



HAL
open science

On values taken by the largest prime factor of shifted primes

Jie Wu

► **To cite this version:**

Jie Wu. On values taken by the largest prime factor of shifted primes. Journal of the Australian Mathematical Society, 2019, 10.1017/S1446788700017511 . hal-02322809

HAL Id: hal-02322809

<https://hal.science/hal-02322809v1>

Submitted on 21 Oct 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

ON VALUES TAKEN BY THE LARGEST PRIME FACTOR OF SHIFTED PRIMES

JIE WU

ABSTRACT. Denote by \mathbb{P} the set of all prime numbers and by $P(n)$ the largest prime factor of positive integer $n \geq 1$ with the convention $P(1) = 1$. In this paper, we prove that for each $\eta \in (\frac{32}{17}, 2.1426\dots)$, there is a constant $c(\eta) > 1$ such that for every fixed non-zero integer $a \in \mathbb{Z}^*$ the set

$$\{p \in \mathbb{P} : p = P(q - a) \text{ for some prime } q \text{ with } p^\eta < q \leq c(\eta)p^\eta\}$$

has relative asymptotic density 1 in \mathbb{P} . This improves a similar result due to Banks & Shparlinski [2, Theorem 1.1], which requires $\eta \in (\frac{32}{17}, 2.0606\dots)$ in place of $\eta \in (\frac{32}{17}, 2.1426\dots)$.

1. INTRODUCTION

The largest prime factors of shifted primes appears in many well-known arithmetic questions (such as the Fermat last theorem, the twin prime conjecture, RSA schemes of cryptology, etc), and their distribution plays a key role. The study of this problem has received much attention. Denote by \mathbb{P} the set of all prime numbers and by $P(n)$ the largest prime factor of the positive integer $n \geq 1$ with the convention $P(1) = 1$. For example, we are interested in the greatest value of θ for which there is a positive proportion of primes p such that $P(p - a) \geq p^\theta$ (see [7, 6, 1, 17, 14]). For given $\theta \in (0, 1)$, we also considered the relative asymptotic density of such primes in \mathbb{P} (see [12, 3, 5]). Motivated by these questions, Liu, Wu & Xi [11] studied the distribution of primes in arithmetic progressions with friable indices, i.e., $\{a + mq\}_m$ friable (recall that a positive integer m is friable if its all prime factors are small), and established analogues of classical Siegel-Walfisz theorem, Bombieri-Vinogradov theorem and Brun-Titchmarsh theorem.

In [2], Banks & Shparlinski studied the related problem of estimating the number of primes p that occur as the largest prime factor of a shifted prime $q - a$ when $q \in \mathbb{P}$ lies in a certain interval determined by p . It is worthy to note that this question has applications in theoretical computer science and has been considered by Vishnoi [16] (in a different form).

For $a \in \mathbb{Z}^*$, real numbers $c > 1$ and $\eta > 0$, define

$$\mathcal{P}_{a,c,\eta} := \{r \in \mathbb{P} : r = P(q - a) \text{ for some prime } q \text{ with } r^\eta < q \leq cr^\eta\}$$

and

$$\pi_{a,c,\eta}(x) := |\{r \leq x : r \in \mathcal{P}_{a,c,\eta}\}|, \quad \pi(x) := |\{r \leq x : r \in \mathbb{P}\}|.$$

Date: May 30, 2019.

2010 Mathematics Subject Classification. 11N05, 11N25, 11N36.

Key words and phrases. Shifted prime, Friable integer, Sieve.

Banks & Shparlinski [2, Theorem 1.1] proved that for every $\eta \in (\frac{32}{17}, 1 + \frac{3}{4}\sqrt{2})$, there exists a constant $c = c(\eta) > 1$ such that the asymptotic formula

$$(1.1) \quad \pi_{a,c,\eta}(x) = \pi(x) + O_{A,a,c,\eta}\left(\frac{x}{(\log x)^A}\right)$$

holds for each fixed non-zero integer $a \in \mathbb{Z}^*$ and any constant $A > 1$. Moreover for $2 \leq \eta < 1 + \frac{3}{4}\sqrt{2}$, this estimate holds for any constant $c > 1$.

The aim of this paper is to improve the result of Banks-Shparlinski by extending the domain of η . Our result is as follows.

Theorem 1. *Let $\eta_0 \approx 2.1426$ be the unique solution of the equation*

$$(1.2) \quad \eta - 1 - 4\eta \log(\eta - 1) = 0.$$

For each real number $\eta \in (\frac{32}{17}, \eta_0)$, there exists a constant $c = c(\eta) > 1$ such that the asymptotic formula (1.1) holds for every fixed non-zero integer $a \in \mathbb{Z}^$ and any $A > 1$, where the implied constant depends only on A, a, c and η . Moreover for $2 \leq \eta < \eta_0$, this asymptotic formula holds for any constant $c > 1$.*

For comparison, we have

$$\frac{32}{17} \approx 1.8823, \quad 1 + \frac{3}{4}\sqrt{2} \approx 2.0606 \quad \text{and} \quad \eta_0 \approx 2.1426.$$

We shall prove Theorem 1 by refining Banks-Shparlinski's argument. Our key point is Proposition 2.1 below, which gives a better upper bound for the counting function (see (2.4) below)

$$\mathcal{Q}_2(r) := \sum_{\substack{y < q \leq cy \\ q \equiv a \pmod{r}, P(q-a) > r}} 1$$

than [2, Formula (9) or Page 143, line 2] of Banks & Shparlinski, who obtained $8\eta(\eta - 2)$ in place of $\frac{4\eta \log(\eta - 1)}{\eta - 1}$. In view of the inequality $\log(1 + t) < t$ for $t > 0$, we see that

$$\eta > 2 \quad \Rightarrow \quad \frac{\log(\eta - 1)}{\eta - 1} < \frac{\eta - 2}{\eta - 1} < \eta - 2.$$

Therefore our bound must be better. This improvement comes from the following two observations:

(i) In many arithmetic applications, the linear sieve is more powerful than the sieve of dimension 2;

(ii) With the help of the Chen-Iwaniec switching principle [4, 8] and our theorem of Bombieri-Vinogradov type (see Proposition 3.2 below), we can sieve the sequence of convolution defined as in (4.1) below by the linear sieve, instead of fixing k and sieving $\{n(knr + a)\}_n$ by the sieve of dimension 2 as in [2].

2. BANKS-SHPARLINSKI'S ARGUMENT AND SKETCH OF THE PROOF OF THEOREM 1

In this section, we shall present the sketch of the proof of Theorem 1 by simplifying the Banks-Shparlinski argument [2]. In view of the Banks-Shparlinski result (1.1), it suffices to prove Theorem 1 for $\eta \in (2, \eta_0)$.

The letters p, q, r and ℓ are always used to denote prime numbers, and $d, m,$ and n always denote positive integers. In what follows, let a and A be as in Theorem 1 and $\eta \in (2, \eta_0)$. Let δ be a sufficiently small positive constant and let $c > 1$ be a parameter to be chosen later. Let $x_0(A, a, \eta, \delta, c)$ be a large constant depending on A, a, η, δ, c at most. For $x \geq x_0(A, a, \eta, \delta, c)$ and $r \in (\frac{1}{2}x, x]$, put $y := r^\eta$.

As usual, for $(a, d) = 1$ define

$$\pi(x; d, a) := \sum_{p \leq x, p \equiv a \pmod{d}} 1.$$

The Bombieri-Vinogradov theorem plays an important role in the Banks-Shparplinski argument. This theorem can be stated as follows: *For any $A > 0$, there exists a constant $B = B(A) > 0$ such that*

$$(2.1) \quad \sum_{d \leq x^{1/2}(\log x)^{-B}} \max_{z \leq x} \max_{(a, d)=1} \left| \pi(z; d, a) - \frac{\pi(z)}{\varphi(d)} \right| \ll_A \frac{x}{(\log x)^A}$$

for all $x \geq 2$, where $\varphi(n)$ denotes the Euler totient function and the implied constant depends on A only.

For $z \leq x^{1/2}(\log x)^{-B}$, put

$$\mathcal{D}(x; z) := \left\{ d \leq z : \left| \pi(x; d, a) - \frac{\pi(x)}{\varphi(d)} \right| \geq \delta \frac{\pi(x)}{\varphi(d)} \right\}.$$

By using (2.1) with $A + 1$ in place of A , we deduce that, for every $d \in \mathcal{D}(x; z)$,
 remove

$$\delta \frac{\pi(x)}{z} |\mathcal{D}(x; z)| \ll_A \frac{x}{(\log x)^{A+1}},$$

which gives immediately

$$(2.2) \quad |\mathcal{D}(x; z)| \ll_{A, \delta} \frac{z}{(\log x)^A}.$$

Define

$$\mathcal{R}(x) := \left\{ \frac{1}{2}x < r \leq x : \pi(y; r, a) \leq (1 + \delta) \frac{\pi(y)}{\varphi(r)} \text{ and } \pi(cy; r, a) \geq (c - \delta) \frac{\pi(y)}{\varphi(r)} \right\}.$$

Since $\eta > 2$, we have $r = y^{1/\eta} \leq y^{1/2}(\log y)^{-B}$. Thus the last estimation in (2.2) with $(x, z) = (y, x)$ implies that

$$(2.3) \quad |\mathcal{R}(x)| = \pi(x) - \pi(\frac{1}{2}x) + O_{A, a, \eta, \delta, c} \left(\frac{x}{(\log x)^A} \right) \quad (x \geq 2).$$

For every prime $r \in \mathcal{R}(x)$, define

$$(2.4) \quad \mathcal{Q}_1(r) := \sum_{\substack{y < q \leq cy \\ P(q-a)=r}} 1 \quad \text{and} \quad \mathcal{Q}_2(r) := \sum_{\substack{y < q \leq cy \\ q \equiv a \pmod{r}, P(q-a) > r}} 1,$$

Then the definition of $\mathcal{R}(x)$ allows us to write

$$(2.5) \quad \begin{aligned} \mathcal{Q}_1(r) &= \pi(cy; r, a) - \pi(y; r, a) - \mathcal{Q}_2(r) \\ &\geq (c - 1 - 2\delta) \frac{\pi(y)}{\varphi(r)} - \mathcal{Q}_2(r). \end{aligned}$$

The following result gives us the required upper bound for $\mathcal{Q}_2(r)$, which constitutes the key to our improvement.

Proposition 2.1. *Under the previous notation, for $r \in \mathbb{P} \cap [\frac{1}{2}x, x]$ we have*

$$(2.6) \quad \mathcal{Q}_2(r) \leq (c-1+2\delta) \frac{4\eta \log(\eta-1)}{\eta-1} \cdot \frac{\pi(y)}{\varphi(r)} \left\{ 1 + O\left(\frac{1}{\sqrt[3]{\log r}}\right) \right\}$$

for $x \geq x_0(A, a, \eta, \delta, c)$.

In Section 4, we shall prove this proposition. Now we suppose this proposition and complete the proof of Theorem 1.

Inserting (2.6) into (2.5), it follows that

$$\mathcal{Q}_1(r) \geq \frac{c-1-2\delta}{\eta-1} \left(\eta-1-4\eta \log(\eta-1) \cdot \frac{c-1+2\delta}{c-1-2\delta} \right) \frac{\pi(y)}{\varphi(r)}.$$

Taking $c = 1 + 2\sqrt{\delta}$, we can find that

$$\begin{aligned} \mathcal{Q}_1(r) &\geq 2 \frac{\sqrt{\delta}-\delta}{\eta-1} \left(\eta-1-4\eta \log(\eta-1) \cdot \frac{1+\sqrt{\delta}}{1-\sqrt{\delta}} \right) \frac{\pi(y)}{\varphi(r)} \\ &= \{G(\eta) + O(\sqrt{\delta})\} 2\sqrt{\delta} \frac{1-\sqrt{\delta}}{\eta-1} \cdot \frac{\pi(y)}{\varphi(r)}, \end{aligned}$$

where

$$(2.7) \quad G(\eta) := \eta - 1 - 4\eta \log(\eta - 1).$$

It is easy to see that $G(\eta)$ is decreasing on $[2, \infty)$ and $G(2) = 1$. Therefore there is a unique real number $\eta_0 \in (2, \infty)$ such that $G(\eta_0) = 0$ and for $\eta \in [2, \eta_0)$ we have the inequality

$$(2.8) \quad \mathcal{Q}_1(r) \gg_{A,a,\eta,\delta} \frac{\pi(y)}{\varphi(r)}$$

for $x \geq x_0(A, a, \eta, \delta, c)$. From (2.8), we deduce that

$$\mathcal{R}(x) \subseteq \mathcal{P}_{a,c,\eta} \cap \left(\frac{1}{2}x, x\right].$$

Combining this with (2.3) lead to

$$\pi_{a,c,\eta}(x) - \pi_{a,c,\eta}\left(\frac{1}{2}x\right) = \pi(x) - \pi\left(\frac{1}{2}x\right) + O_{A,a,\eta,\delta,c}\left(\frac{x}{(\log x)^A}\right).$$

This implies the required asymptotic formula (1.1). The proof of Theorem 1 is completed assuming Proposition 2.1.

3. LINEAR SIEVE AND MEAN VALUE THEOREM

The aim of this section is devoted to present two tools and a preliminary lemma. They will be needed in the proof of Proposition 2.1 above.

3.1. The Rosser-Iwaniec linear sieve. The first one is the Rosser-Iwaniec linear sieve [9, 10]. As usual, denote by $\mu(n)$ the Möbius function.

Lemma 3.1. *Let $D \geq 2$. There are two sequences $\{\lambda_d^\pm\}_{d \geq 1}$, vanishing for $d > D$ or $\mu(d) = 0$, verifying $|\lambda_d^\pm| \leq 1$, such that*

$$(3.1) \quad \sum_{d|n} \lambda_d^- \leq \sum_{d|n} \mu(d) \leq \sum_{d|n} \lambda_d^+ \quad (n \geq 1)$$

and

$$(3.2) \quad \sum_{d|P(z)} \lambda_d^+ \frac{w(d)}{d} \leq \prod_{\substack{p \leq z \\ p \in \mathcal{P}}} \left(1 - \frac{w(p)}{p}\right) \left\{ F(s) + O\left(\frac{e^{\sqrt{L}-s}}{\sqrt[3]{\log D}}\right) \right\}$$

$$(3.3) \quad \sum_{d|P(z)} \lambda_d^- \frac{w(d)}{d} \geq \prod_{\substack{p \leq z \\ p \in \mathcal{P}}} \left(1 - \frac{w(p)}{p}\right) \left\{ f(s) + O\left(\frac{e^{\sqrt{L}-s}}{\sqrt[3]{\log D}}\right) \right\}$$

for any $z \in [2, D]$, $s = (\log D)/\log z$, set of prime numbers \mathcal{P} and multiplicative function w satisfying

$$(3.4) \quad 0 < w(p) < p \quad (p \in \mathcal{P}),$$

$$(3.5) \quad \prod_{u < p \leq v, p \in \mathcal{P}} \left(1 - \frac{w(p)}{p}\right)^{-1} \leq \frac{\log v}{\log u} \left(1 + \frac{L}{\log u}\right) \quad (2 \leq u \leq v),$$

where $P(z) := \prod_{p \leq z, p \in \mathcal{P}} p$ and the implied O -constants are absolute. Here F, f are defined by the continuous solutions to the system

$$\begin{cases} (sF(s))' = f(s-1) & (s > 2) \\ (sf(s))' = F(s-1) & (s > 2) \end{cases}$$

with the initial condition

$$\begin{cases} sF(s) = 2e^\gamma & (1 \leq s \leq 2) \\ sf(s) = 0 & (0 < s \leq 2) \end{cases}$$

where γ is the Euler constant.

3.2. A mean value theorem of Bombieri-Vinogradov type.

In order to control the error term coming from the linear sieve in our case, we need a mean value theorem of Bombieri-Vinogradov type. For this, we consider non-negative arithmetic functions κ , which satisfy the properties (\mathcal{A}) , (\mathcal{B}) and (\mathcal{C}) as introduced by Motohashi [13]:

(\mathcal{A}) There is a positive constant C such that $\kappa(n) \ll \tau(n)^C$, where $\tau(n)$ is the classical divisor function.

(\mathcal{C}) If the conductor of a non-trivial Dirichlet character χ is $O((\log x)^D)$ for some $D > 0$, then

$$\sum_{n \leq x} \kappa(n) \chi(n) \ll x(\log x)^{-3D}.$$

(\mathcal{C}) For any $A > 0$, there exists a constant $B = B(A) > 0$ such that

$$\sum_{d \leq x^{1/2} (\log x)^{-B}} \max_{z \leq x} \max_{(a,d)=1} \left| \sum_{\substack{n \leq z \\ n \equiv a \pmod{d}}} \kappa(n) - \frac{1}{\varphi(d)} \sum_{\substack{q \leq z \\ (d,q)=1}} \kappa(q) \right| \ll \frac{x}{(\log x)^A}$$

for all $x \geq 3$.

In [13, Theorem 1], Motohashi proved the following result: *If f and g have the properties (\mathcal{A}), (\mathcal{B}) and (\mathcal{C}), then so does the multiplicative convolution $f * g$.*

The following proposition will play a key role in the proof of Proposition 2.1 above. Evidently it is of independent interest and should have other applications.

Proposition 3.2. *Let $\kappa_1(m)$ and $\kappa_2(m)$ be the characteristic functions of the odd integers and of even integers, respectively. Then for any $A > 0$, there is a constant $B = B(A) > 0$ such that the inequality*

$$\sum_{\substack{d \leq x^{1/2} (\log x)^{-B} \\ 2 \nmid d}} \max_{z \leq x} \max_{(a,d)=1} \left| \sum_{\substack{mp \leq z \\ mp \equiv a \pmod{d}}} \kappa_i(m) - \frac{1}{\varphi(d)} \sum_{\substack{mp \leq z \\ (d,mp)=1}} \kappa_i(m) \right| \ll_A \frac{x}{(\log x)^A}$$

holds for all $x \geq 3$.

Proof. In view of the Bombieri-Vinogradov theorem (2.1), the characteristic function of the primes has the properties (\mathcal{A}), (\mathcal{B}) and (\mathcal{C}). According to Motohashi's result mentioned above, it is sufficient to verify that κ_1 and κ_2 satisfy (\mathcal{A}), (\mathcal{B}) and (\mathcal{C}).

The property (\mathcal{A}) is obvious for these two functions.

Since $n \mapsto \chi(n)$ is completely multiplicative, we have

$$\sum_{n \leq x} \kappa_2(n) \chi(n) = \chi(2) \sum_{m \leq x/2} \chi(m) \ll (\log x)^D \ll x (\log x)^{-3D}.$$

This shows that κ_2 has the property (\mathcal{B}). Defining $\mathbb{1}(n) := 1$ for $n \geq 1$ and noticing that $\kappa_1 = \mathbb{1} - \kappa_2$, the function κ_1 also has the property (\mathcal{B}).

It remains to prove that κ_i satisfies the property (\mathcal{C}). For $2 \nmid d$, we have

$$\begin{aligned} \sum_{\substack{n \leq z \\ (n,d)=1}} \kappa_2(n) &= \sum_{\substack{m \leq z/2 \\ (m,d)=1}} 1 = \sum_{m \leq z/2} \sum_{d' | (m,d)} \mu(d') \\ &= \sum_{d' | d} \mu(d') \sum_{m \leq z/(2d')} 1 = \frac{\varphi(d)}{2d} z + O(\tau(d)). \end{aligned}$$

Thus

$$\sum_{\substack{n \leq z \\ n \equiv a \pmod{d}}} \kappa_2(n) - \frac{1}{\varphi(d)} \sum_{\substack{n \leq z \\ (n,d)=1}} \kappa_2(n) = \sum_{\substack{m \leq z/2 \\ m \equiv \bar{2}a \pmod{d}}} 1 - \frac{z}{2d} + O\left(\frac{\tau(d)}{\varphi(d)}\right) \ll 1,$$

where $\bar{2}$ is the inverse of 2 modulo d . From this we deduce immediately

$$\sum_{\substack{d \leq x^{1/2} (\log x)^{-B} \\ 2 \nmid d}} \max_{z \leq x} \max_{(a,d)=1} \left| \sum_{\substack{n \leq z \\ n \equiv a \pmod{d}}} \kappa_2(n) - \frac{1}{\varphi(d)} \sum_{\substack{n \leq z \\ (n,d)=1}} \kappa_2(n) \right| \ll \frac{x^{1/2}}{(\log x)^B}.$$

This proves that the function $\kappa_2(n)$ has the property (\mathcal{C}) . A similar argument shows that the function $\mathbb{1}$ has the property (\mathcal{C}) . Since $\kappa_1(n) = \mathbb{1}(n) - \kappa_2(n)$ for all integers $n \geq 1$, the sequence $\{\kappa_1(n)\}_{n \geq 1}$ satisfies the property (\mathcal{C}) . \square

3.3. A preliminary lemma.

Lemma 3.3. *For each positive integer $n \geq 1$, define*

$$(3.6) \quad \psi(n) := \prod_{2 < p|n} \frac{p-1}{p-2}.$$

Then we have

$$\sum_{n \leq x} \psi(n) = \Xi_2^{-1}x + O\left(\frac{x}{\log x}\right)$$

for $x \geq 2$, where

$$(3.7) \quad \Xi_2 := \prod_{p > 2} \left(1 - \frac{1}{(p-1)^2}\right).$$

Proof. Since the function $n \mapsto \psi(n)$ is strongly multiplicative such that

$$\psi(2^\nu) = 1 \quad \text{and} \quad \psi(p^\nu) = \frac{p-1}{p-2} \quad (p \text{ odd prime}),$$

for $\Re s > 1$ we can write

$$\begin{aligned} \sum_{n \geq 1} \frac{\psi(n)}{n^s} &= \prod_p \left(1 + \sum_{\nu \geq 1} \frac{\psi(p^\nu)}{p^{\nu s}}\right) \\ &= \frac{1}{1-2^{-s}} \prod_{p > 2} \left(1 + \frac{p-1}{p-2} \frac{p^{-s}}{1-p^{-s}}\right) \\ &= \zeta(s) \prod_{p > 2} \left(1 + \frac{1}{(p-2)p^s}\right), \end{aligned}$$

where $\zeta(s) := \prod_p (1 - p^{-s})^{-1}$ is the Riemann ζ -function. Using [15, Theorem II.5.3], we obtain the required result. \square

4. PROOF OF PROPOSITION 2.1

As indicated in the introduction, our method is different from [2].

If a prime number q is counted in $\mathcal{Q}_2(r)$, then we can write $q - a = k\ell r$, where ℓ is the largest prime factor of $q - a$. Since $\ell > r \in (\frac{1}{2}x, x]$ and $y < q \leq cy$, we have $k \leq (cy - a)/(\ell r) \leq 2cr^{\eta-2}$. On the other hand, noticing that ℓ, r and $q = k\ell r + a$ are odd, we must have $2 \nmid (a + k)$.

For simplicity of notation, we put

$$c_1 := 1 - \delta, \quad c_2 := c + \delta.$$

By the Chen-Iwaniec switching principle [4, 8], we see that $\mathcal{Q}_2(r)$ does not exceed the number of primes in the sequence

$$(4.1) \quad \{k\ell r + a : k \leq 2cr^{\eta-2}, 2 \nmid (a + k), c_1 y / (kr) < \ell \leq c_2 y / (kr)\}.$$

We shall sieve this sequence by the set of primes $\mathcal{P}_{2r} := \{p \in \mathbb{P} : p \nmid 2r\}$. Define $P_{2r}(z) := \prod_{p < z, p \nmid 2r} p$ with $z := (y/r)^{1/4} (\log(y/r))^{-B(3)} < r$ and denote by $\mu(n)$ the Möbius function. The inversion formula of Möbius allows us to write that

$$\begin{aligned} \mathcal{Q}_2(r) &\leq \sum_{k \leq 2cr^{\eta-2}, 2 \nmid (a+k)} \sum_{\substack{c_1 y/(kr) < \ell \leq c_2 y/(kr) \\ k\ell r + a \text{ is prime}}} 1 \\ &\leq \sum_{k \leq 2cr^{\eta-2}, 2 \nmid (a+k)} \sum_{\substack{c_1 y/(kr) < \ell \leq c_2 y/(kr) \\ (k\ell r + a, P_{2r}(z)) = 1}} 1 \\ &= \sum_{k \leq 2cr^{\eta-2}, 2 \nmid (a+k)} \sum_{c_1 y/(kr) < \ell \leq c_2 y/(kr)} \sum_{d | (k\ell r + a, P_{2r}(z))} \mu(d). \end{aligned}$$

By using Lemma 3.1, it follows that

$$\begin{aligned} \mathcal{Q}_2(r) &\leq \sum_{k \leq 2cr^{\eta-2}, 2 \nmid (a+k)} \sum_{c_1 y/(kr) < \ell \leq c_2 y/(kr)} \sum_{d | (k\ell r + a, P_{2r}(z))} \lambda_d^+ \\ &= \sum_{d | P_{2r}(z)} \lambda_d^+ \sum_{k \leq 2cr^{\eta-2}, 2 \nmid (a+k)} \sum_{\substack{c_1 y/(kr) < \ell \leq c_2 y/(kr) \\ k\ell r \equiv -a \pmod{d}}} 1 \\ &= \sum_{d | P_{2r}(z)} \lambda_d^+ \sum_{k \leq 2cr^{\eta-2}, 2 \nmid (a+k)} \sum_{\substack{c_1 y/(kr) < \ell \leq c_2 y/(kr) \\ k\ell \equiv -a\bar{r} \pmod{d}}} 1, \end{aligned}$$

where \bar{r} is the inverse of r module d , i.e., $r\bar{r} \equiv 1 \pmod{d}$.

Introducing the notation

$$E(t; d, b) := \sum_{\substack{k \leq 2cr^{\eta-2}, 2 \nmid (a+k) \\ k\ell \equiv b \pmod{d}}} \sum_{\ell \leq t/(kr)} 1 - \frac{1}{\varphi(d)} \sum_{k \leq 2cr^{\eta-2}, 2 \nmid (a+k)} \sum_{\substack{\ell \leq t/(kr) \\ (k\ell, d) = 1}} 1,$$

we write

$$\begin{aligned} \sum_{\substack{k \leq 2cr^{\eta-2}, 2 \nmid (a+k) \\ k\ell \equiv -a\bar{r} \pmod{d}}} \sum_{c_1 y/(kr) < \ell \leq c_2 y/(kr)} 1 &= \frac{1}{\varphi(d)} \sum_{k \leq 2cr^{\eta-2}, 2 \nmid (a+k)} \sum_{\substack{c_1 y/(kr) < \ell \leq c_2 y/(kr) \\ (k\ell, d) = 1}} 1 \\ &\quad + E(c_2 y; d, -a\bar{r}) - E(c_1 y; d, -a\bar{r}). \end{aligned}$$

Inserting into the preceding formula, it follows that

$$(4.2) \quad \mathcal{Q}_2(r) \leq \mathcal{M}(r) + \mathcal{E}(r),$$

where

$$\begin{aligned} \mathcal{M}(r) &:= \sum_{d | P_{2r}(z)} \frac{\lambda_d^+}{\varphi(d)} \sum_{k \leq 2cr^{\eta-2}, 2 \nmid (a+k)} \sum_{\substack{c_1 y/(kr) < \ell \leq c_2 y/(kr) \\ (k\ell, d) = 1}} 1, \\ \mathcal{E}(r) &:= \sum_{d | P_{2r}(z)} \lambda_d^+ (E(c_2 y, d, -a\bar{r}) - E(c_1 y, d, -a\bar{r})). \end{aligned}$$

Firstly, by inversion of summations and Lemma 3.1 with

$$w(d) = d/\varphi(d), \quad D := z^2, \quad \mathcal{P} = \{p \in \mathbb{P} : p \nmid 2k\ell r\},$$

it follows that

$$\begin{aligned} \mathcal{M}(r) &= \sum_{\substack{k \leq 2cr^{\eta-2}, 2 \nmid (a+k) \\ c_1y/(kr) < \ell \leq c_2y/(kr)}} \sum_{d|P_{2k\ell r}(z)} \frac{\lambda_d^+}{\varphi(d)} \\ &\leq \left\{ F(2) + O\left(\frac{1}{\sqrt[3]{\log r}}\right) \right\} \sum_{\substack{k \leq 2cr^{\eta-2} \\ 2 \nmid (a+k)}} \sum_{\substack{c_1y/(kr) < \ell \leq c_2y/(kr)}} \prod_{\substack{p \leq z \\ p \nmid 2k\ell r}} \left(1 - \frac{1}{p-1}\right). \end{aligned}$$

On the other hand, the Mertens formula allows us to deduce that

$$\begin{aligned} \prod_{p \leq z, p \nmid 2m} \left(1 - \frac{1}{p-1}\right) &= \prod_{2 < p \leq z} \left(1 - \frac{1}{p-1}\right) \prod_{2 < p|m} \frac{p-1}{p-2} \\ &= \prod_{2 < p \leq z} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{2 < p|m} \frac{p-1}{p-2} \prod_{2 < p \leq z} \left(1 - \frac{1}{p}\right) \\ &= \frac{2\Xi_2\psi(m)e^{-\gamma}}{\log z} \left\{1 + O\left(\frac{1}{\log z}\right)\right\}, \end{aligned}$$

where Ξ_2 and $\psi(m)$ are defined as in (3.7) and (3.6), respectively. Inserting it into the preceding relation and using the fact that $F(2) = e^\gamma$, we find

$$\mathcal{M}(r) \leq \left\{1 + O\left(\frac{1}{\sqrt[3]{\log r}}\right)\right\} \frac{2\Xi_2}{\log z} \sum_{\substack{k \leq 2cr^{\eta-2} \\ 2 \nmid (a+k)}} \sum_{\substack{c_1y/(kr) < \ell \leq c_2y/(kr)}} \psi(k\ell r).$$

Noticing that $\ell > r > \frac{1}{2}x$ and that ℓ and r are primes, we have

$$\psi(k\ell r) \leq \psi(k)\psi(\ell)\psi(r) = \{1 + O(x^{-1})\}\psi(k).$$

Thus

$$\begin{aligned} \mathcal{M}(r) &\leq \left\{1 + O\left(\frac{1}{\sqrt[3]{\log r}}\right)\right\} \frac{2\Xi_2}{\log z} \sum_{\substack{k \leq 2cr^{\eta-2} \\ 2 \nmid (a+k)}} \psi(k) \sum_{c_1y/(kr) < \ell \leq c_2y/(kr)} 1 \\ &= \left\{1 + O\left(\frac{1}{\sqrt[3]{\log r}}\right)\right\} \frac{2\Xi_2}{\log z} \sum_{\substack{k \leq 2cr^{\eta-2} \\ 2 \nmid (a+k)}} \psi(k) \frac{(c_2 - c_1)y}{kr \log(y/kr)} \\ &= \left\{1 + O\left(\frac{1}{\sqrt[3]{\log r}}\right)\right\} \frac{2\Xi_2(c_2 - c_1)y}{r(\log z) \log(y/r)} \mathcal{S}(r), \end{aligned}$$

where

$$\mathcal{S}(r) := \sum_{\substack{k \leq 2cr^{\eta-2} \\ 2 \nmid (a+k)}} \frac{\psi(k)}{k(1 - (\log k)/\log(y/r))}.$$

With the help of Lemma 3.3, a simple partial integration leads to

$$\begin{aligned}
\mathcal{S}(r) &= \left\{1 + O\left(\frac{1}{\log r}\right)\right\} \frac{1}{2} \sum_{k \leq cr^{\eta-2}} \frac{\psi(k)}{k(1 - (\log k)/\log(y/r))} \\
&= \left\{1 + O\left(\frac{1}{\log r}\right)\right\} \frac{1}{2\Xi_2} \int_1^{cr^{\eta-2}} \frac{dt}{t(1 - (\log t)/\log(y/r))} \\
&= \left\{1 + O\left(\frac{1}{\log r}\right)\right\} \frac{\log(y/r)}{2\Xi_2} \int_0^{(\eta-2)/(\eta-1)} \frac{dv}{1-v} \\
&= \left\{1 + O\left(\frac{1}{\log r}\right)\right\} \frac{\log(\eta-1)}{2\Xi_2} \log(y/r),
\end{aligned}$$

where Ξ_2 is defined as in (3.7). Combining it with the preceding formula, it follows that

$$\begin{aligned}
(4.3) \quad \mathcal{M}(r) &\leq \left\{1 + O\left(\frac{1}{\sqrt[3]{\log r}}\right)\right\} \frac{(c_2 - c_1)y \log(\eta-1)}{r \log z} \\
&\leq \left\{1 + O\left(\frac{1}{\sqrt[3]{\log r}}\right)\right\} \frac{4(c-1+2\delta)\eta \log(\eta-1) \pi(y)}{\eta-1 \varphi(r)}.
\end{aligned}$$

With the help of Proposition 3.2, it is easy to see that

$$(4.4) \quad \mathcal{E}(r) \ll \frac{y}{r(\log y)^A}.$$

Inserting (4.3) and (4.4) into (4.2), we obtain the required inequality (2.6).

Acknowledgements. The author is supported in part by NSFC No. 11771121.

REFERENCES

- [1] R. C. Baker & G. Harman, *The Brun-Titchmarsh theorem on average*, Analytic Number Theory, Vol. 1 (Allerton Park, IL, 1995), Progr. Math., 138, Birkhäuser Boston, Boston, MA, 1996, 39–103.
- [2] W. Banks & Igor E. Shparlinski, *On values taken by the largest prime factor of shifted primes*, J. Aust. Math. Soc. **82** (2015), 133–147.
- [3] F.-J. Chen & Y.-G. Chen, *On the largest prime factor of shifted primes*, Acta Math. Sinica, English Series, August 15, 2016.
- [4] J.-R. Chen, *On the representation of a large even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica **16** (1973), 157–176.
- [5] B. Feng & J. Wu, *On the density of shifted primes with large prime factors*, Science China Mathematics, 2017, 60, doi: 10.1007/s11425-016-9065-7.
- [6] É. Fouvry, *Théorème de Brun-Titchmarsh; application au théorème de Fermat*, Invent. Math., **79** (1985), 383–407.
- [7] M. Goldfeld, *On the number of primes p for which $p+a$ has a large prime factor*, Mathe-matika, **16** (1969) 23–27.
- [8] H. Iwaniec, *Primes of the type $\phi(x, y) + A$ where ϕ is a quadratic form*, Acta Arith. **21** (1972), 203–234.
- [9] H. Iwaniec, *Rosser’s sieve*, Acta Arith., **36** (1980), 171–202.
- [10] H. Iwaniec, *A new form of the error term in the linear sieve*, Acta Arith., **37** (1980), 307–320.

- [11] J.-Y. Liu, J. Wu & P. Xi, *Primes in arithmetic progressions with friable indices*, Preprint 2017.
- [12] F. Luca, R. Menares & A. Pizarro-Madariaga, *On shifted primes with large prime factors and their products*, Bull. Belg. Math. Soc. Simon Stevin, **22** (2015), 39–47.
- [13] Y. Motohashi, *An induction principle for the generalization of Bombieri's prime number theorem*, Proc. Japan Acad. **52** (1976), 273–275.
- [14] Rivest R, Silverman R. Are 'Strong' Prime Needed for RSA ? Cryptology ePrint Archive: Report 2001/007, <http://eprint.iacr.org/2001/007>.
- [15] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Translated from the second French edition (1995) by C. B. Thomas, Cambridge Studies in Advanced Mathematics **46**, Cambridge University Press, Cambridge, 1995. xvi+448 pp.
- [16] N. K. Vishnoi, *Theoretical aspects of randomization in computation*, Ph. D. Thesis, Georgia Inst. of Technogy, 2004. (<http://smartech.gatech.edu:8282/dspace/handle/1853/5049>)
- [17] Y. Zhang, *Bounded gaps between primes*, Ann of Math, 2014, 179: 1121–1174.

CNRS UMR 8050, LABORATOIRE D'ANALYSE ET DE MATHÉMATIQUES APPLIQUÉES, UNIVERSITÉ PARIS-EST CRÉTEIL, 61 AVENUE DU GÉNÉRAL DE GAULLE, 94010 CRÉTEIL CEDEX, FRANCE

E-mail address: `jie.wu@u-pec.fr`