ACTA ARITHMETICA
176.4 (2016)

# On exponents of modular subgroups generated by small consecutive integers

by

Jacek Pomykała (Warszawa)

**1. Introduction.** Let $n$ be a positive squarefree integer, coprime to 6, and let $B \geq 2$. Letting $G_B = G_B(n)$ be the subgroup of $\mathbb{Z}_n^*$ generated by all positive integers coprime to $n$ included in the interval $[1, B]$, we denote by $G = G(n)$ the least $B$ such that $G_B(n) = \mathbb{Z}_n^*$. The evaluation of $G(n)$ has attracted much attention in the literature (see e.g. [B-H], [Bur]). Conditionally, under the Riemann Hypothesis for Dirichlet $L$-functions we have $G_B(n) = \mathbb{Z}_n^*$ for $B \geq 2\log^2 n$ (see [B-H]).

In this paper we focus on the exponents $E_B(n)$ of the subgroups $G_B(n)$ as $n \to \infty$. More precisely we investigate the distances defined by $D_B(n) = \lambda(n)/E_B(n)$, where $\lambda$ is the Carmichael function. If $G_B(n) = \mathbb{Z}_n^*$ then obviously the (global) distance $D_B(n)$ is trivial, i.e. equal to 1. The best known value of $B = B(n)$ such that $D_B(n)$ is trivial is of order $n^{1/4e^{1/2}+\varepsilon}$ (see [Bur]).

The numbers $n \leq x$ with all local distances $D_B(p)$ $(p \mid n)$ nontrivial and large $B$ should be regarded as exceptional. In the first part of the article we will be concerned with an upper bound for the size of the set of $B$-exceptional numbers $n \leq x$ (i.e. such that all local distances are $\geq 2$). For relatively small $B = B(x)$ the corresponding bound can be obtained by an application of the Montgomery–Vaughan [M-V] large sieve inequality. Namely from the proof of [L-W, Theorem 2] one can easily deduce that the number of primes $n \equiv 1 \pmod 4$ with $n \leq x$ such that $D_B(n)$ is even (and thus nontrivial) is at most $\ll x^{1-c/\log\log x}$ provided $B = B(x)$ is at least $C\log x$, for some absolute constants $c$ and $C > 0$.

2010 *Mathematics Subject Classification*: Primary 11N, 11M; Secondary 14G50.
*Key words and phrases*: Dirichlet characters, Dirichlet $L$-functions, least character nonresidues, zero density estimates, modular groups, large exponent modular subgroups, large sieve estimates, smooth numbers, deterministic reductions in cryptography.
Received 10 August 2015; revised 5 August 2016.
Published online 1 December 2016.

DOI: 10.4064/aa8255-8-2016

In this paper we will be concerned with an upper bound for the set of $B$-exceptional numbers $n \in \mathbb{N}_s$ (see Notation) for significantly greater values of $B = B(x)$. For this reason we use the zero density estimate for the Dirichlet $L$-functions and the device applied in [Pom] to obtain an upper bound for the size of the corresponding set of type $x^{5\delta_0} \log^{c_1} x$, where $\delta_0 = \log\log x^{c_0}/\log B$ for some $c_0 > 0$ and any $c_1 > 14$. Furthermore applying the asymptotic equality for the smooth numbers counting function $\psi_n(x, B)$ proved in [F-T] and the Gallagher large sieve (see [Gal]), we improve the above bound to $x^{2\delta_0(1+o(1))}$ in the region $B(x) > \exp((\log\log x)^{5/3+\varepsilon})$ as $x \to \infty$.

It is known that the quantities $E_B(m)$ and $D_B(m)$, where $m \mid n$, are important in deterministic primality testing (see [F-K]), the conditional factoring problem (see [Con]), the least Euler–Euclid witnesses problem (see [Zra]), or the hardness of the discrete logarithm problem in $\mathbb{Z}_m^*$ (see [P-Z]). The maximal possible value of $D_B(n)$ (equal to $\operatorname{lcm}_{p \mid n} D_B(p)$) defines the $B$-special numbers. They play a significant role in the reduction of factoring $n$ to the computation of the Euler function $\phi(n)$. If many (characterized by the parameter $\beta$) of the values of $D_B(p)$ for $p \mid n$ have nontrivial common divisors, we call $n$ $(B, \beta)^*$-*special*.

In this article we will prove a fairly strong average upper bound for $D_B(n)$ over the set of $(B, \beta)^*$-special numbers. This seems to be useful for a precise characterization of numbers that are hard to factor from the algorithmic point of view. On the other hand, we give an average upper bound for the value $w_B(n) = \prod_{p \mid n}(D_B(p) - 1)$ over the set of $B$-exceptional numbers.

The efficient reduction of factoring $n$ to computing $\phi(n)$ depends essentially on the set of $B$-exceptional numbers $n$ with at least $l$ prime divisors and at least $t$ distinct prime factors of $D_B(p)$ for all $p \mid n$, where $l, t \geq 1$. We prove that the cardinality of the set of such numbers $\leq x$ for sufficiently large $t$ is at most $x^{5\delta_0 - (\gamma(l,t) + l\log(1-t^{-t})/\log x)} \log^{c_1} x$, where $\gamma(l,t) = lt\log t/\log x$, $c_0$ and $c_1$ are as above and $B \geq (c_0 \log x)^c$ with $c = \max(5, 5/(2(c_1 - 14))$, with the corresponding improvement for $B(x) > \exp((\log\log x)^{5/3+\varepsilon})$.

There are two basic ingredients in our approach. One is the combinatorial Lemma 4.4 giving an upper bound for the least common multiple of an arbitrary set of positive integers $d_j$ having many nontrivial values $\nu_q(d_j)$ for primes $q \mid \prod_{j \leq r} d_j$. The second is a generalization of the method applied in [Pom] for nonprime moduli $n \leq x$ and the values of the local distances $D_B(p)$ divisible by arbitrary $d$, which may now depend on $n$. The key point here is to investigate the primitive Dirichlet characters $\chi$ of order dividing $D = \operatorname{lcm} D_B(p)$, so that $\chi([1, B]) \subset \{0, 1\}$. Applying density estimates for the zeros of the corresponding Dirichlet $L$-functions we obtain a suitable average upper bound for $w_B(n)$, and hence for the size of the set of $B$-exceptional numbers $n \leq x$ with large value of $lt\log t$. Finally, letting $l$ and $t$ be of order

$T(x,u) \le (\log x)^{1/u}(\log\log x)^{u-1}$, $(3 \le u < \varepsilon \log\log x/\log\log\log x)$ we deduce that either $n \le x$ can be factored in subexponential time $\exp(T(x,u))$, or $n$ belongs to a set of cardinality $\ll x^{2\delta-\delta^{u-2}(1-2\varepsilon)/u}\log x \log\log x$, for any sufficiently small $\varepsilon > 0$ and sufficiently large $x > x_0(\varepsilon)$, where $\delta = \log(2\log x)/(2\log x)^{1/u}$. The result is interesting when $u > 3$ since then we do not know any deterministic reduction of factoring $n$ to computation of $\phi(n)$ of complexity $\ll \exp((\log x)^{1/u}(\log\log x)^{u-1})$ (see [Zra]).

**Notation.** Throughout, $m, n$ stand for positive integers, while $p, q$ are prime numbers.

- $\mathbb{N}$ := the set of all positive integers
- $\mathbb{N}_s$ := the set of all squarefree positive integers, coprime to 6
- $\phi$ := the Euler phi function
- $\lambda$ := the Carmichael function, i.e. $\lambda(n) = \mathrm{lcm}_{p\,|\,n}(p-1)$ if $n \in \mathbb{N}_s$
- $P_+(n)$ := the greatest prime divisor of $n$
- $\omega(n)$ := the number of distinct prime divisors of $n$
- $\nu_q(n)$ := the highest power of $q$ dividing $n$
- $k(n)$ := the kernel of $n$, i.e. the largest squarefree divisor of $n$
- $\#A$ := the cardinality of the (finite) set $A$
- $\delta(x,y) := \dfrac{\log\log x}{\log y}$ $(y > 1,\ x \ge 3)$
- $\mathrm{ord}_n\, b$ := the order of $b$ mod $n$, where $\gcd(b,n) = 1$
- For $B > 1$,
$$E_B(n) := \operatorname*{lcm}_{b\le B,\,\gcd(b,n)=1} \mathrm{ord}_n\, b, \qquad D_B(n) := \frac{\lambda(n)}{E_B(n)},$$
$$w_B(n) := \prod_{p\,|\,n}(D_B(p)-1).$$
- $\log n$ := the natural logarithm of $n$
- For any Dirichlet character $\chi = \chi \pmod n$ we denote by $L(s,\chi)$ the $L$-series $\sum_{n\ge1}\chi(n)n^{-s}$ analytically continued onto the whole complex plane $\mathbb{C}$
- $N(\sigma,t,\chi)$ := the number of zeros $\rho$ of $L(s,\chi)$ in the region $\operatorname{Re}\rho \ge \sigma$, $|\operatorname{Im}\rho| \le t$

**2. $B$-distance and $B$-exceptionality.** Let $B \ge 2$ and $\lambda = \lambda(n)$ be the Carmichael function. For $n \in \mathbb{N}_s$ we define the *$B$-distance* of $n$ by

$$D_B(n) = \frac{\lambda(n)}{E_B(n)}. \tag{2.1}$$

Here $E_B(n)$ is the exponent of the subgroup of $\mathbb{Z}_n^*$ generated by the positive integers coprime to $n$ from the interval $[1,B]$. The *local $B$-distance* of $n$

(related to any prime $p\,|\,n$) is defined by the equality

$$D_B(p) = \frac{p-1}{E_B(p)}. \tag{2.2}$$

In this paper we investigate the positive integers having a nontrivial (global or local) $B$-distance. If $n$ has a nontrivial (global) $B$-distance, i.e. $q\,|\,D_B(n)$, then $E_B(n)\,|\,\frac{\lambda(n)}{q}$ for some prime $q\,|\,\lambda(n)$. Let $p\,|\,n$ be such that $\nu_q(\lambda(n)) = \nu_q(p-1)$. Then

$$\nu_q(E_B(p)) \le \nu_q(E_B(n)) < v_q(\lambda(n)) = \nu_q(p-1).$$

This proves that $D_B(p) \ge q$, hence $n$ also has some nontrivial local $B$-distance. The converse is not true. To see this, choose distinct primes $p_1$, $p_2$ such that 2 is not a primitive root mod $p_1$ but 2 is a primitive root mod $p_2$ and $p_1 - 1\,|\,p_2 - 1$. Then $E_2(p_1) < p_1 - 1 < \lambda(p_1p_2)$ but $E_2(p_1p_2) = \mathrm{lcm}(E_2(p_1), E_2(p_2)) = \mathrm{lcm}(E_2(p_1), p_2 - 1) = p_2 - 1 = \mathrm{lcm}(p_1 - 1, p_2 - 1) = \lambda(p_1p_2)$. Hence the local distance $D_2(p_1)$ is nontrivial, while $D_2(p_1p_2) = 1$, which is the case in particular when $p_1 = 7$ and $p_2 = 13$. The investigation of $n \le x$ with $D_B(n) > 1$ can therefore be reduced to the investigation of primes $p \le x$ with $D_B(p)$ nontrivial. The numbers $n \in \mathbb{N}_s$ with many large local distances are in some sense exceptional. This leads to the following

Definition 2.1. $n \in \mathbb{N}_s$ is called *$B$-exceptional* if $D_B(p) \ge 2$ for all $p\,|\,n$. Moreover a $B$-exceptional number $n$ is called *$(B, l, T)$-exceptional* ($T \ge 2$, $l \ge 1$) if

$$\#\{p\,|\,n : D_B(p) \ge T\} \ge l. \tag{2.3}$$

For a $B$-exceptional number $n$ we define the nonzero number $w_B(n) = \prod_{p\,|\,n}(D_B(p) - 1)$. To collect the basic facts on $D_B(n)$, $D_B(p)$ and $w_B(n)$, we refer to the familiar lower bound for the smooth numbers counting function.

Lemma 2.2 (see [K-P]). *Let $x \ge 4$ and $2 \le y \le x$. Then*

$$\psi(x, y) := \#\{m \le x : P^+(m) \le y\} > x^{1-\delta(x,y)} \tag{2.4}$$

*where $\delta(x, y) = \log\log x/\log y$.*

Proposition 2.3. *Let $n \in \mathbb{N}_s$, $n \ge 4$, $B \ge 2$, $T \ge 2$, and $l \ge 1$. Then*

$$\mathrm{gcd}_{p\,|\,n}(D_B(p))\,|\,D_B(n)\,|\,\operatorname*{lcm}_{p\,|\,n} D_B(p), \tag{2.5}$$

$$D_B(n) < n^{\delta(n,B)}. \tag{2.6}$$

*Let $n$ be $(B, l, T)$-exceptional and define $\alpha(l, T, n) := l\log T/\log n$. Then*

$$\alpha(l, T, n) < \delta(n, B) \quad \text{and} \quad w_B(n) \ge n^{\alpha(l,T-1,n)}. \tag{2.7}$$

*Furthermore if* $E_B(n) = E_B(p)$ *for every prime* $p \,|\, n$ *then* $D_B(n) = \operatorname{lcm}_{p\,|\,n} D_B(p)$ *and for any* $a > \log 2$ *there exists a constant* $c = c(a)$ *such that if* $\omega(n) > c(a)$ *then*

$$D_B(n) > \omega(n)^{(\log\log \omega(n))/a}.$$

*Proof.* To prove (2.5) consider any prime $q \,|\, \lambda(n)$ and a prime $p_0 = p_0(q) \,|\, n$ such that

$$\nu_q(p_0 - 1) = \nu_q(\lambda(n)).$$

Then

$$\begin{aligned}\nu_q\biggl(\operatorname*{lcm}_{p\,|\,n} \frac{p-1}{E_B(p)}\biggr) &\geq \nu_q\biggl(\frac{p_0-1}{E_B(p_0)}\biggr) = \nu_q\biggl(\frac{\lambda(n)}{E_B(p_0)}\biggr)\\ &\geq \nu_q\biggl(\frac{\lambda(n)}{\operatorname{lcm}_{p\,|\,n} E_B(p)}\biggr) = \nu_q\biggl(\frac{\lambda(n)}{E_B(n)}\biggr).\end{aligned}$$

Similarly letting $p_1 = p_1(q) \,|\, n$ satisfy $\nu_q(E_B(p_1)) = \nu_q(E_B(n))$ we conclude that

$$\nu_q\biggl(\frac{\lambda(n)}{E_B(n)}\biggr) = \nu_q\biggl(\frac{\lambda(n)}{E_B(p_1)}\biggr) \geq \nu_q\biggl(\frac{p_1-1}{E_B(p_1)}\biggr) \geq \min_{p\,|\,n} \nu_q\biggl(\frac{p-1}{E_B(p)}\biggr)$$

giving the remaining divisibility of (2.5). Moreover by Lemma 2.2,

$$\begin{aligned}D_B(n) \,|\, \operatorname*{lcm}_{p\,|\,n} D_B(p) &\leq \prod_{p\,|\,n} D_B(p) = \prod_{p\,|\,n} \frac{p-1}{E_B(p)}\\ &< \prod_{p\,|\,n} p^{\delta(p,B)} \leq \prod_{p\,|\,n} p^{\delta(n,B)} = n^{\delta(n,B)}\end{aligned}$$

as required.

Moreover if $E_B(n) = E_B(p)$ for every prime $p \,|\, n$ then

$$D_B(p) = \frac{p-1}{E_B(p)} = \frac{p-1}{E_B(n)} \,\Big|\, \frac{\lambda(n)}{E_B(n)} = D_B(n),$$

hence by (2.5) we obtain $D_B(n) = \operatorname{lcm}_{p\,|\,n} D_B(p)$.

To prove (2.7) assume that $l \leq \omega(n)$ and $n$ is $(B, l, T)$-exceptional. Then

$$T^l \leq \prod_{p\,|\,n} D_B(p) < n^{\delta(n,B)},$$

and taking the logarithms of both sides we obtain the first inequality of (2.7). Moreover

$$w_B(n) = \prod_{p\,|\,n} (D_B(p) - 1) \geq (T-1)^l = n^{\alpha(l,T-1,n)},$$

as claimed.

To prove the last assertion let $n \in \mathbb{N}_s$, $B \geq 2$, $M = M(n) = \gcd_{p\,|\,n}(p-1)$ and $r = \omega(n)$. Letting $p - 1 = Mm_p$ $(p\,|\,n)$, we see that the $m_p$ are distinct positive integers. The assumption $E_B(n) = E_B(p)\,|\,p-1$ yields

$$\frac{\lambda(n)}{D_B(n)} = E_B(n)\,|\,M(n). \tag{2.8}$$

By definition

$$\lambda(n) = \operatorname*{lcm}_{p\,|\,n}(p-1) = M \operatorname*{lcm}_{p\,|\,n} m_p, \tag{2.9}$$

hence by (2.8), dividing both sides of (2.9) by $M$ we obtain

$$\operatorname*{lcm}_{p\,|\,n} m_p\,|\,D_B(n),$$

and therefore for $D = D_B(n)$ we have

$$\tau(D) = \tau(D_B(n)) \geq \tau\Big(\operatorname*{lcm}_{p\,|\,n} m_p\Big) \geq r,$$

where $\tau(D)$ denotes the number of all positive divisors of $D$. Applying [H-W, Theorem 3.17, p. 262] we deduce, for any $a > \log 2$ and sufficiently large $r > c(a)$, that $D > c(a)$ and

$$\log \tau(D) < a\frac{\log D}{\log\log D},$$

hence

$$\log r \leq a\frac{\log D}{\log\log D}.$$

Since $r \leq D$, we obtain (for $D > c(a)$)

$$\log r \log\log r < \log r \log\log D \leq a \log D,$$

giving $D > r^{(\log\log r)/a}$, as claimed. ■

**3. Upper bound for $(B, l, T)$-exceptional numbers.** Here we will deal with the asymptotic behaviour of $(B, l, T)$-exceptional numbers $n \leq x$, where $T \geq 2$ and $l \geq 1$. Let $B = B(x)$, $T = T(x)$, $l = l(x)$ be functions satisfying the following conditions:

$$(c_0 \log x)^2 \leq B(x) < x, \tag{3.1}$$

$$l(x) \log T(x) \leq \frac{\log x}{\log B(x)} \log\log x, \tag{3.2}$$

where $c_0$ is some absolute positive constant. Our aim is to get an asymptotic upper bound for the cardinality of

$$\operatorname{Exc}(x; B, l, T) = \{n \leq x : n \text{ is } (B, l, T)\text{-exceptional}\} \tag{3.3}$$

as $x \to \infty$. The main result of this section gives an upper bound for $\#\operatorname{Exc}(x; B, l, T)$ in terms of $l$, $T$ and $\delta(x, B)$.

Let $n \in \mathbb{N}_s$ and consider the family $\mathcal{F}_D$ of all Dirichlet characters modulo $n$ of order dividing $D = \operatorname{lcm}_{p\,|\,n} D_B(p)$ that can represented as

$$\chi = \prod_{p\,|\,n} \psi_p^{\frac{p-1}{D_B(p)} m_p}$$

where $\psi_p$ is a fixed Dirichlet character modulo $p$ of order $p-1$ and $m_p$ runs over the set of all residue classes modulo $D_B(p)$. Let $\mathcal{F}_D^* \subset \mathcal{F}_D$ be the set of corresponding primitive characters. We denote by $[1, B]$ the set of positive integers $b$ not exceeding $B$.

We have

Lemma 3.1. *Let $n \in \mathbb{N}_s$ and $\mathcal{F}_D, \mathcal{F}_D^*$ be as above. Then for any $\chi \in \mathcal{F}_D$,*

$$\chi([1, B]) \subset \{0, 1\}. \tag{3.4}$$

*Moreover*

$$\#\mathcal{F}_D^* = \prod_{p\,|\,n} [D_B(p) - 1]. \tag{3.5}$$

*In particular for prime $n$ all $D_B(p)-1$ nonprincipal characters are primitive.*

*Proof.* Assume that $b \le B$ and $\gcd(b, n) = 1$. Then

$$\begin{aligned}\chi(b) &= \prod_{p\,|\,n} \psi_p^{\frac{p-1}{D_B(p)} m_p}(b \bmod p) = \prod_{p\,|\,n} \psi_p^{m_p}[(b \bmod p)^{E_B(p)}] \\ &= \prod_{p\,|\,n} \psi_p^{m_p}(1) = 1.\end{aligned}$$

Moreover (see [Dav, Section 5]) $\chi$ is primitive provided $m_p \pmod{D_B(p)} \neq 0$. Hence the number of primitive $\chi$'s is equal to $\prod_{p\,|\,n}[D_B(p) - 1] = D$, as required. ∎

Let $L(s, \chi)$ be the $L$-function attached to $\chi$ and let $N(\sigma, t, \chi) = \#\{\rho : L(\rho, \chi) = 0,\ |\operatorname{Im} \rho| \le t,\ \operatorname{Re} \rho \ge \sigma\}$.

Lemma 3.2 (see e.g. [Mon2, Section 9, Theorem 1]). *There exists an absolute positive constant $c_0$ such that for any Dirichlet character $\chi = \chi \pmod n$ and for $\delta$ satisfying $(\log n)^{-1} < \delta \le 1/2$ we have*

$$N(1 - \delta, \delta^2 \log n, \chi) = 0 \ \Rightarrow\ B_\chi < (c_0 \delta \log n)^{1/\delta}, \tag{3.6}$$

*where $B_\chi$ is the least character nonresidue, i.e. the least $b \in \mathbb{N}$ such that $\chi(b) \notin \{0, 1\}$.*

LEMMA 3.3 (see [Mon1, Theorem 12.2]). *Let $Y \ge 1$ and $t \ge 0$. Then for $1/2 \le \sigma \le 4/5$,*

$$\sum_{n\le Y} \sum_{\chi \bmod n}^{*} N(\sigma,t,\chi) \ll (Y^2(t+2))^{\frac{3(1-\sigma)}{2-\sigma}} (\log Y(t+2))^9,$$

*while for $4/5 \le \sigma \le 1$ we have*

$$\sum_{n\le Y} \sum_{\chi \bmod n}^{*} N(\sigma,t,\chi) \ll (Y^2(t+2))^{2(1-\sigma)/\sigma} (\log Y(t+2))^{14}$$

*where $\sum^*$ denotes the summation over primitive characters modulo $n$.*

The following theorem gives an upper bound for the number of $(B,l,T)$-exceptional numbers. Condition (3.8) below is assumed to avoid the trivial bound for $\#\operatorname{Exc}(x;B,l,T)$ following from (2.7) of Proposition 2.3.

THEOREM 3.4. *There exists an absolute constant $c_0 > 0$ such that for any $c_1 > 14$ and $B = B(x)$, $T = T(x) \ge 2$, $l = l(x) \ge 1$ satisfying*

$$(c_0 \log x)^{\max(5, \frac{5}{2(c_1-14)})} \le B(x) < x, \tag{3.7}$$

$$l(x)\log T(x) \le \frac{\log x}{\log B(x)} \log\log x, \tag{3.8}$$

*we have*

$$\#\operatorname{Exc}(x;B,l,T) \ll (T-1)^{-l} x^{5\delta_0} \log^{c_1} x,$$

*where $\delta_0 = \delta(x^{c_0}, B)$ and $x > x_0$ is sufficiently large.*

*Proof.* Consider any character $\chi \in \mathcal{F}_D^*$ where $D = \operatorname{lcm}_{p\mid n} D_B(p)$ and $B = B(x)$. Then by Lemma 3.1 the least character nonresidue $B_\chi$ is $> B(x)$. Let $\delta_0 = \log\log x^{c_0}/\log B(x)$. By (3.7) we have

$$(c_0 \log x)^2 \le B(x) < x, \tag{3.9}$$

which in turn implies that

$$\frac{1}{\log x} < \delta_0 \le \frac{1}{2} \tag{3.10}$$

for $x > x_0(c_0)$. Since $\delta_0 \le 1$ we have

$$B(x) = (c_0 \log x)^{1/\delta_0} \ge (c_0\delta_0 \log x)^{1/\delta_0},$$

and in view of Lemma 3.2 the condition $B_\chi > B(x) \ge (c_0\delta_0\log x)^{1/\delta_0} \ge (c_0\delta_0\log n)^{1/\delta_0}$ implies that

$$N(1-\delta_0, \delta_0^2 \log x, \chi) \ge N(1-\delta_0, \delta_0^2\log n, \chi) \ge 1$$

provided

$$(\log n)^{-1} < \delta_0 \le 1/2. \tag{3.11}$$

We consider the sum

$$\sum := \sum_{\substack{n\le x\\ n\ (B,l,T)\text{-exc}}} \sum_{\chi \bmod n}^{*} N(1-\delta_0, t_0, \chi) \quad \text{with} \quad t_0 = \delta_0^2 \log x.$$

If $n \le B(x)$ then $n$ is not $(B,l,T)$-exceptional, hence without looss of generality we may assume that $n > B(x)$ in the sum above. Then the left bound of (3.11) follows since

$$(\log n)^{-1} < (\log B(x))^{-1} \le \frac{\log\log x^{c_0}}{\log B(x)} \quad \text{for } x > x_0 \text{ sufficiently large,}$$

while the right bound of (3.11) follows from the right bound of (3.10).

Now, we are in a position to apply Lemma 3.3 to the sum $\sum$ with $Y = x$, $\delta = \delta_0$, $\sigma = 1-\delta_0$, $t = t_0 = \delta_0^2 \log x \le \log x$ to see that $3/(2-\sigma) = 2/\sigma = 5/2$ for $\sigma = 4/5$ and obtain

$$\sum \ll (x^2 \log x)^{\frac{5}{2}\delta} [\log(x\log x)]^{14} \ll x^{5\delta} (\log x)^{14+\frac{5}{2}\delta} \ll x^{5\delta} \log^{c_1} x. \tag{3.12}$$

The last inequality follows since by (3.7) we have $14 + \frac{5}{2}\delta \le c_1$. Finally, in view of Lemma 3.1 we obtain

$$\begin{aligned}\sum &\ge \sum_{\substack{n\le x\\ n\ (B,l,T)\text{-exc}}} \prod_{p\,|\,n} (D_B(p)-1)\\ &\ge \sum_{\substack{n\le x\\ n\ (B,l,T)\text{-exc}}} (T(x)-1)^{l(x)} = (T(x)-1)^{l(x)} \#\operatorname{Exc}(x; B, l, T),\end{aligned}$$

which gives the required upper bound for the cardinality of $\operatorname{Exc}(x; B, l, T)$. ∎

Denoting by $\operatorname{Exc}(x; B)$ the set of $B$-exceptional numbers $\le x$ we apply the bound (3.12) for the sum $\sum$ above with $T = T(x) = 2$ and $l = l(x) = \omega(\lfloor x \rfloor)$, where $\lfloor x \rfloor$ denotes the integral part of $x$, to conclude that under (3.7) we have

$$\sum_{n\in \operatorname{Exc}(x;B)} w_B(n) \ll x^{5\delta_0} \log^{c_1} x. \tag{3.13}$$

Letting $\alpha(a,b,c) = a \log b/\log c$ we see that condition (3.8) of Theorem 3.4 is equivalent to the inequality $\alpha(l,T,x) \le \delta(x,B)$. Since $(T-1)^l = x^{\alpha(l,T-1,x)}$ we directly deduce

COROLLARY 3.5. *Let $T = T(x) \ge 2$, $l = l(x) \ge 1$ and $\alpha(a,b,c) = a\log b/\log c$. There exists an absolute constant $c_0 > 0$ such that for any positive constant $c_1 > 14$, $B = B(x)$ and $\alpha(l,T,x)$ satisfying*

$$(c_0 \log x)^{\max(5, \frac{5}{2(c_1-14)})} \le B(x) < x, \tag{3.14}$$

$$\alpha(l,T,x) \le \delta(x,B), \tag{3.15}$$

*we have*

$$\#\operatorname{Exc}(x;B,l,T)\ll x^{5\delta_0-\alpha(l,T-1,x)}\log^{c_1}x \tag{3.16}$$

*for $x>x_0$ sufficiently large.*

The above estimate is strong for relatively small values of $B=B(x)$. On the other hand, if $B(x)\ge \exp\{(\log\log x)^{5/3+\varepsilon}\}$ then a significantly better estimate is given by

THEOREM 3.6. *Let $\varepsilon>0$ be sufficiently small and $x>x_0(\varepsilon)$ sufficiently large. Let $l=l(x)\ge 1$, $T=T(x)\ge 2$, and $B=B(x^2)$ satisfy*

$$\exp\{(\log\log x^2)^{5/3+\varepsilon}\}\le B(x^2)<x^2. \tag{3.17}$$

*Then for $x\to\infty$,*

$$\begin{aligned}\#\operatorname{Exc}&(x;B(x^2),l,T)\\ &<(\pi+1)e^{\gamma}(\log\log x)x^{2\delta(x^2,B(x^2))-\alpha(l,T-1,x)}(1+o(1)),\end{aligned} \tag{3.18}$$

*where*

$$\alpha(a,b,c)=\frac{a\log b}{\log c},\qquad \delta(x,y)=\frac{\log\log x}{\log y}.$$

The proof of Theorem 3.6 is based on the following two lemmas.

LEMMA 3.7 (see [Gal]). *For every sequence $(z_b)_{M+1\le b\le M+y}$ of complex numbers and Dirichlet characters $\chi=\chi\ (\mathrm{mod}\ n)$ we have*

$$\sum_{n\le x}\frac{n}{\varphi(n)}\sum_{\chi \bmod n}{}^{*}\Big|\sum_{b=M+1}^{M+y}z_b\chi(b)\Big|^2\le (x^2+\pi y)\sum_{b=M+1}^{M+y}|z_b|^2, \tag{3.19}$$

*where $\sum^*$ denotes summation over primitive characters modulo $n$.*

LEMMA 3.8 (see [F-T]). *Let $\psi_n(y,B)=\#\{b\le y:\gcd(b,n)=1,\ P^+(b)\le B\}$. For any sufficiently small $\varepsilon>0$, sufficiently large $y>y_0(\varepsilon)$, $B=B(y)$ and $n$ satisfying*

$$\exp\{(\log\log y)^{5/3+\varepsilon}\}\le B(y)\le y, \tag{3.20}$$

$$\log\log(n+2)\le\left(\frac{\log y}{\log\{\log y/\log B+1\}}\right)^{1-\varepsilon}, \tag{3.21}$$

*we have*

$$\psi_n(y,B)=\frac{\phi(n)}{n}\psi(y,B)(1+\varDelta(n,B,y)) \tag{3.22}$$

*where*

$$\varDelta(n,B,y)\ll\frac{\log\log(nB)\log\log y}{\log y}. \tag{3.23}$$

*Proof of Theorem 3.6.* For $\chi = \chi \pmod{n}$ we let

$$T(\chi) = \sum_{b \le y} z_b \chi(b), \qquad S(x,y) = \sum_{n \le x} \frac{n}{\varphi(n)} \sideset{}{^*}\sum_{\chi \bmod n} |T(\chi)|^2,$$

where

$$z_b = \begin{cases} 1 & \text{if } P^+(b) \le B, \\ 0 & \text{otherwise.} \end{cases}$$

If $b \le B$ satisfies $\gcd(b,n) = 1$ then by Lemma 3.1, $\chi(b) = 1$ for all $w_B(n)$ Dirichlet characters of orders dividing $\operatorname{lcm}_{p \mid n} D_B(p)$. Hence for every $B$-exceptional number $n$ the inner sum above is equal to

$$\sideset{}{^*}\sum_{\chi \bmod n} \psi_n(y, B(y))^2 = w_B(n) \psi_n(y, B(y))^2.$$

By Lemma 3.7 (with $M = 0$) we obtain

$$\sum_{n \in \mathrm{Exc}(x; B(y))} \frac{n}{\varphi(n)} w_B(n) \psi_n(y, B(y))^2 \le (x^2 + \pi y) \psi(y, B(y)). \tag{3.24}$$

Now applying Lemma 3.8 we conclude that for sufficiently large $y > y_0(\varepsilon)$ and $B = B(y)$ satisfying (3.20) we have

$$\sum_{n \in \mathrm{Exc}(x; B(y))} \frac{\varphi(n)}{n} w_B(n) (1 + \Delta(n, B(y), y))^2 \le \frac{x^2 + \pi y}{\psi(y, B(y))}. \tag{3.25}$$

Choosing $y = x^2$ and applying the lower bound for $\psi(y, B(y))$ given by Lemma 2.2 we obtain

$$\begin{aligned} \sum_{n \in \mathrm{Exc}(x; B)} \frac{\varphi(n)}{n} w_B(n) &\le (\pi + 1) \frac{x^2}{\psi(x^2, B(x^2))} (1 + o(1)) \\ &\le (\pi + 1) x^{2\delta(x^2, B(x^2))} (1 + o(1)) \end{aligned} \tag{3.26}$$

as $x \to \infty$ provided $B(y)$ $(y = x^2)$ satisfies (3.20). Since $w_B(n) = \prod_{p \mid n} (D_B(p) - 1) \ge (T-1)^l = x^{\alpha(l, T-1, x)}$ and (by [H-W, Theorem 328, p. 267])

$$\liminf_{n \to \infty} \frac{\phi(n) \log\log n}{n} = e^{-\gamma},$$

in the region

$$l \log T \le \delta(x^2, B(x^2)) \log x$$

we obtain the required estimate

$$\# \mathrm{Exc}(x; B(x^2), l, T) \le (\pi + 1) e^{\gamma} x^{2\delta(x^2, B(x^2)) - \alpha(l, T-1, x)} \log\log x \, (1 + o(1))$$

as $x \to \infty$. ∎

**4. $B$-special numbers.** In this section we will investigate the numbers occurring in the reduction of factoring $n$ to computation of $\phi(n)$. In this connection we give

DEFINITION 4.1. A composite number $n \in \mathbb{N}_s$ is called *$B$-special* if for every prime $p \mid n$ we have

$$D_B(p) \mid D_B(n). \tag{4.1}$$

Directly from the definition, for every $B$-special number $n$ we have $\operatorname{lcm}_{p \mid n} D_B(p) \mid D_B(n)$, and Proposition 2.3 implies that $D_B(n) = \operatorname{lcm}_{p \mid n} D_B(p)$.

The numbers satisfying (4.1) play a significant role in the reduction of factoring $n$ to the computation of $\phi(n)$. The complexity of such reduction depends on the size of the minimal local distance $D_B(p)$.

Certainly the global distance $D_B(n)$ does not exceed the product $\prod_{p \mid n} D_B(p)$ that well approximates the value of $w_B(n)$. Therefore in view of inequality (3.13) we obtain a bound for the average value of $D_B(n)$ over $B$-special numbers such that $\omega(D_B(p)) \ge 1$ for every prime $p \mid n$. From the point of view of applications an important task is to control the relation between the values of $\omega(D_B(n))$ and $\omega(D_B(p))$, as given in the definition below. For $B$-special numbers with large values of $\omega(D_B(p))$ we will prove a significantly stronger inequality for the average value of $D_B(n)$. This leads to the definition of $(B,\beta)^*$-special numbers ($\beta \in (0,1)$) given by

DEFINITION 4.2. The number $n \in \mathbb{N}_s$ is called *$(B,\beta)^*$-special* if it is *$B$-special* and

$$\omega(D_B(n)) \le \beta\omega(n) \min_{p \mid n} \omega(D_B(p)). \tag{4.2}$$

Let $t \ge 2$ and $w_B(n) = \prod_{p \mid n}(D_B(p) - 1)$. Let $S^*(x; B, \beta, t)$ be the set of $(B,\beta)^*$-special numbers $n \in (x/2, x]$ with $t_n := \min_{p \mid n} \omega(D_B(p)) \ge t$. We will prove

THEOREM 4.3. *For any $\eta = \eta(x) \in (0, 1/2)$ and sufficiently large $t > 2/\eta$ we have*

$$\sum_{n \in S^*(x; B, 1-2\eta, t)} D_B(n) \le \sum_{n \in \operatorname{Exc}(x; B, \omega(n), t^t)} w_B(n) \exp\biggl\{-\omega(n)\eta t \log(\eta t)\biggl(1 + \frac{\log(1 - t^{-t})}{\eta t \log(\eta t)}\biggr)\biggr\}.$$

In the proof of Theorem 4.3 we will need

LEMMA 4.4. *Let $r, s, d_1, \ldots, d_r \in \mathbb{N}$ and let the largest squarefree divisor of $d_1 \ldots d_r$ be $k(d_1 \ldots d_r) = q_1 \ldots q_s$ with prime $q_1 < \cdots < q_s$. Then for any*

$\alpha \in (0,1)$ *and* $\tau, s, r$ *satisfying*

$$\max(1/\alpha, 2/(1-\alpha)) < \tau < s < \tau r,$$
$$\#\{(i,j) : \nu_{q_i}(d_j) \geq 1,\ i \leq s,\ j \leq r\} \geq r\tau$$

*we have*

$$\frac{\prod_{j\leq r} d_j}{\mathrm{lcm}_{j\leq r}\, d_j} \geq \{(1-\alpha)\tau\log((1-\alpha)\tau)\}^{\alpha r\tau+(1-\alpha)\tau-s-1}. \tag{4.3}$$

*Proof.* Let $K(i) = \#\{j : \nu_{q_i}(d_j) \geq 1\}$, where $\alpha \geq 1/\tau$ and $l = l(\alpha)$ satisfy

$$\begin{aligned} K(s)+K(s-1)+\cdots+K((s-(l-2)) &< \alpha r\tau \\ &\leq K(s)+\cdots+K(s-(l-2))+K(s-(l-1)). \end{aligned}$$

Hence summing the first $s-(l-1)$ numbers $K(i)$ we have, by assumption,

$$K(1)+\cdots+K(s-l)+K(s-(l-1)) > (1-\alpha)r\tau.$$

Since $K(i) \leq r$ for $i \leq s$, we obtain

$$(1-\alpha)r\tau < r(s-(l-1)),$$

i.e.

$$s-(l-1) > (1-\alpha)\tau.$$

Therefore the sum of $K(i)$ for $i \geq s-(l-1)$ is at least $\alpha r\tau$, where $s-(l-1) \geq \lceil (1-\alpha)\tau\rceil$ and $\lceil y\rceil$ stands for the smallest integer $\geq y$. Thus

$$\begin{aligned} \frac{\prod_{j\leq r} d_j}{\mathrm{lcm}_{j\leq r}\, d_j} &= \prod_{i\leq s} q_i^{\sum_j \nu_{q_i}(d_j)-\max_{j\leq r}\nu_{q_i}(d_j)} \\ &\geq \prod_{\lceil(1-\alpha)\tau\rceil\leq i\leq s} q_i^{\sum_{j\leq r}\nu_{q_i}(d_j)-\max_{j\leq r}\nu_{q_i}(d_j)} \geq q_{\lceil(1-\alpha)\tau\rceil}^{\alpha r\tau-(s-\lceil(1-\alpha)\tau\rceil)-1}. \end{aligned}$$

By [Dus] we know that the $k$th prime number is $> k\log k$ for $k > 2$. Therefore letting $k = \lceil(1-\alpha)\tau\rceil$ we find that for $\tau > 2/(1-\alpha)$,

$$q_{\lceil(1-\alpha)\tau\rceil} \geq \lceil(1-\alpha)\tau\rceil \log\lceil(1-\alpha)\tau\rceil.$$

Since $\alpha r\tau - (s-\lceil(1-\alpha)\tau\rceil)-1 \geq \alpha r\tau+(1-\alpha)\tau-s-1$, we obtain (4.3). ∎

Let $\alpha = 1-\eta$, $\tau = t$ and suppose $s, r$ satisfy

$$\max\left(\frac{1}{1-\eta}, \frac{2}{\eta^2}\right) < t < s < tr(1-2\eta).$$

Then for $t > 2/\eta$, in view of the inequality $\alpha rt+(1-\alpha)t-s-1 \geq \eta rt$, we have $q_{\lceil(1-\alpha)\tau\rceil}^{\alpha r\tau-(s-\lceil(1-\alpha)\tau\rceil)-1} \geq (\eta t\log\eta t)^{\eta rt}$, and thus we obtain

Corollary 4.5. *Let $q_1 \ldots q_s$ be the largest squarefree divisor of $d_1 \ldots d_r$ and assume that $\omega(d_j) \geq t$ for every $j \leq r$. Then for any $\eta \in (0, 1/2)$ and $t, s, r \in \mathbb{N}$ satisfying*

$$2/\eta < t < s < tr(1-2\eta)$$

*we have*

$$\frac{\prod_{j\leq r} d_j}{\mathrm{lcm}_{j\leq r}\, d_j} \geq \exp\bigl\{r\eta t\bigl(\log(\eta t) + \log\log \eta t\bigr)\bigr\}. \tag{4.4}$$

*Proof of Theorem 4.3.* Let $n \in S^*(x; B, 1-2\eta, t)$, where $\eta = \eta(x) \in (0, 1/2)$. Then by [Rob] for $t > t_0 = \exp\exp(1.077)$ the product of $t$ primes is $\geq t^t$, and therefore $D_B(p) \geq t^t$ for sufficiently large $t > t_0$, so that $n$ is $(B, \omega(n), t^t)$-exceptional. It remains to prove that then

$$D_B(n) \leq w_B(n)\exp\biggl\{-\omega(n)\eta t\log(\eta t)\biggl(1 + \frac{\log(1-t^{-t})}{\eta t\log(\eta t)}\biggr)\biggr\}$$

provided $t > \max(t_0, 2/\eta)$. We have

$$\begin{aligned} w_B(n) &= \prod_{p\,|\,n}(D_B(p) - 1) = \prod_{p\,|\,n}\biggl\{D_B(p)\biggl(1 - \frac{1}{D_B(p)}\biggr)\biggr\} \\ &\geq \Bigl(\prod_{p\,|\,n} D_B(p)\Bigr)(1-t^{-t})^{\omega(n)}. \end{aligned} \tag{4.4a}$$

Letting $r = \omega(n)$, $s = \omega(\prod_{p\,|\,n} D_B(p))$ and $t = t_n = \min_{p\,|\,n}\omega(D_B(p)) > \max(t_0, 2/\eta)$ in Corollary 4.5 we see that if $n \in S^*(x; B, 1-2\eta, t_n)$ then by (4.2) we have $s = \omega(\prod_{p\,|\,n} D_B(p)) = \omega(k(\prod_{p\,|\,n} D_B(p))) = \omega(k(\mathrm{lcm}_{p\,|\,n} D_B(p))) = \omega(\mathrm{lcm}_{p\,|\,n} D_B(p)) = \omega(D_B(n)) \leq (1-2\eta)\omega(n)t_n$, and the inequalities for $t, r$ and $s$ required in Corollary 4.5 are satisfied. Therefore by Proposition 2.3 we have $D_B(n) = \mathrm{lcm}_{p\,|\,n} D_B(p)$, and since $t_n \geq t$ we obtain

$$\begin{aligned} D_B(n) &= w_B(n)\Bigl(\mathop{\mathrm{lcm}}_{p\,|\,n} D_B(p)\Bigr)/w_B(n) \\ &\leq w_B(n)\Bigl(\Bigl(\mathop{\mathrm{lcm}}_{p\,|\,n} D_B(p)\Bigr)/\prod_{p\,|\,n} D_B(p)\Bigr)(1-t_n^{-t_n})^{-\omega(n)} \\ &\leq w_B(n)\exp\{-\omega(n)\eta t_n\log(\eta t_n) - \omega(n)\log(1-t_n^{-t_n})\} \\ &= w_B(n)\exp\biggl\{-\omega(n)\eta t_n\log(\eta t_n)\biggl(1 + \frac{\log(1-t_n^{-t_n})}{\eta t_n\log(\eta t_n)}\biggr)\biggr\} \\ &\leq w_B(n)\exp\biggl\{-\omega(n)\eta t\log(\eta t)\biggl(1 + \frac{\log(1-t^{-t})}{\eta t\log(\eta t)}\biggr)\biggr\} \end{aligned}$$

for sufficiently large $t > \max(t_0, 2/\eta)$. This completes the proof of Theorem 4.3. ■

Below we will prove the average estimate of the global distance $D_B(n)$ for $(B, 1-2\eta)^*$-special numbers, where $\eta$ depends on the value of the largest squarefree divisor of $D_B(n)$. We let $\eta = \eta(x)$ and recall that $t_n = \min_{p\,|\,n} \omega(D_B(p))$.

DEFINITION 4.6. A $B$-special number $n$ is called $(x; B, \eta, t)$-*special* if $n \in (x/2, x]$ and

$$k(D_B(n)) \le n^{(1-3\eta)\delta}, \qquad \omega(n) t \log t \ge (1-\eta)\delta \log x, \tag{4.5}$$

where $k(m)$ stands for the largest squarefree divisor of $m$ and $\delta = \delta(x, B)$.

We denote by $S(x; B, l, t)$ and $S(x; B, \eta, l, t)$ the sets of $B$-special numbers from the interval $(x/2, x]$ and of $(x; B, \eta, t)$-special numbers respectively, such that $\omega(n) \ge l$ and $t_n \ge t$.

Assume that $B = B(x)$, $l = l(x) \ge 2$, $t = t(x) \ge 2$ are functions satisfying

$$lt \log t \le \delta \log x. \tag{4.6}$$

It is easily seen from (5.3) of Proposition 5.1 that (4.6) gives a natural restriction for the parameters $l$ and $t$ describing the numbers $n \in S(x; B, l, t)$. In the next theorem we give an upper bound for the cardinality of $S(x; B, l, t)$ and the average value of $D_B(n)$ over $S(x; B, \eta, l, t)$.

THEOREM 4.7. *Let $\gamma = \gamma(l, t, x) = lt \log t / \log x$. There exists a positive absolute constant $c_0$ such that for any $c_1 > 14$ and functions $B = B(x)$, $\eta = \eta(x) < 1/3$, $l = l(x) \ge 2$, and $t = t(x) \ge 2$ satisfying*

$$(c_0 \log x)^{\max(5, \frac{5}{2(c_1 - 14)})} \le B(x) < x, \tag{4.7}$$

$$\left(\frac{\log 2}{2\delta \log x}\right)^{1/2} < \eta(x) < 1/3, \tag{4.8}$$

$$\gamma(l, t, x) \le \delta(x, B(x)), \tag{4.9}$$

*for sufficiently large $t$ and $x$ we have*

$$\#S(x; B, l, t) \ll x^{5\delta_0 - (\gamma(l,t,x) + l \log(1 - t^{-t})/\log x)} \log^{c_1} x. \tag{4.10}$$

*Furthermore if $B(x)$ satisfies*

$$x^{1/2} > B(x) \ge \exp\{(\log\log x)^{5/3+\varepsilon'}\}$$

*then for $x > x_0(\varepsilon')$ we have*

$$\#S(x; B(x^2), l, t) \ll x^{2\delta(x^2, B(x^2)) - (\gamma(l,t,x) + l \log(1 - t^{-t})/\log x)} \log\log x. \tag{4.11}$$

*Moreover if additionally* $\eta(x) > (2/t)^{1/2}$ *then*

$$\sum_{n\in S(x;B,\eta,l,t)} D_B(n) \ll x^{5\delta_0}\log^{c_1} x \exp\left\{-l\eta t\log(\eta t)\left(1-\frac{2t^{-t}}{\eta t\log(\eta t)}\right)\right\} \tag{4.12}$$

*where* $\delta_0 = \delta(x^{c_0}, B(x))$. *As in* (4.11), *in the RHS of* (4.12) *the quantity* $x^{5\delta_0}\log^{c_1} x$ *can be replaced by* $x^{2\delta(x^2,B(x^2))}\log\log x$, *provided* $B(x) \geq \exp\{(\log\log x)^{5/3+\varepsilon'}\}$ *and* $x > x_0(\varepsilon')$ *is sufficiently large.*

The proof of Theorem 4.7 will be given in the next section. A significant ingredient in the proof of (4.12) is the fact that if $n \in S(x; B, \eta, l, t)$ then $n \in S^*(x; B, 1-2\eta, t)$, and thus we are able to apply Theorem 4.3 giving the exponential factor decay in the corresponding upper bound for $D_B(n)$.

Now let us apply the estimate (4.11) for a function $B(x)$ of subexponential order, $B_u(x) = \exp\{(\log x)^{1/u}\}$ $(u \geq 3)$. It can be directly checked that if condition (4.13) below holds true, then $B_u(x) > \exp((\log\log x)^2) > \exp((\log\log x)^{5/3+\varepsilon'})$ for $\varepsilon' < 1/3$, hence by (4.11) we deduce

Corollary 4.8. *Let* $B_u(x) = \exp\{(\log x)^{1/u}\}$, *let* $\varepsilon > 0$ *be sufficiently small and let* $u = u(x)$ *satisfy*

$$3 \leq u(x) < \varepsilon\frac{\log\log x}{\log\log\log x}. \tag{4.13}$$

*Then*

$$\#S(x; B_u, l_u, t_u) \ll x^{2\delta(x^2,B(x^2))-(\delta^{u-2}/u)(1-2\varepsilon)}\log\log x \tag{4.14}$$

*where* $l_u = \delta_u^{-1}$,

$$t_u = \delta_u^{-1}(\log\log x)^{u-1}, \qquad \delta_u = \log\log x/\log B_u(x) = \log\log x/(\log x)^{1/u}$$

*and* $x \geq x_0(\varepsilon)$ *is sufficiently large.*

*Proof.* In view of (4.13) and (4.10) it is sufficient to prove that

$$\gamma(l_u, t_u, x) \geq (1-\varepsilon)\delta_u^{u-2}/u \quad\text{and}\quad -l_u\log(1-t_u^{-t_u})/\log x \leq \varepsilon\gamma(l_u, t_u, x),$$

where $\gamma(l_u, t_u, x) = l_u t_u \log t_u/\log x$ and $t_u = t_u(\varepsilon)$ is sufficiently large.

Indeed, we have $-l_u\log(1-t_u^{-t_u})/\log x \leq 2l_u t_u^{-t_u}/\log x \leq \varepsilon\gamma(l_u, t_u, x)$ for sufficiently large $t_u \geq t(\varepsilon)$.

To prove the left inequality above, we have by straightforward calculation

$$\begin{aligned}\gamma(l_u,t_u,x) &= l_ut_u\log t_u/\log x\\ &= \delta_u^{-2}(\log\log x)^{u-1}\log(\delta_u^{-1}(\log\log x)^{u-1})/\log x\\ &= \delta_u^{-2}(\log\log x)^{u-1}\big(\log\delta_u^{-1}+(u-1)\log\log\log x\big)/\log x\\ &= \frac{1}{\log x}\left(\delta_u^{-2}(\log\log x)^{u-1}\left(\frac{1}{u}\log\log x-\log\log\log x\right)\right)\\ &= \frac{1}{\log x}\left(\delta_u^{-2}\frac{(\log\log x)^u}{u}\left(1-\frac{u\log\log\log x}{\log\log x}\right)\right)\\ &= \frac{1}{\log x}\left(\delta_u^{u-2}\frac{\log x}{u}\left(1-\frac{u\log\log\log x}{\log\log x}\right)\right)\\ &= \left(\frac{\delta_u^{u-2}}{u}\left(1-\frac{u\log\log\log x}{\log\log x}\right)\right)\ge(1-\varepsilon)\frac{\delta_u^{u-2}}{u}\end{aligned}$$

provided $x\ge x_0(\varepsilon)$. This completes the proof since $B_u(x)>\exp\{(\log\log x)^2\}$ for $u\le\frac{\log\log x}{2\log\log\log x}$. ■

**5. Application to conditional factoring.** In this section we deduce Theorem 4.7 from Theorems 3.4 and 4.3 and apply the resulting estimate to conditional factoring. We start from an auxiliary result giving in particular sufficient conditions for $n\in\mathbb{N}_s$ to be $B$-special or $(B,\omega(n),T)$-exceptional, where $T\ge 2$.

PROPOSITION 5.1.

(i) *Asume that $n\in\mathbb{N}_s$ and for every $b\le B$ such that* $\gcd(b,n)=1$ *and every prime $q\mid\operatorname{ord}_n b$ we have*

$$\gcd(b^{(\operatorname{ord}_n b)/q}-1,n)=1. \tag{5.1}$$

*Then $n$ is $B$-special.*

(ii) *Additionally if for any positive integer $\tau<T$ (with $T\ge 2$) we have*

$$\gcd(\tau E_B(n)+1,n)=1 \tag{5.2}$$

*then $n$ is $(B,\omega(n),T)$-exceptional. Moreover if* (5.2) *holds for some $n\in(x/2,x]$ such that $\omega(n)\ge l$ and every $\tau\mid\prod_{p\mid n}D_B(p)$ satisfying $\omega(\tau)<t$, then $n\in S(x;B,l,t)$.*

(iii) *Furthermore if $l\ge 2$ and $t$ is sufficiently large then we have the following. If $n\in S(x;B,l,t)$, then*

$$lt\log t\le\delta\log x. \tag{5.3}$$

*Moreover if $n\in S(x;B,l,t)$ and (see Notation) $k(D_B(n))\le n^{\alpha\delta}$, where $\delta=\delta(x,B)$ and $\alpha\in(0,1)$, then*

$$\omega(D_B(n))\le\frac{\alpha\delta\log x}{\log t}.$$

*Proof.* Condition (5.1) implies that $\mathrm{ord}_n b = \mathrm{ord}_p b$ for every prime $p \mid n$ and $b \le B$ such that $\gcd(b,n) = 1$. Hence $E_B(n) = \mathrm{lcm}_{b\le B} \mathrm{ord}_n b = \mathrm{lcm}_{b\le B} \mathrm{ord}_p b = E_B(p)$, and therefore by Proposition 2.3 we obtain $D_B(n) = \mathrm{lcm}\, D_B(p)$, so $n$ is $B$-special. Letting $\tau = D_B(p)$ we conclude that the LHS of (5.2) would be divisible by $p$ if $D_B(p) < T$, giving a contradiction. Therefore $D_B(p) \ge T$ for every prime $p \mid n$, and hence $n$ is $(B, \omega(n), T)$-exceptional. The last conclusion of (ii) easily follows by remarking that (5.2) implies that each $D_B(p)$ must have at least $t$ prime divisors, hence belongs to $S(x; B, l, t)$.

To prove (iii) let $n \in S(x; B, l, t)$ and $\min_{p\mid n} D_B(p) = q_1 \ldots q_t$. Then by (2.6) for prime arguments we have $(q_1 \ldots q_t)^l \le \prod_{p\mid n} D_B(p) < \prod_{p\mid n} p^\delta \le x^\delta$. Hence taking the logarithms of both sides we obtain the required inequality in view of [Rob].

To prove the last assertion, let $s = \omega(D_B(n))$. Since for $n$ $B$-special we have $D_B(p) \mid D_B(n)$, one concludes that $s \ge t$, and similar arguments to those above (for $l = 1$ and $\delta$ replaced by $\alpha\delta$) give

$$t \log t \le s \log s < \alpha\delta \log x,$$

hence

$$s \le \frac{\alpha\delta \log x}{\log t}$$

provided $t$ is sufficiently large. ■

*Proof of Theorem 4.7.* To prove (4.10) we apply (3.16), while in the proof of (4.12) we apply Theorem 4.3 and Proposition 5.1. Finally, (4.11) will follow from Theorem 3.6.

First, let us remark that if $n \in S(x; B, l, t)$ then $n$ is also $(B, l, T)$-exceptional for $T = t^t$. To apply Corollary 3.5 we remark that $T - 1 = \theta t^t$ for $\theta = 1 - t^{-t}$. Therefore

$$\alpha(l, T-1, x) = l \log(\theta t^t)/\log x = \gamma(l, t, x) + l \log(1 - t^{-t})/\log x,$$

and so by (3.16) we obtain

$$\#S(x; B, l, t) \ll x^{5\delta_0 - \alpha(l,T-1,x)} \log^{c_1} x \le x^{5\delta_0 - (\gamma(l,t,x) + l\log(1-t^{-t})/\log x)} \log^{c_1} x$$

provided $t$ is sufficiently large.

In order to prove the upper bound (4.12) we let $\eta = \eta(x)$ satisfy (4.8) and assume that $n \in \mathbb{N}_s$ belongs to the set $S(x; B, \eta, l, t)$. By (4.5) we have $\omega(n) t \log t \ge (1 - \eta)\delta \log x$ for $\delta = \delta(x, B)$. Hence applying Proposition 5.1(iii) with $\alpha = 1 - 3\eta$ we obtain

$$\begin{aligned} s = \omega(D_B(n)) &\le \frac{(1-3\eta)\delta \log x}{\log t} = \delta \log x \left(\frac{1-3\eta}{\log t}\right) \\ &\le \omega(n) t \frac{1-3\eta}{1-\eta} \le (1-2\eta)\omega(n) t \end{aligned}$$

by the second inequality of (4.5).

Therefore $n \in S^*(x; B, 1-2\eta, t)$ and $\omega(n) \geq l$. Now applying Theorem 4.3 (with $\omega(n)$ replaced by its lower bound $l$), we see that the sum appearing there is bounded by

$$\exp\biggl\{-l\eta t\log(\eta t)\biggl(1-\frac{2t^{-t}}{\eta t\log(\eta t)}\biggr)\biggr\}$$

multiplied by an upper bound for

$$\sum_{n\in\mathrm{Exc}(x;B,l,t^t)} w_B(n),$$

giving in view of (3.13) the bound

$$x^{5\delta_0}\log^{c_1}x\exp\biggl\{-l\eta t\log(\eta t)\biggl(1-\frac{2t^{-t}}{\eta t\log(\eta t)}\biggr)\biggr\}$$

provided $t \geq 2/\eta$ is sufficiently large. The estimate (4.11), and also (4.12) with $x^{5\delta_0}(\log\log x)^{c_1}$ replaced by $x^{2\delta(x^2,B(x^2))}\log\log x$, follow easily in view of (3.26), (4.4a) and the implication $n \in S(x; B, \eta, l, t) \Rightarrow n \in S^*(x; B, 1-2\eta, t)$ by repeating the arguments applied in the proof of Theorem 4.3. We remark that the condition $3 \leq u < \log\log x/2\log\log\log x$ implies $B_u(x) > \exp\{(\log\log x)^{5/3+\varepsilon'}\}$ whenever $\varepsilon' < 1/3$. This completes the proof of Theorem 4.7. ■

Below we will show that the cardinality of the set of positive integers $n \in \mathbb{N}_s$ with $n \leq x$ that cannot be factored using at most $T_u$ gcd computations (5.1) and (5.2) does not exceed

$$\#S(x; B_u, \delta_u^{-1}, \delta_u^{-1}(\log\log x)^{u-1})\log x \ll x^{2\delta-\delta^{u-2}(1-2\varepsilon)/u}\log x\log\log x, \tag{5.4}$$

where $T_u = \exp((\log x)^{1/u}(\log\log x)^{u-1})$, $B_u = B_u(x^2) = \exp((2\log x)^{1/u})$, $\delta_u = \delta(x^2, B_u(x^2))$ and $u$ satisfies

$$3 \leq u < \varepsilon\log\log x/\log\log\log x \tag{5.5}$$

for sufficiently small $\varepsilon > 0$ and sufficiently large $x > x_0(\varepsilon)$. We start from

Lemma 5.2. *Let $B \geq 3$, $n \in \mathbb{N}_s$, $n \leq y$ $(y \geq 4)$, $\tau \in \mathbb{N}$ and $D_B(p)$ be defined by* (2.2). *Then the number of divisors of $\prod_{p\mid n} D_B(p)$ having exactly $\tau$ distinct prime factors is at most*

$$\exp\biggl\{\tau\biggl[\log\biggl(\frac{\delta(y,B)\log y}{\log 2}+\tau\biggr)-\log\tau+1\biggr]\biggr\}. \tag{5.6}$$

*Proof.* Let $D \geq 2$ and let $N_\tau(d)$ stand for the number of positive divisors of $d$ having exactly $\tau$ prime factors. First we will prove that

$$\max_{d\leq D} N_\tau(d) \leq \exp\bigl\{\tau\bigl(\log(A+\tau)-\log\tau+1\bigr)\bigr\} \tag{5.7}$$

where $A = \lfloor \log D / \log 2 \rfloor$. We write

$$d = \prod_{q\,|\,d} q^{\nu_q(d)}$$

where $\omega(d) = \tau$. Hence taking the logarithms of both sides we obtain

$$\sum_{q\,|\,d} \nu_q(d) \le \lfloor \log D / \log 2 \rfloor.$$

Therefore the number of such $d$'s is by Stirling's formula at most

$$\binom{A+\tau}{\tau} \le \left(\frac{A+\tau}{\tau/e}\right)^{\tau} = \exp\{\tau(\log(A+\tau) - \log\tau + 1)\},$$

giving (5.7).

Now we apply the above estimate for $d = \prod_{p\,|\,n} D_B(p)$ and $D = y^{\delta}$ to conclude that the number of divisors in question is at most

$$\max_{d\le D} N_\tau(d) \le \exp\left\{\tau\left[\log\left(\frac{\delta\log y}{\log 2} + \tau\right) - \log\tau + 1\right]\right\},$$

where $\delta = \log\log y / \log B$. ■

To prove (5.4) we split the set of positive integers in $(1, x]$ into at most $\log x$ subintervals of type $(y/2, y]$, where $1 < y \le x$. Now let $n \in \mathbb{N}_s$ be such that $\omega(n) = l$ and $n \in (y/2, y]$. If (5.1) holds then $E_B(n) = E_B(p)$ for all primes $p\,|\,n$ and $n$ is $B$-special. Moreover letting

$$\tau = D_B(p) \,|\, \prod_{p\,|\,n} D_B(p) = \prod_{p\,|\,n} \frac{p-1}{E_B(n)} = \frac{\lambda(n)}{(E_B(n))^l}$$

we see that $\tau < y^{\delta(y,B)}$. If furthermore (5.2) holds for all $\tau \,|\, \frac{\lambda(n)}{(E_B(n))^l}$ such that $\omega(\tau) < t$ then $t_n = \min_{p\,|\,n} \omega(D_B(p)) \ge t$ and $n \in S(x; B, l, t)$. Let

$$\mathcal{T}(t,y) = t\exp\left\{t\left[\log\left(\frac{\delta(y,B)\log y}{\log 2} + t\right) - \log t + 1\right]\right\}. \tag{5.8}$$

By Lemma 5.2 the number of required computations (5.1) and (5.2) for $n \in \mathbb{N}_s$ with $n \in (y/2, y]$ is at most

$$T_u(y) = B_u(y) + \mathcal{T}(t,y) \tag{5.9}$$

where $B = B_u(y) = \exp((\log y)^{1/u})$. As follows from [Zra], the deterministic reduction of factoring $n$ to computation of the Euler function $\phi(n)$ is very efficient (i.e. of polynomial time compexity) if

$$\omega(n) \le \delta(n,B)^{-1}.$$

Therefore without loss of generality we may assume that the opposite condition $l > \delta(n, B_u)^{-1} \ge \delta(y, B_u)^{-1}$ is valid. Now let $l = l_u \ge \delta(y, B_u)^{-1}$, $t = t_u(y) = \delta(y, B_u)^{-1}(\log\log y)^{u-1}$, and fix a sufficiently small $\varepsilon > 0$ and

$u$ satisfying (5.5) with $x$ replaced by $y$. Since $n \in S(y; B, l, t)$, summation over at most $\log x$ intervals of type $(y/2, y]$ and application of Corollary 4.8 (with $x$ replaced by $y$) implies that the number of $n \in \mathbb{N}_s$ with $n \le x$ that cannot be factored in at most $T_u(x)\log x$ computations of (5.1) and (5.2) is

$$\begin{aligned} \ll (\log x) \max_{y \le x} \# S(y; B_u, l_u, t_u) &\le (\log x) \# S(x; B_u, \delta_u^{-1}, \delta_u^{-1}(\log\log x)^{u-1}) \\ &\ll x^{2\delta - \delta^{(u-2)(1-2\varepsilon)/u}} \log x \log\log x, \end{aligned}$$

where $\delta_u = \delta(x^2, B_u(x^2)) = \delta(x^2, (2\log x)^{1/u})$.

To complete the argument it is sufficient to remark that the dominating term $\mathcal{T}(t_u, x^{\delta_u})$ in $T_u(x^{\delta_u})$, where $t_u = \delta_u^{-1}(\log\log x)^{u-1}$, is

$$\begin{aligned} \mathcal{T}(t_u, x^{\delta_u}) &\le t_u \exp\biggl\{ t_u \log\biggl( \frac{\delta_u \log x}{\log 2} + t_u \biggr) \biggr\} \\ &\le t_u \exp\biggl\{ t_u \log\biggl( \delta_u \log x \left( \frac{1}{\log 2} + 1 \right) \biggr) \biggr\} \\ &\le \exp\biggl\{ t_u \biggl( \biggl( 1 - \frac{1}{u} \biggr) \log\log x + \log\log\log x + O(1) \biggr) \biggr\} \\ &\le \exp\biggl\{ t_u \biggl( \biggl( 1 - \frac{1}{2u} \biggr) \log\log x + 2\log\log\log x) \biggr) \biggr\} \\ &\le \exp\biggl\{ t_u \biggl( 1 - \frac{1}{3u} \biggr) \log\log x) \biggr\} \le \exp\biggl\{ \biggl( 1 - \frac{1}{3u} \biggr) \delta_u^{-1} (\log\log x)^u \biggr\} \\ &\le \exp\biggl\{ \biggl( 1 - \frac{1}{3u} \biggr) (\log x)^{1/u} (\log\log x)^{u-1} \biggr\} \\ &\le \exp\{ (\log x)^{1/u} (\log\log x)^{u-1} \} = T_u \end{aligned}$$

provided $u < \varepsilon \log\log x / \log\log\log x$, for any sufficiently small $\varepsilon > 0$ and sufficiently large $x > x_0(\varepsilon)$. This completes the proof of estimate (5.4) for $u$ restricted by (5.5). ∎

**Acknowledgements.** The author is grateful to an anonymous referee whose valuable comments and suggestions contributed to the clarification and improvement of the final version of the paper.

This work was supported by the NCBR grant DOBR/0001/RON/ID1/2013/01.

## References

[B-H] E. Bach and L. Huelsbergen, *Statistical evidence for small generating sets*, Math. Comp. 61 (1993), 69–82.

[Bur] R. J. Burthe, *Upper bound for least witnesses and generating sets*, Acta Arith. 80 (1997), 311–326.

[Con] J. B. Conrey, *Problem 8*, in: Future Directions in Algorithmic Number Theory, Amer. Inst. Math., 2003, http://aimath.org/WWN/primesinp/.

[Dav] H. Davenport, *Multiplicative Number Theory*, Markham Publ., Chicago, 1967.

[Dus] P. Dusart, *The $k$-th prime is greater than* $k(\log k + \log\log k - 1)$ *for* $k > 2$, Math. Comp. 68 (1999), 411–415.

[F-K] M. R. Fellows and N. Koblitz, *Self-witnessing polynomial-time complexity and prime factorization*, Designs Codes Cryptography 2 (1992), 231–235.

[F-T] E. Fouvry et G. Tenenbaum, *Diviseurs de Titchmarsh des entiers sans grand facteur premier*, in: Analytic Number Theory (Tokyo, 1988), K. Nagasaka and E. Fouvry (eds.), Lecture Notes in Math. 1434, Springer, Berlin, 1990, 86–102.

[Gal] P. X. Gallagher, *The large sieve*, Mathematika 14 (1967), 14–20.

[H-W] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford Sci. Publ., Oxford Univ. Press, 1979.

[K-P] S. Konyagin and C. Pomerance, *On primes recognizable in deterministic polynomial time*, in: The Mathematics of Paul Erdős, R. L. Graham and J. Nešetril (eds.), Springer, 1997, 176–198.

[L-W] Y.-K. Lau and J. Wu, *On the least quadratic non-residue*, preprint.

[Mon1] H. L. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Math. 227, Springer, Berlin, 1971.

[Mon2] H. L. Montgomery, *Ten Lectures on the Interface between Analytic Number Theory and Harmonic Analysis*, CBMS Reg. Conf. Ser. Math. 84, Amer. Math. Soc., Providence, RI, 1994.

[M-V] H. L. Montgomery and R. C. Vaughan, *Extreme values of Dirichlet L-functions at 1*, in: Number Theory in Progress, Vol. 2 (Zakopane-Kościelisko, 1997), K. Győry et al. (eds.), de Gruyter, Berlin, 1999, 1039–1052.

[Pom] J. Pomykała, *On $q$-orders in primitive modular groups*, Acta Arith. 166 (2014), 397–404.

[P-Z] J. Pomykała and B. Źrałek, *On reducing factorization to the discrete logarithm problem modulo a composite*, Comput. Complexity 21 (2012), 421–429.

[Rob] G. Robin, *Estimation de la fonction de Tchebychef $\theta$ sur le $k$-ième nombre premier et grandes valeurs de la fonction $\omega(n)$, nombre de diviseurs premiers de $n$*, Acta Arith. 42 (1983), 367–389.

[Zra] B. Źrałek, *A deterministic version of Pallard's $p-1$ algorithm*, Math. Comp. 79 (2010), 513–533.

Jacek Pomykała
Institute of Mathematics
Warsaw University
Banacha 2
02-097 Warszawa, Poland
E-mail: pomykala@mimuw.edu.pl