view of (5.2), we can take \( y_n \geq y \) such that

\[
\eta(y_n) < 1 - \beta < 2\eta(y_n).
\]

By Lemma 2, \( \beta \) is the only exceptional zero of \( \prod_{\ell=1,4} L_\ell(s, P_{y_n}) \) in the region

\[
\sigma > 1 - 2\eta(y_n) \quad \text{and} \quad |\tau| \leq \log P_{y_n}.
\]

Together with the first inequality in (5.6), this forces \( \prod_{\ell=1,4} L_\ell(s, P_{y_n}) \) to have no zero in the region (5.5). It follows that we can find a sequence of positive real numbers \( \{y_n\}_{n=1}^\infty \) with \( y_n \to \infty \) such that both \( L_1(s, P_{y_n}) \) and \( L_4(s, P_{y_n}) \) have no zero in this region. \( \square \)

Lemma 4. Let \( \ell = 1 \) or 4 and \( y \geq 100 \). Then there is an absolute constant \( C_2 \) such that

\[
N_\ell(\alpha) \ll \begin{cases} 
\exp \left\{ \frac{C_2(1 - \alpha) \log P_y}{\sqrt{\log_2 P_y}} + \frac{\log_3 P_y}{2} \right\} & \text{if } \alpha \geq 1 - \eta_1(y), \\
\exp \left\{ \frac{C_2(1 - \alpha) \log P_y}{\log(1/(1 - \alpha))} \right\} & \text{if } \alpha < 1 - \eta_1(y),
\end{cases}
\]

where

\[
k_0(y) := [(\log_2 P_y)^{1/2}] \quad \text{and} \quad \eta_1(y) := \frac{k_0(y)}{2(2k_0(y) - 2)}.
\]
Proof. The case of $\ell = 1$ has been done in [14, Sections 7 and 8] and $N_4(\alpha)$ can be treated in the same way by applying (5.1) to our $\chi_{4m}$. \qed

§ 6. Proof of Theorem 3

In this section, we denote by $p$ and $q$ prime numbers. Define

$$\mathbb{P}_y := \{p : p \equiv 1 \pmod{4} \text{ and } \chi_p(q) = 1 \text{ for all } q \leq y\}.$$

Clearly we have $n_{\chi_p} > y$ for any $p \in \mathbb{P}_y$. We shall first show that the set $\mathbb{P}_y$ is not too small for suitable $y$.

**Proposition.** Let $\delta > 0$ be a fixed small constant and $y(x)$ be a strictly increasing function defined on $[120, \infty)$ satisfying

$$(6.1) \quad (\log x)\frac{e^{-\delta(\log x)^{1/2}}}{\log^{3} x} \leq y(x) \leq \frac{\delta}{\log x} \log 3x.$$

Then there are a positive constant $c = c(\delta)$ and a sequence of positive real numbers $\{x_n\}_{n=1}^{\infty}$ with $x_n \to \infty$ such that

$$(6.2) \quad \sum_{x_n^{1/2} < \mathbb{P}_y \leq x \log x \atop p \in \mathbb{P}_y(x_n)} 1 \gg x_n e^{-cy(x_n)/\log y(x_n)}.$$

Further if we assume that both $L_1(s, \mathbb{P}_y)$ and $L_4(s, \mathbb{P}_y)$ have no zeros in the region (5.4) for all $y \geq 100$, then there is a positive constant $c$ such that for all $x \geq 100$ we have

$$(6.3) \quad \sum_{x^{1/2} < p \leq x \log x \atop p \in \mathbb{P}_y} 1 \gg x e^{-cy(x)/\log y(x)}.$$

Proof. First let $10 \leq y \leq x^{1/2}$. As usual, $\pi(y)$ denotes the number of prime numbers $\leq y$. Clearly we have

$$(6.4) \quad 2^{-\pi(y)-1} \left(1 + \chi_4(p)\right) \prod_{q \leq y} (1 + \chi_p(q)) = \begin{cases} 1 & \text{if } p \in \mathbb{P}_y, \\ 0 & \text{if } p \notin \mathbb{P}_y. \end{cases}$$

When $p$ and $q$ are odd primes with $p \equiv 1 \pmod{4}$, i.e. $\chi_4(p) = 1$, we infer by quadratic reciprocity law that

$$\chi_p(q) = \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \chi_q(p) \quad (q' := (-1)^{(q-1)/2}q).$$

Note also for odd prime $p$,

$$\chi_p(2) = \left(\frac{p}{2}\right) = \left(\frac{2}{p}\right) = \chi_8(p).$$

Thus we can replace $\chi_p(q)$ by $\left(\frac{q}{p}\right)$ in (6.4) to write

$$\sum_{x^{1/2} < p \leq x \log x \atop p \in \mathbb{P}_y} \frac{1}{2^{\pi(y)+1}} \sum_{x^{1/2} < p \leq x \log x} (1 + \chi_4(p)) \prod_{q \leq y} \left(1 + \left(\frac{q}{p}\right)\right).$$
It is convenient to introduce the weight factor \((\log p) \left(e^{-p/(2x)} - e^{-p/x}\right)\) to the summands,

\[
\sum_{\ell^{-1/2} < p \leq x \log x} \frac{1}{2\pi(y)^2 \log x} \sum_{\ell^{-1/2} < p \leq x \log x} (\log p) \left(e^{-p/(2x)} - e^{-p/x}\right) \times (1 + \chi_4(p)) \prod_{q \leq y} \left(1 + \left(\frac{q}{p}\right)\right).
\]

We want to relax the range of the sum over \(p\). To this end, we observe that by the prime number theorem and integration by parts,

\[
\frac{1}{2\pi(y) \log x} \sum_{x \log x < p \leq x^2} (\log p) \left(e^{-p/(2x)} - e^{-p/x}\right) \left(1 + \chi_4(p)\right) \prod_{q \leq y} \left(1 + \left(\frac{q}{p}\right)\right) \ll \sum_{x \log x < p \leq x^2} \left(e^{-p/(2x)} - e^{-p/x}\right) \ll x^{1/2}/\log x.
\]

Combining this with the preceding inequality, we obtain

\[
(6.5) \quad \sum_{\ell^{-1/2} < p \leq x \log x} \frac{1}{2\pi(y)^2 \log x} \sum_{m|P_y} (S_x(m) + S_x(4m)) + O\left(\frac{x^{1/2}}{\log x}\right),
\]

where \(\ell = 1\) or \(4\), and

\[
S_x(\ell m) := \sum_{\ell^{-1/2} < p \leq x^2} (\log p) \left(e^{-p/(2x)} - e^{-p/x}\right) \chi_{\ell m}(p).
\]

By the Perron formula, we can write

\[
(6.6) \quad S_x(\ell m) = \frac{1}{2\pi i} \int_{2 - \infty}^{2 + \infty} \frac{L'}{L}(s, \chi_{\ell m}) (2^s - 1) \Gamma(s) x^s \, ds + O\left(x^{1/2}/\log x\right).
\]

We shift the line of integration to \(\sigma = -\frac{3}{4}\). The function \((2^s - 1)\Gamma(s)x^s\) has no pole in the strip \(-\frac{3}{4} \leq \sigma \leq 2\) since the pole of \(\Gamma(s)\) at \(s = 0\) is canceled by the zero of \((2^s - 1)\). Thus the only poles of the integrand in (6.6) occur at \(s = 1\) if \(\ell m = 1\) (note that \(L(s, \chi_1)\) is the Riemann \(\zeta\)-function), or at the zeros \(\rho(\ell m) = \beta(\ell m) + i\gamma(\ell m)\) of \(L(s, \chi_{\ell m})\). It follows that

\[
S_x(\ell m) = \delta_{m,1} x - \sum_{\rho(\ell m)} \left(2^{\rho(\ell m)} - 1\right) \Gamma(\rho(\ell m)) x^{\rho(\ell m)} + O\left(x^{1/2}/\log x\right),
\]

where \(\delta_{m,1} = 1\) if \(j = 1\) and \(0\) otherwise, and the sum is over all zeros with \(0 \leq \beta(\ell m) < 1\).

We write \(N(T, \chi_{\ell m})\) for the number of zeros of \(L(s, \chi_{\ell m})\) in the rectangle \(0 < \beta(\ell m) < 1\) and \(|\gamma| \leq T\). Then we have the classical bound

\[
(6.7) \quad N(T, \chi_{\ell m}) \ll T \log(Tm),
\]

which implies, for any \(\alpha \in (0, 1)\),

\[
(6.8) \quad N_{\ell}(\alpha) \leq \sum_{m|P_y} N(\log P_y, \chi_{\ell m}) \ll 2\pi(y) y^2.
\]
On the other hand, by means of \((2^s - 1)\Gamma(s)x^s \ll x^\sigma|\tau|\varepsilon^{-(\pi/2)|\tau|}\), the contribution of the zeros with \(|\gamma(\ell m)| \geq \log P_y\) to \(S_x(\ell m)\) is \(\ll 1\). Let \(\varepsilon\) be an arbitrarily small positive number. The zeros with \(\beta(\ell m) \leq 1 - \varepsilon\) and \(|\gamma(\ell m)| \leq \log P_y\) contribute

\[
\ll x^{1-\varepsilon}N(\log P_y, \chi_{\ell m}) \ll x^{1-\varepsilon}(\log P_y)^2 \ll x^{1-\varepsilon}y^2.
\]

Combining these with (6.5), we conclude

\[\sum_{x^{1/2} < \rho \leq x \log x} \frac{1}{\rho} \geq \frac{x}{(\log x)^{2\pi(y)+1}} + O\left(x^{1-\varepsilon}2^{\pi(y)}y^2 + \frac{T_1(x,y) + T_4(x,y)}{(\log x)^{2\pi(y)}}\right)\]

uniformly for \(x \geq 10\) and \(1 \leq y \leq x^{1/2}\), where

\[T_\ell(x,y) := \sum_{m \mid P_y} \sum_{\rho(\ell m) \geq 1, \beta(\ell m) \leq \log P_y} x^{\beta(\ell m)}\]

\[= - \int_{1-\varepsilon}^1 x^{\alpha}dN_\ell(\alpha).\]

It remains to estimate \(T_\ell(x,y)\). From now on we take \(y = y(x)\). By integration by parts and by using (6.8), we can deduce

\[T_\ell(x,y) \ll x^{1-\varepsilon}2^{\pi(y)}y^2 + x(\log x)I_\ell,\]

where

\[I_\ell := \int_0^\varepsilon x^{-\beta}N_\ell(1-\beta)d\beta.\]

Let \(\eta = \eta(y)\) and \(\eta_1 = \eta_1(y)\) be defined as in Lemmas 3 and 4, respectively. Set \(\eta_2 := 2y(x)/(\log x)\log y\). It is easy to verify that \(0 < \eta < \eta_1 < \eta_2 < \varepsilon\). (The inequality \(\eta_1 < \eta_2\) governs the lower bound of \(y(x)\) in (6.1).) Thus we can divide the interval \([0, \varepsilon]\) into four subintervals \([0, \eta], [\eta, \eta_1], [\eta_1, \eta_2]\) and \([\eta_2, \varepsilon]\), and denote by \(I_{\ell,0}, I_{\ell,1}, I_{\ell,2}\) and \(I_{\ell,3}\) the corresponding contribution to \(I_\ell\). Plainly we have

\[\frac{1}{2}\log_3 P_y \leq \frac{\eta_1}{4}\log x, \quad \frac{C_2 \log P_y}{\log_2 P_y} \leq \frac{1}{4}\log x, \quad \frac{C_2 \log P_y}{\log(1/\eta_2)} \leq \frac{1}{2}\log x, \quad \frac{y}{\log y} \geq \frac{\eta_2}{2}\log x.\]

(The third inequality governs the upper bound of \(y(x)\) in (6.1).) From Lemma 4 and (6.8), we deduce that

\[I_{\ell,1} \ll \int_\eta^{\eta_1} \exp\left\{-\beta \log x + \frac{C_2 \beta \log P_y}{\log_2 P_y} + \frac{1}{2}\log_3 P_y\right\}d\beta \ll \frac{x^{-\eta/2}}{\log x},\]

\[I_{\ell,2} \ll \int_{\eta_1}^{\eta_2} \exp\left\{-\beta \log x + \frac{C_2 \beta \log P_y}{\log(1/\beta)}\right\}d\beta \ll \frac{x^{-\eta_1/2}}{\log x},\]

\[I_{\ell,3} \ll \int_{\eta_2}^{\varepsilon} \exp\left\{-\beta \log x + \frac{y}{\log y}\right\}d\beta \ll \frac{x^{-\eta_2/2}}{\log x}.\]

Hence, all of them satisfy

\[I_{\ell,i} = o((\log x)^{-1}) \quad (i = 1, 2, 3).\]
If we assume that both $L_1(s, P_y)$ and $L_4(s, P_y)$ have no zeros in the region (5.4) for all $y \geq 100$, then $I_{\ell,0} = 0$. Otherwise we use Lemma 3 to ensure the existence of $\{y_n\}_{n=1}^\infty$ such that $I_{\ell,0} = 0$.

With (6.10), our conclusion is

$$T_\ell(x_n, y_n) = o \left( \frac{x_n}{(\log x_n)^2} \pi(y_n) \right) \quad (n \to \infty),$$

or

$$T_\ell(x, y) = o \left( \frac{x}{(\log x)^2} \pi(y) \right) \quad (x \to \infty)$$

under the assumption that both $L_1(s, P_y)$ and $L_4(s, P_y)$ have no exceptional zeros. Clearly this and (6.9) imply the required result. This completes the proof of Proposition. □

Now we are ready to prove Theorem 3.

Taking $Q_n = x_n \log x_n$ and $y(x) = 100\delta \log x$ in Proposition and noticing that $p \in P_y \Rightarrow n \chi_p \geq y$, we have

$$\sum_{n \chi_p \geq 100\delta \log Q_n} \frac{1}{2} \gg Q_n e^{-c_1(\log Q_n)/\log_2 Q_n}.$$ 

It implies the first assertion of Theorem 3, and the second one can be treated similarly. This concludes Theorem 3. □

§ 7. Proof of Theorem 4

Let $1 < c < \frac{32}{29}$ and $\varepsilon$ be an arbitrary but sufficiently small positive constant. The upshot is to show

$$(7.1) \quad n_{\chi_{\nu'},c} \ll n_{\chi_{\nu'}}^{9/(16-10c)+\varepsilon}$$

whenever $n_{\chi_{\nu'}} \geq N_0(c, \varepsilon)$ for some suitably large constant $N_0(c, \varepsilon)$ depending only on $c$ and $\varepsilon$. Once (7.1) is established, the required results follow from Burgess’ upper bound (1.5) or (1.11).

To prove (7.1), we make use of the observation that the integer $mn_{\chi_{\nu'}}$ is quadratic non-residue for any integer $m < n_{\chi_{\nu'}}$. Now, we want to find a positive $M (< \frac{1}{2} n_{\chi_{\nu'}})$ as small as possible such that

$$(7.2) \quad [n'] = mn_{\chi_{\nu'}}$$

for some integers $m \in (M, 2M]$ and $n > 1$. This implies

$$(7.3) \quad n_{\chi_{\nu'},c} \ll (Mn_{\chi_{\nu'}})^{1/c}$$

which leads to (7.1) with a suitable estimate on $M$.

Apparently, (7.2) is equivalent to

$$(7.4) \quad (mn_{\chi_{\nu'}})^{1/c} \leq n < (mn_{\chi_{\nu'}} + 1)^{1/c}. $$

Denote by $\{x\}$ the fractional part of $x$. Then (7.4) holds if

$$(7.5) \quad 0 < \{(mn_{\chi_{\nu'}} + 1)^{1/c}\} \leq (2^{1/c-2}/c)(Mn_{\chi_{\nu'}})^{1/c-1} =: \Delta < 1 \quad (c > 1), $$
since

\[(mn_{x'} + 1)^{1/c} - (mn_{x'})^{1/c} \geq (1/c)(2Mn_{x'})^{1/c-1}.\]

Let \(\delta_\Delta(t)\) be the periodic function of period 1 such that \(\delta_\Delta(t) = 1\) if \(t \in (0, \Delta]\) and \(= 0\) if \(t \in (\Delta, 1]\). Then (7.5) will follow from

\[(7.6) \sum_{M < m \leq 2M} \delta_\Delta((mn_{x'} + 1)^{1/c}) > 0.\]

Introducing the function \(\psi(t) := \frac{1}{2} - \{t\}\), we can express

\[\delta_\Delta(t) = \Delta + \psi(\Delta - t) - \psi(-t).\]

Thus we have

\[\sum_{M < m \leq 2M} \delta_\Delta((mn_{x'} + 1)^{1/c}) = \Delta M + R,\]

where

\[R := \sum_{M < m \leq 2M} \left(\psi(\Delta - (mn_{x'} + 1)^{1/c}) - \psi(-(mn_{x'} + 1)^{1/c})\right)\]

Consider respectively

\[f(t) = \Delta - ((M + t)n_{x'} + 1)^{1/c}, \quad f(t) = -((M + t)n_{x'} + 1)^{1/c}.\]

Then the treatment of \(R\) is reduced to the sum \(\sum_{M < m \leq 2M} \psi(f(m))\), which can be handled using a recent result in [22] via third derivative of \(f(t)\). Applying Theorem 2 of [22], we obtain

\[R \ll c, \varepsilon \left(M\left(M^{1/c-3n_{x'}^{1/c}}\right)^{3/19} + M^{3/4} + (M^{1/c-3n_{x'}^{1/c}})^{-1/3}\right)M^2.\]

Thus (7.6) will hold provided

\[M^{1-\varepsilon} \geq n_{x'}^{(19c-16)/(16-10c)}.\]

Taking \(M = n_{x'}^{(19c-16)/(16-10c)+\varepsilon}\), it follows that

\[R \leq C_0(c, \varepsilon)n_{x'}^{(10c-16)/(19c)M^2\Delta M}\]

for \(n_{x'} \geq N_1(c, \varepsilon)\) where \(C_0(c, \varepsilon)\) and \(N_1(c, \varepsilon)\) are absolute constants depending only on \(c\) and \(\varepsilon\). The hypothesis \(1 < c < \frac{32}{29}\) yields that \(M < \frac{1}{2}n_{x'}\) for all sufficiently large \(n_{x'}\). Furthermore, this hypothesis ensures that the exponent of \(n_{x'}\) is negative and hence \(R\) is suppressed by \(\Delta M\) for all large \(n_{x'}\). Consequently, we derive (7.6) for \(n_{x'} \geq N_2(c, \varepsilon)\), and therefore (7.1) by inserting the value of \(M\) into (7.3). The proof of Theorem 4 is thus complete.

\[\square\]

References

[2] S. Baier, A remark on the least \(n\) with \(\chi(n) \neq 1\), Preprint.
On the least quadratic non-residue


Department of Mathematics, The University of Hong Kong, Pokfulam Road, Hong Kong

E-mail: yklau@maths.hku.hk

Institut Elie Cartan, UMR 7502 UHP CNRS INRIA, Université Henri Poincaré (Nancy 1), 54506 Vandœuvre-lès-Nancy, France

E-mail: wujie@iecn.u-nancy.fr