On shifted primes with large prime factors and their products

Florian Luca
Mathematical Institute, UNAM
04510 Mexico DF, Mexico
fluca@matmor.unam.mx

Ricardo Menares
Instituto de Matemáticas
Pontificia Universidad Católica de Valparaíso
Blanco Viel 596, Cerro Barón, Valparaíso, Chile
ricardo.menares@ucv.cl

Amalia Pizarro-Madariaga
Departamento de Matemáticas
Universidad de Valparaíso, Chile
amalia.pizarro@uv.cl

November 12, 2013

Abstract
We estimate from below the lower density of the set of prime numbers $p$ such that $p - 1$ has a prime factor of size at least $p^c$, where $1/4 \leq c \leq 1/2$. We also establish upper and lower bounds on the counting function of the set of positive integers $n \leq x$ with exactly $k$ prime factors, counted with or without multiplicity, such that the largest prime factor of $\gcd(p - 1 : p \mid n)$ exceeds $n^{1/2k}$.

Contents

1 Introduction 2
2 Proof of Theorem 1 4
1 Introduction

For an integer \( n \) put \( P(n) \) for the maximum prime factor of \( n \) with the convention that \( P(0) = P(\pm 1) = 1 \). A lot of work has been done understanding the distribution of \( P(p - 1) \) for prime numbers \( p \). The extreme cases \( P(p - 1) = 2 \) and \( P(p - 1) = (p - 1)/2 \) correspond to Fermat primes and Sophie-Germain primes, respectively. Not only do we not know if there are infinitely many primes of these kinds, but we do not know whether for each \( \varepsilon > 0 \) arbitrarily small there exist infinitely many primes \( p \) with \( P(p - 1) < p^\varepsilon \) or \( P(p - 1) > p^{1-\varepsilon} \).

For a set \( \mathcal{C} \) of positive integers and a positive real number \( x \) we put \( \mathcal{C}(x) = \mathcal{C} \cap [1, x] \). Let

\[
P_\varepsilon := \{ \text{prime : } P(p - 1) \geq p^{1-\varepsilon} \}, \quad \kappa(\varepsilon) = \liminf_{x \to \infty} \frac{#P_\varepsilon(x)}{\pi(x)}.
\]

Goldfeld proved in [5] that \( \kappa(1/2) \geq 1/2 \). It is not known whether \( P_{1/2} \) has a relative density, nor what this density could be in case it exists. Fouvry [4], showed that there exists \( \varepsilon_0 \in (0, 1/3) \) such that \( \kappa(\varepsilon_0) > 0 \). Baker and Harman [1], found \( 0 < \varepsilon_1 < \varepsilon_0 \) such that \( P_{\varepsilon_1} \) is infinite.

In this article, we generalize Goldfeld’s result in two different directions. First, we estimate from below the lower density of \( P_\varepsilon \) for all \( \varepsilon \in [1/2, 3/4] \). Secondly, we estimate the counting function of the set of square free positive integers having prime divisors that, when shifted, share a large common prime factor. Both questions are motivated by a technique used in [3] to bound from below the degree of the field of coefficients of newforms in terms of the level. A feature of the method in loc. cit. is that what is needed are values of \( \varepsilon \) such that \( \kappa(\varepsilon) \) is as large as possible. Since \( \kappa(\varepsilon) \) is clearly an increasing function of \( \varepsilon \), in contrast with the aforementioned works, which are focused in dealing with smaller and smaller values of \( \varepsilon \), here we concentrate on the case where this parameter is bigger than 1/2.

We obtain the following results.

**Theorem 1.** Let \( 0 \leq \alpha \leq 1/4 \). Let

\[
N_\alpha = \{ \text{prime such that } P(p - 1) \geq p^{1/2-\alpha} \}.
\]
Then

\[ \#N_\alpha(x) \geq \left( \frac{1}{2} + \alpha \right) \frac{x}{\log x} + E(x); \quad E(x) = \begin{cases} O\left( \frac{x \log \log x}{(\log x)^2} \right) & (\alpha < 1/4) \\ O\left( \frac{x}{(\log x)^{5/3}} \right) & (\alpha = 1/4). \end{cases} \]

The implied constant depends on \( \alpha \). In particular,

\[ \kappa(1/2 + \alpha) \geq 1/2 + \alpha \quad \text{for all} \quad \alpha \in [0, 1/4]. \]

The case \( \alpha = 0 \) is Goldfeld’s result mentioned above. Our proof of Theorem 1 follows closely his method.

For any \( k \geq 1 \) and \( a \in (0, 1/k) \), let

\[ A_{k,a} = \{ n = p_1 \cdots p_k, P(\gcd(p_1 - 1, \ldots, p_k - 1)) > n^a \}. \]

By Goldfeld’s result, \( \#A_{1,1/2}(x) \asymp x/\log x \). Here, we prove the following result.

**Theorem 2.** If \( k \geq 2 \) and \( a \in \left[ 1/(2k), 17/(32k) \right) \) are fixed, then

\[ \frac{x^{1-a(k-1)}}{(\log x)^{k+1}} \ll \#A_{k,a}(x) \ll \frac{x^{1-a(k-1)}(\log \log x)^{k-1}}{(\log x)^2}. \] (1)

The case \( a = 1/(2k) \) is important for the results from \( \mathbb{3} \). We have the estimate

\[ \#A_{k,1/(2k)}(x) = x^{1/2+1/2k+o(1)}, \quad x \to \infty. \] (2)

Goldfeld’s method does not seem to extend to the situation in Theorem 2 (see the last section). Instead, we follow a more direct method. For the lower bound, we rely on a refined version of the Brun-Titchmarsh inequality due to Banks and Shparlinsky \( \mathbb{2} \).

We remark that both theorems presented here remain valid if, instead of considering large factors of \( p - 1 \), we look at large factors \( p + n \) for an arbitrary nonzero fixed integer \( n \).

We leave as a problem for the reader to determine the exact order of magnitude of \( \#A_{k,a}(x) \), or an asymptotic for it.

Throughout this paper, we use \( p, q, r \) with or without subscripts for primes. We use the Landau symbols \( O, o \) and the Vinogradov symbols \( \ll \) and \( \gg \) with their regular meaning. The constants implied by them might depend on some other parameters such as \( \alpha, k, \varepsilon \) which we will not indicate.
2 Proof of Theorem 1

We follow Goldfeld’s general strategy. Put \( c = \frac{1}{2} - \alpha \). So, \( 1/4 \leq c \leq 1/2 \).

Let

\[
N_c'(x) = \#\{p \leq x : p \text{ is prime and } P(p - 1) \geq x^c\}.
\]

Since \( \#N_\alpha(x) \geq N_c'(x) \), it is enough to give a lower bound for \( N_c'(x) \). Put

\[
M_c(x) = \sum_{p \leq x} \sum_{\ell \geq x^c} \log \ell,
\]

where \( p \) and \( \ell \) denote primes. Since

\[
\sum_{\ell \geq x^c} \log \ell \begin{cases} = 0, & \text{if } P(p - 1) < x^c; \\ \leq \log x, & \text{otherwise} \end{cases}
\]

we have that

\[
M_c(x) \leq \log x \sum_{p \leq x} \frac{1}{P(p - 1) \geq x^c} = N_c'(x) \log x.
\]

Hence, \( N_c'(x) \geq M_c(x) / \log x \). Then, in order to prove Theorem 1 it is enough to show that

\[
M_c(x) = (1 - c)x + F(x), \quad F(x) = \begin{cases} O_c \left( \frac{x \log \log x}{\log x} \right), & (c > 1/4); \\ O \left( \frac{x}{(\log x)^{2/3}} \right), & (c = 1/4). \end{cases} \tag{3}
\]

We denote by \( \Lambda(\cdot) \) the von Mangoldt’s function. As usual, \( \pi(x; b, a) \) is the number of primes \( q \leq x \) in the arithmetic progression \( q \equiv a \pmod{b} \).

We define

\[
L(x; u, v) = \sum_{u < m \leq v} \Lambda(m)\pi(x; m, 1).
\]

**Lemma 1.** Assume \( 1/4 \leq c \leq 1/2 \). Then

\[
L(x; x^c, x) = M_c(x) + O \left( \frac{x^{7/6 - 2c/3}}{(\log x)^r} \right),
\]

where \( r = 0 \) when \( c > 1/4 \) and \( r = 2/3 \) when \( c = 1/4 \).
Proof. Let $0 < d < 1 - c$ be a real number and $r \in (0, 1)$. We assume that $x$ is large enough so that the inequality $x^{1-d}(\log x)^r < x$ holds. We put

$$M_1^d(x) = \sum_{x^c < \ell^k \leq x^{1-d}(\log x)^r} \pi(x; \ell^k, 1) \log \ell,$$
$$M_2^d(x) = \sum_{x^{1-d}(\log x)^r \leq \ell^k \leq x} \pi(x; \ell^k, 1) \log \ell.$$

Hence,

$$L(x; x^c, x) - M_c(x) = M_1^d(x) + M_2^d(x).$$

(4)

Using the Brun-Titchmarsh inequality, we have that

$$M_1^d(x) \ll \frac{x}{\log x} \sum_{x^c < \ell^k \leq x^{1-d}(\log x)^r} \frac{\log \ell}{\ell^{k-1}(\ell - 1)}.$$

$$\leq \frac{x}{\log x} \sum_{\ell \leq x^{(1-d)/2}(\log x)^{r/2}} \frac{2 \log \ell}{\ell} \sum_{k \geq c \log x / \log \ell} \frac{1}{\ell^k}.$$

$$\leq \frac{x}{\log x} \sum_{\ell \leq x^{(1-d)/2}(\log x)^{r/2}} \frac{4 \log x}{x^c}.$$

$$= 4x^{1-c} \pi \left( x^{(1-d)/2}(\log x)^{r/2} \right).$$

$$\ll \frac{x^{1-c+(1-d)/2}}{(\log x)^{1-r/2}}.$$

On the other hand, for an integer $m > x^{1-d}(\log x)^{\alpha}$, we have that

$$\pi(x; m, 1) \leq \sum_{n \leq x \mod m} 1 \leq \frac{x}{m} < \frac{x^d}{(\log x)^{\alpha}}.$$

Hence,

$$M_2^d(x) \ll \frac{x^d}{(\log x)^{\alpha}} \sum_{x^{1-d}(\log x)^{\alpha} \leq \ell^k \leq x} \log \ell.$$

$$\ll \frac{x^d}{(\log x)^{\alpha}} (\log x) \pi(\sqrt{x}) \ll \frac{x^d}{(\log x)^{\alpha}}.$$
Using (4), we obtain
\[ L_c(x) - M_c(x) = O \left( \frac{x^{1-c+(1-d)/2}}{(\log x)^{1-r/2}} + \frac{x^{d+\frac{1}{2}}}{(\log x)^r} \right). \]

We take \( d = 2/3(1 - c) \) and then both exponents of \( x \) above are equal and evaluate to \( 7/6 - 2/3c \). Taking \( r = 0 \) when \( c < 1/4 \) and \( r = 2/3 \) when \( c = 1/4 \), we obtain the desired estimate.

Lemma 2. Assume that \( c \in (0, 1/2] \). Then, for \( B > 0 \), we have
\[ L \left( x; x^c/(\log x)^B, x^c \right) = O \left( \frac{x \log \log x}{\log x} \right), \quad (x \to \infty). \]

Proof. This follows immediately from the Brun-Titchmarsh inequality (see, for example, equation (3) in \[5\]).

Lemma 3. Assume that \( c \in (0, 1/2] \). Then, there exists \( B > 0 \) such that
\[ L \left( x; x^c/(\log x)^B \right) = cx + O \left( \frac{x \log \log x}{\log x} \right), \quad (x \to \infty). \]

Proof. This follows easily from the Bombieri-Vinogradov theorem (see, for example, equation (2) in \[5\]).

Proof of Theorem 1: We have (see p. 23 in \[5\]),\n\[ L(x; 1, x) = x + O \left( \frac{x}{\log x} \right), \quad (x \to \infty). \]
(5)

Take \( B > 0 \) as in Lemma 3. Since
\[ L(x; 1, x) = L \left( 1, \frac{x^c}{(\log x)^B} \right) + L \left( x, \frac{x^c}{(\log x)^B}, x^c \right) + L(x; x^c, x), \]
the result follows by combining (3) and Lemmas 1, 2 and 3.

3 Proof of Theorem 2

3.1 The upper bound

Let \( x \) be large. It is sufficient to prove the upper bound indicated at (1) for the number of integers \( n \in A_{k,a} \cap [x/2, x] \), since then the upper bound
will follow by changing $x$ to $x/2$, then to $x/4$ and so on, and summing up the resulting estimates. So, we assume that $n \geq x/2$ is in $A_{k,a}(x)$. Then $n = p_1 \cdots p_k \leq x$, where $p_1 \leq p_2 \leq \cdots \leq p_k$, and $p_i = p\lambda_i + 1$ for $i = 1, \ldots, k$, where

$$p > n^a > (x/2)^a.$$ 

Note that

$$p^k \lambda_1 \cdots \lambda_k \leq \phi(n) < n < x.$$ 

Thus, $p < x^{1/k}$. Let $B_1(x)$ be the set of such $n \leq x$ such that $\lambda_k \leq x^\delta$, where $\delta = \delta_k = 15(k - 1)/(32k^2)$. Since $\lambda_1 \leq \cdots \leq \lambda_k$, we get that $\lambda_i \leq x^\delta$ for all $i = 1, \ldots, k$. This shows that

$$\#B_1(x) \leq \pi(x^{1/k})(x^\delta)^k < x^{1/k + 15(k - 1)/(32k)} = o(x^{1-a(k-1)}) \quad (x \to \infty), \tag{6}$$

where we used the fact that $1/k + 15(k - 1)/(32k) < 1 - a(k - 1)$, which holds for all $k \geq 2$ and $a \in (0, 17/(32k))$.

From now on, we assume that $n \in B_2(x) = (A_k \cap [x/2, x]) \setminus B_1(x)$. Fix the primes $p_1 \leq \cdots \leq p_{k-1}$. Then $p$ is fixed, $p_k \leq x/(p_1 \cdots p_{k-1})$ and $p_k \equiv 1 \pmod p$. The number of such primes is, by the Brun-Titchmarsh theorem (see [6]), at most

$$\pi(x/(p_1 \cdots p_{k-1}); p, 1) \leq \frac{2x}{(p - 1)p_1 \cdots p_{k-1} \log(x/(p_1 \cdots p_{k-1}))}.$$ 

Since $x/(p_1 \cdots p_{k-1}) > \lambda_k > x^\delta$, we get that the last bound is at most

$$\ll \frac{x}{(\log x)p_1 \cdots p_{k-1}}.$$ 

Keeping $p$ fixed and summing up the above bound over all ordered $k - 1$-tuples of primes $(x/2)^a < p_1 \leq \cdots \leq p_{k-1} \leq x$ such that $p_i \equiv 1 \pmod p$ for $i = 1, \ldots, k - 1$, we get a bound of

$$\frac{x}{(\log x)p} \sum_{q \equiv 1 \pmod p, q \leq x} \frac{1}{q} \ll \frac{x(\log \log x)^{k-1}}{(\log x)p^k}, \tag{7}$$

where we used the fact that

$$\sum_{q \equiv 1 \pmod p, q \leq x} \frac{1}{q} \ll \frac{\log \log x}{p}.$$ 

7
uniformly in \((x/2)^a \leq p \leq x^{1/k}\), which follows from the Brun-Titchmarsh theorem by partial summation. Summing up the above bound (7) over all \(p > (x/2)^a\) gives

\[
\# B_2(x) \ll \frac{x (\log \log x)^{k-1}}{\log x} \sum_{(x/2)^a < p \leq x^{1/k}} \frac{1}{p^k}
\]

\[
\ll \frac{x (\log \log x)^{k-1}}{\log x} \int_{(x/2)^a}^{x^{1/k}} \frac{d\pi(t)}{t^k}
\]

\[
\ll \frac{x (\log \log x)^{k-1}}{\log x} \left( \frac{1}{t^{k-1} \log t} \bigg|_{t=(x/2)^a}^{t=x^{1/k}} + \int_{(x/2)^a}^{x^{1/k}} \frac{dt}{t^k \log t} \right)
\]

\[
\ll \frac{x (\log \log x)^{k-1}}{\log x} \left( \frac{1}{x^{a(k-1)} \log x} \right)
\]

\[
\ll \frac{x^{1-a(k-1)} (\log \log x)^{k-1}}{(\log x)^2}. \tag{8}
\]

The upper bound follows from (6) and (8).

3.2 The lower bound

The following result is Lemma 2.1 in [2].

**Lemma 4.** There exist functions \(C_2(\nu) > C_1(\nu) > 0\) defined for all real numbers \(\nu \in (0, 17/32)\) such that for every integer \(u \neq 0\) and positive real number \(K\), the inequalities

\[
\frac{C_1(\nu) y}{p \log y} < \pi(y; p, u) < \frac{C_2(\nu) y}{p \log y}
\]

hold for all primes \(p \leq y^\nu\) with \(O(y^\nu/(\log y)^K)\) exceptions, where the implied constant depends on \(u, \nu, K\). Moreover, for any fixed \(\epsilon > 0\), these functions can be chosen to satisfy the following properties:

- \(C_1(\nu)\) is monotonic decreasing, and \(C_2(\nu)\) is monotonic increasing;
- \(C_1(1/2) = 1 - \epsilon\) and \(C_2(1/2) = 1 + \epsilon\).

So, we take \(y = x^{1/k}\) and consider primes \(p \in I = [y^{ak}, 2y^{ak}]\). Then \(2y^{ak} = y^\nu\), where \(\nu = ak + (\log 2)/(ak \log y) < 17/32\) for all \(x\) sufficiently large. So, let \(\epsilon > 0\) be such that \(a < 17/32 - \epsilon\) and assume that \(x\) is
sufficiently large such that \( \log 2/(\log y) < \varepsilon/2 \). Then, by Lemma 4 with \( u = 1 \) and \( K = 2 \), the set \( \mathcal{P} \) of primes \( p \leq 2y \) such that
\[
\pi(y; p, 1) > \frac{C_1(17/32 - \varepsilon/2)y}{p \log y}
\]
contains all primes \( p \leq 2y^a \) with \( O(y^a/(\log y)^2) \) exceptions. Thus, the number of primes \( p \in \mathcal{P} \cap I \) satisfies
\[
\# (\mathcal{P} \cap I) \geq \pi(2y^a) - \pi(y^a) - O\left(\frac{y^a}{(\log y)^2}\right) > \frac{y^a}{\log y}
\]
for all \( x \) sufficiently large independently in \( k \) and \( a \). Consider numbers of the form \( n = p_1 \cdots p_k \), where \( p_1 < \cdots < p_k \leq y \) are all primes congruent to 1 modulo \( p \). Furthermore, it is clear that \( p = P(p_i - 1) \) for \( i = 1, \ldots, k \). Note that \( n \leq x \). The number of such \( n \) is, for \( p \) fixed,
\[
\left( \frac{\pi(y; p, 1)}{k} \right) \gg \left( \frac{y}{p \log y} \right)^k \gg \frac{x}{p^k (\log x)^k}.
\]
Summing up the above bound over \( p \in \mathcal{P} \cap I \), we get that
\[
\# A_{k,a}(x) \gg \frac{x}{(\log x)^k} \sum_{p \in \mathcal{P} \cap I} \frac{1}{p^k} \gg x \left( \frac{\# (\mathcal{P} \cap I)}{y^{ak^2}} \right) \gg \frac{xy^a}{y^{ak^2} (\log x)^k \log y} \gg \frac{x^{1-a(k-1)}}{(\log x)^{k+1}},
\]
which is what we wanted.

4 Comments and Remarks

It is not likely that Goldfeld’s method extends to the situation considered in Theorem 2. As we have seen, the proof of Theorem 1 is based on the identity (5). Then, Mertens’s theorem, the Brun-Titchmarsh inequality and the Bombieri-Vinogradov theorem are used to extract the desired estimate out of it. If we try to follow the same strategy to prove Theorem 2, for example with \( a = 1/(2k) \), we are then led to replace the left hand side of (5) by
\[
L_k(x) := \sum_{m \leq x^{1/k}} \Lambda(m) \pi_k(x; m, 1),
\]
where $\pi_k(x; m, 1) = \# \{ n \in A_k(x) : p | n \Rightarrow p \equiv 1 \mod m \}$. Let $\pi_k(x)$ denote the number of squarefree integers up to $x$ having exactly $k$ prime factors. Then, letting $p_1, p_2, \ldots, p_k$ denote primes,

$$L_k(x) = \sum_{p_1 < p_2 < \cdots < p_k} \sum_{m \mid \gcd(p_i - 1) \text{ for } 1 \leq i \leq k} \Lambda(m) \sum_{p_1 < p_2 < \cdots < p_k \leq x} \log (\gcd \ (p_i - 1 : 1 \leq i \leq k)) \geq (\log 2) \pi_k(x) \gg_k \frac{x \log \log x}{\log x}, \quad x \to \infty.$$

In view of (2), we see that $L_k(x)$ grows much faster, when $k \geq 2$, than the counting function we are interested in. Hence, it is unlikely that $L_k(x)$ can be used to obtain information on the growth of $A_k(x)$.

**Acknowledgement.** We thank N. Billerey for stimulating questions. Part of this work was done during a visit of F. L. at the Mathematics Department of the Universidad de Valparaiso during 2013 with a MEC project from CONICYT. He thanks the people of this Department for their hospitality. F. L. was also partially supported by a Marcos Moshinsky Fellowship and Projects PAPIIT IN104512, CONACyT 163787 and CONACyT 193539. R.M. is partially supported by FONDECYT grant 11110225.

**References**

[1] R. C. Baker and G. Harman, “The Brun-Titchmarsh theorem on average,” In Analytic number theory, Vol. 1 (Allerton Park, IL, 1995), 138 of Progr. Math., 39–103. Birkhäuser Boston, Boston, MA, 1996.

[2] W. D. Banks and I. E. Shparlinski, “On values taken on by the largest prime factor of shifted primes”, J. Australian Math. Soc. 82 (2007), 133–147.

[3] N. Billerey and R. Menares, “On the modularity of reducible mod $l$ Galois representations”, Preprint, arXiv:1309.3717v2.

[4] Étienne Fouvry, “Théorème de Brun-Titchmarsh: application au théorème de Fermat,” Invent. Math. 79, (1985), 383–407.

[5] M. Goldfeld, “On the number of primes $p$ for which $p + a$ has a large prime factor”, Mathematika 16 (1969), 23–27.
[6] H. L. Montgomery and R. C. Vaughan, “The large sieve”, *Mathematika* 20 (1973), 119–134.