MATHEMATICS OF COMPUTATION
https://doi.org/10.1090/mcom/3368
Article electronically published on August 1, 2018

AN EXTENSION OF A RESULT ABOUT DIVISORS IN A RESIDUE CLASS AND ITS APPLICATION TO REDUCING INTEGER FACTORIZATION TO COMPUTING EULER'S TOTIENT

BARTOSZ ŹRAŁEK

Abstract. According to a theorem of Coppersmith, Howgrave-Graham, and Nagaraj, relying on lattice basis reduction, the divisors of an integer n which lie in some fixed residue class modulo a given integer A can be computed efficiently if A is large enough. We extend their algorithm to the setting when the modulus is a product $A \cdot B$, where A is given and the unknown B divides an integer whose prime factors are known. The resulting tool is applied in the context of reducing integer factorization to computing Euler's totient function φ. Our reduction is deterministic, runs in at most $\exp\left(\left(72^{-\frac{1}{3}} + o(1)\right)(\ln n)^{\frac{1}{3}}(\ln\ln n)^{\frac{2}{3}}\right)$ time, and requires no more than $\ln_8 n$ chosen values of φ. This improves upon a previous recent result both in terms of the factor $72^{-\frac{1}{3}}$ and the number of values of φ needed.

In a more concrete setting, another algorithmic extension of the theorem of Coppersmith et al. may be worth noting. We can make use of the (unknown) smooth part of a shifted divisor d of n (or even several shifts of d) to compute a suitably large modulus A and the corresponding residue class $d \bmod A$ via Chinese remaindering.

1. Introduction

Euler's totient function $\varphi(n)$ counts for natural n the number of positive integers less than or equal to n which are coprime to n. It is well known that φ is multiplicative and that $\varphi(p^e) = p^{e-1}(p-1)$ for prime p. Thus given the complete factorization of n we can efficiently compute $\varphi(n)$. The inverse task of finding a deterministic, polynomial time reduction of factoring integers to computing φ is an open problem. There are few partial results: Miller [10] found a deterministic reduction, but conditionally on the Extended Riemann Hypothesis. Long [9] gave an unconditional reduction, but one which relies on randomness (see Theorem 3 in [1]). More recently we proved [13] that a suitable reduction exists for some classes of integers (in terms of multiplicative structure). We also showed in [13] a deterministic algorithm which given the sequence of iterations $(n, \varphi(n), \varphi(\varphi(n)), \ldots)$ of $\varphi(n)$, factors n in at most $L\left(n, \frac{1}{3}\right)^{1+o(1)}$ subexponential time, where traditionally $L(x, \alpha) = \exp\left((\ln x)^{\alpha}(\ln\ln x)^{1-\alpha}\right)$. This last result is

Received by the editor July 26, 2016, and, in revised form, September 23, 2017, and March 13, 2018.

2010 *Mathematics Subject Classification.* Primary 11Y16; Secondary 11Y05.

Key words and phrases. Euler's totient function, deterministic integer factoring.

The author was partially supported by MNiSW grant IP2011 064471.

addressed here; under a slightly different assumption we will improve the reduction to obtain a $L\left(n, \frac{1}{3}\right)^{\frac{1}{\sqrt[3]{72}}+o(1)}$ time upper bound.

Theorem 1. *Let $\mathcal{A}(d)$ be an abstract algorithm which outputs $\varphi(d)$ for input $d \in \mathbb{N}$. Let $n \in \mathbb{N}$ be given. Having access to at most $\ln_8 n$ chosen outputs of $\mathcal{A}$ (with inputs less than or equal to n), we can compute deterministically the prime factorization of n in no more than $L\left(n, \frac{1}{3}\right)^{\frac{1}{\sqrt[3]{72}}+o(1)}$ time. The reduction has space complexity $O(\ln^2 n)$.*

The reduction in [13], however, had the advantage that the general form of the queries sent to algorithm/oracle $\mathcal{A}$ was known beforehand. In this more restrictive case a sharper upper bound is likewise possible.

Theorem 2. *Let $n \in \mathbb{N}$. Given the sequence of iterations $(n, \varphi(n), \varphi(\varphi(n)), \ldots)$, we can completely factor n deterministically in at most $L\left(n, \frac{1}{3}\right)^{\frac{1}{\sqrt[3]{18}}+o(1)}$ time with space complexity $O(\ln^2 n)$.*

Before getting into the details of the proofs, laid out in section 2, we have to recall the strategy used in [13]. There we noticed that it is enough to show an efficient way of retrieving the complete factorization of n from the prime factorization of the totient $\varphi(n)$. Indeed, the k-th iteration $\varphi^k(n)$ eventually equals 1 (for $k \leq 1 + \ln_2 n$), so we can reason by induction: recover the factorization of $\varphi^{i-1}(n)$ from the factorization of $\varphi^i(n)$ until we get to $i = 1$.

As we want n to be completely factored and not merely split, we seek to split recursively each divisor d of n found. If d cannot be split further, then it is prime. We called an element $b \in \mathbb{Z}_d^*$—the multiplicative group of the ring of integers modulo d—a Fermat–Euclid witness (of the compositeness of d) if

$$\operatorname{GCD}\left(b^{\frac{\operatorname{ord}_d(b)}{s}} - 1, d\right) \neq 1$$

for some prime s dividing the order $\operatorname{ord}_d(b)$ of b. Note that $\operatorname{ord}_d(b)$ and its prime factors are easily computable once we know the complete factorization of $\varphi(n)$ (a multiple of $\operatorname{ord}_d(b)$). We defined

$$\mathcal{B}_d = \left\{2, 3, \ldots, \left[L\left(d, \frac{1}{3}\right)\right]\right\} \mod d$$

(where the symbol $[x]$ represents the integer part of the real number x) and studied two cases. If $\mathcal{B}_d$ contains a Fermat–Euclid witness, d can be easily split. Otherwise we computed

$$A = \operatorname{LCM}_{b \in \mathcal{B}_d} \operatorname{ord}_d(b)$$

and noted that all the prime factors p of d lie in the residue class 1 modulo A, say $p - 1 = Ay_p$. The fact that A is "large" follows crucially from an estimate for the number $\psi(x, y)$ of y-smooth positive integers (i.e., positive integers whose prime factors do not exceed y) less than or equal to x.

Theorem 3 (Canfield, Erdős, Pomerance [2])**.** *For $u = \frac{\ln x}{\ln y} < (1 - \varepsilon)\frac{\ln x}{\ln \ln x}$, we have*

$$\psi(x, y) = xu^{-u+o(u)}$$

uniformly as $u \to \infty$.

To find a prime divisor of d two methods were used, depending on the size of the number $\omega(d)$ of distinct prime factors of d:

(1) If $\omega(d)$ is "large", $\omega(d) > \left(\frac{\ln d}{\ln\ln d}\right)^{\frac{1}{3}}$, then for p equal to the least prime factor of d we have $y_p < L\left(d, \frac{1}{3}\right)$. A trivial search $y_p = 1, 2, \ldots$ was performed (Lemma 8.3 of [13]).

(2) If $\omega(d)$ is "small", $\omega(d) \leq \left(\frac{\ln d}{\ln\ln d}\right)^{\frac{1}{3}}$, then consider d written in base A: $d = 1 + a_1 A + \ldots + a_k A^k$, $a_i \in \mathbb{Z}$, $0 \leq a_i < A$. The polynomial $g = 1 + a_1 X + \ldots + a_k X^k$ factors in $\mathbb{Z}[X]$ into linear factors: $g = \prod_p (y_p X + 1)$, thus revealing the prime factorization of $d = g(A)$ (Lemmas 8.4 and 8.5 from [13]).

The improvement on the trivial search in method 1 is the subject of this paper. Let

$$\mathcal{D}_z(m) = \{f \in \mathbb{N} : f \mid m \wedge f \leq z\},$$

where $\wedge$ simply stands for *and*. Keeping the notation above, we do not have to search trivially y_p in a set $\{1, 2, \ldots, z\}$, but can find it instead in a set $\mathcal{D}_z(m)$ with $z = \frac{d^{\frac{1}{\omega(d)}}}{A}$ and $m = \frac{\varphi(d)}{A^{\omega(d)}}$. The value of $\varphi(d)$ would have to be known, so that we could compute the prime factors of the quotient $\frac{\varphi(d)}{A^{\omega(d)}}$ (using the prime factorization of its multiple $\varphi(n)$) and list systematically the elements of $\mathcal{D}_z(m)$. We construct in Lemma 5 an obvious injection from $\mathcal{D}_z(m)$ to the set of integers counted by $\psi(z, p_{\omega(m)})$, where $p_1 = 2, p_2 = 3, \ldots$ is the strictly increasing sequence of all prime numbers. This gives $\#\mathcal{D}_z(m) \leq \psi(z, p_{\omega(m)})$. There is a slight subtlety here, as we choose $m = \frac{\varphi(d)}{A^{\omega(d)}}$, not $m = \frac{\varphi(n)}{A^{\omega(d)}}$, in order to get a good upper bound on $\omega(m)$. It should be also observed that the bound $\#\mathcal{D}_z(m) \leq \psi(z, p_{\omega(m)})$ cannot be significantly improved. Take, for instance, $m = p_1 \cdot \cdots \cdot p_l$. Then $\#\mathcal{D}_z(m)$ is just the number of squarefree p_l-smooth positive integers less than or equal to z, usually denoted by $\psi_2(z, p_l)$. We can expect, at least for some range of x and y, that $\psi_2(x, y) \sim \frac{6}{\pi^2}\psi(x, y)$. This asymptotic formula is in fact a theorem of Ivić and Tenenbaum [6] for $x, y \to \infty$, $\ln^{2+\varepsilon} x < y \leq x$ and fixed ε. The constant factor $\frac{6}{\pi^2}$ would vanish in the final complexity of our algorithm.

We refine further the search for p; the key tool is the following result about computing divisors in residue classes (formulated with some change in notation and simplified to our needs), itself based on the LLL basis reduction algorithm [8].

Lemma 4 (Coppersmith, Howgrave-Graham, Nagaraj [3])**.** *Let $d, A, h, u \in \mathbb{N}$ be given, $1 < A < d$, $GCD(A, d) = 1$, $h > u > 0$. Let $\alpha, \gamma \in \mathbb{R}$,*

$$-\varepsilon = u(u+1) + \gamma h(h-1) - 2\alpha u h,$$

such that $0 < \alpha < 1$, $0 < \gamma \leq 1 - \alpha$, $\varepsilon > 0$, $A \geq d^\alpha$. Finally, let

$$d_0 = 1 + \left\lfloor \left(2^{(h-1)/4}\sqrt{h}\right)^{\frac{2h}{\varepsilon}} \right\rfloor.$$

If $d > d_0$, then the divisors d' of d of the form $d' = Ax + 1$, with $1 \leq x \leq d^\gamma$, can be found deterministically in time polynomial in h and $\ln d$, with space complexity $O(h^3 \ln d)$.

It turns out that it is sufficient to find a large enough divisor B of y_p (still among the divisors of $m = \frac{\varphi(d)}{A^{\omega(d)}}$), namely such that $A \cdot B$ exceeds a required

threshold d^α. By taking the smallest such B we reduce the search space to at most $\omega(m) \cdot \#\mathcal{D}_{d^\alpha/A}(m)$ elements (Lemma 7), which is $\#\mathcal{D}_{d^\alpha/A}(m)^{1+o(1)}$ in our setting. At first it may not be obvious how to get this bound, but it accords with the intuition that, in the worst case, m is the product of many small prime numbers. That way we are able to bound from above the time needed to split d by $L\left(d, \frac{1}{3}\right)^{\frac{1}{\sqrt[3]{72}}+o(1)}$ (Lemma 12). However, the direct application of Lemma 4 runs into two technical difficulties. In order to have a better grip on the function $-\varepsilon$ we assume that $\omega(d)$ is "large", say $\omega(d) \geq a_1 \left(\frac{\ln d}{\ln\ln d}\right)^{\frac{1}{3}}$ for some constant a_1, which makes part of the terms negligible. Still $\omega(d)$ cannot be too large, because then the condition $d > d_0$ would be violated, so we also assume that $\omega(d) \leq a_2 \left(\frac{\ln d}{\ln\ln d}\right)^{\frac{1}{3}}$ for another constant a_2. Furthermore, if $\omega(d)$ does not belong to the interval $\left(a_1 \left(\frac{\ln d}{\ln\ln d}\right)^{\frac{1}{3}}, a_2 \left(\frac{\ln d}{\ln\ln d}\right)^{\frac{1}{3}}\right)$, the method from [13] used to split d can be shown to run in at most $L\left(d, \frac{1}{3}\right)^c$ time, where $c = c(a_1, a_2) \to 0$ when $a_1 \to 0$ and $a_2 \to \infty$ (Lemma 13). The right choice of a_1, a_2 is thus to ensure that $c(a_1, a_2) \leq 72^{-\frac{1}{3}}$.

The rest of section 2 is concerned with minimizing the number of times we actually have to call the abstract algorithm $\mathcal{A}$. In [13] we called $\mathcal{A}(n), \mathcal{A}(\mathcal{A}(n)), \ldots$, until the output of some, say k-th iteration $\mathcal{A}^k(n)$ had an obvious prime factorization (e.g., 1). Here we cancel the largest power of 2 from the input before each iteration. At the i-th stage, $1 \leq i \leq k$, when recovering the prime factorization of $\varphi^{k-i}(n)$ from the complete factorization of $\varphi^{k-i+1}(n)$, we may need to make, say N_i additional calls of algorithm $\mathcal{A}$. In this event we exploit the multiplicativity of φ to achieve $N_i \leq 17$ (Lemma 16), and compensate the positive N_i by a smaller k than expected. Overall we prove that the number of calls $k + N_1 + \cdots + N_k$ does not exceed $\ln_8 n$.

In section 3 we mainly discuss a simple deterministic integer factoring algorithm which combines the method of Coppersmith et al. [3] and Chinese remainder theorem (Theorem 19). It is particularly efficient compared to the Pollard–Strassen method [11, 12], when for some small integer r, a shift $d - r$ of a nontrival divisor d of the input n has a large smooth factor.

2. Proof of Theorem 1

Lemma 5. *Let $m \in \mathbb{N}$ and $z \in \mathbb{R}$ be given, m together with its prime factorization. We can compute all the elements of the set $\mathcal{D}_z(m)$, one at time, deterministically using $O\Big(\psi(z, p_{\omega(m)}) \ln^{C_1} m\Big)$ bit operations for some constant C_1.*

Proof. Let $m = P_1^{e_1} \cdot \cdots \cdot P_l^{e_l}$ be the factorization of m into primes P_i, $P_1 < \cdots < P_l$. The map $P_1^{\alpha_1} \cdot \cdots \cdot P_l^{\alpha_l} \mapsto p_1^{\alpha_1} \cdot \cdots \cdot p_l^{\alpha_l}$ is clearly an injection from $\mathcal{D}_z(m)$ into the set of integers counted by $\psi(z, p_l)$. Hence $\#\mathcal{D}_z(m) \leq \psi(z, p_l)$. The elements of $\mathcal{D}_z(m)$ can be effectively listed using a straightforward recursive procedure. Indeed, let $P_1^{\beta_1}$ be the largest power of P_1 dividing m and less than or equal to z. We have

$$\mathcal{D}_z(m) = \bigcup_{0 \leq j \leq \beta_1} P_1^j \cdot \mathcal{D}_{z/P_1^j}(m/P_1^{e_1}), \tag{1}$$

where $f \cdot \mathcal{D}$ denotes the set of elements of the form $f \cdot d$, $d \in \mathcal{D}$. The complexity bound follows. It is important to note that the whole set $\mathcal{D}_z(m)$ does not have to be stored in memory. We only keep track, at each given time, of the sequence of exponents $(j_1, \ldots, j_l)$ in the prime factorization $P_1^{j_1} \cdot \cdots \cdot P_l^{j_l}$ of an element of $\mathcal{D}_z(m)$.

Moving from one sequence to another is done according to the lexicographical order and formula (1). □

Lemma 6. *Suppose we are given real sequences $(v_k), (w_k)$ such that $\lim v_k = \lim w_k = \infty$, $v_k^2 = o(w_k)$. Define $\delta_k = [v_k] + \frac{1}{2}$, $h_k = [\delta_k \omega(k)]$. Finally, let $A', d \in \mathbb{N}$ be given such that $A' \geq d^{\frac{1}{\omega(d)} - \frac{1-\delta_d^{-1}}{\omega(d)^2}}$, $GCD(A', d) = 1$, $\omega(d) \geq w_d$, $d > 1 + \left[\left(2^{(h_d-1)/4}\sqrt{h_d}\right)^{16h_d}\right]$. Then we can find deterministically in time polynomial in $\ln d$ and h_d all the divisors d' of d of the form $d' = A'x + 1$ with $1 \leq x \leq d^{\frac{1-\delta_d^{-1}}{\omega(d)^2}}$. The algorithm has space complexity $O\left(h_d^3 \ln d\right)$.*

Proof. We apply the algorithm from the proof of Lemma 4 with $u = [v_d]$, $h = h_d$, $\alpha = \frac{1}{\omega(d)} - \frac{1-\delta_d^{-1}}{\omega(d)^2}$, $\gamma = \frac{1-\delta_d^{-1}}{\omega(d)^2}$. Of course $\omega(d)$ and thus h_d is not known beforehand, but all possible values can be easily exhausted, as $\omega(d) \leq \ln_2 d$. We evaluate the real $-\varepsilon$ from the aforementioned lemma, dropping the subscript/variable d for simplicity:

$$\begin{aligned}
-\varepsilon &= u(u+1) + \gamma h(h-1) - 2\alpha u h \\
&\leq u^2 + u + \frac{1-\delta^{-1}}{\omega^2}\delta\omega(\delta\omega - 1) - 2\left(\frac{1}{\omega} - \frac{1-\delta^{-1}}{\omega^2}\right)u(\delta\omega - 1) \\
&\leq \left(u^2 + (1-2\delta)u + \delta^2 - \delta\right) \\
&\quad + \left(\frac{\delta^{-1}-1}{\omega}\delta - 2u\left(-\frac{1}{\omega} + \frac{\delta^{-1}-1}{\omega}\delta + \frac{1-\delta^{-1}}{\omega^2}\right)\right).
\end{aligned}$$

The term $u^2 + (1-2\delta)u + \delta^2 - \delta$ turns out to be equal to $-\frac{1}{4}$. The remaining term tends to 0 when $d \to \infty$, and is consequently less than $\frac{1}{8}$ if d exceeds an effective constant (which depends on the growth rates of (v_m) and (w_m)). For such d we get $-\varepsilon < -\frac{1}{8}$. The required condition $d > d_0$ is fulfilled by assumption. □

Lemma 7. *Let $(w_k), (\delta_k), (h_k)$ be given as in Lemma 6. Let also $A, d, m \in \mathbb{N}$ be given, m together with its complete factorization. Suppose that d has a divisor $d' = Ay + 1$ with $y \leq d^{\frac{1}{\omega(d)}}A^{-1}$, $y \mid m$, and that $GCD(Am, d) = 1$, $\omega(d) \geq w_d$, $d > 1 + \left[\left(2^{(h_d-1)/4}\sqrt{h_d}\right)^{16h_d}\right]$. Then d' can be found deterministically in time $O\left(\psi(z, p_{\omega(m)})(h_d \ln(d+m))^{C_2}\right)$, where $z = d^{\frac{1}{\omega(d)} - \frac{1-\delta_d^{-1}}{\omega(d)^2}}A^{-1}$ and C_2 is a constant. The algorithm has space complexity $O\left(h_d^3 \ln d\right)$.*

Proof. We can suppose that $y > z$, in the contrary case, $y \in \mathcal{D}_z(m)$, and the assertion would follow from Lemma 5. Hence

$$t_0 := \min\{t \in \mathbb{N} : t \mid y \wedge t > z\}$$

is properly defined. We further have $t_0 = Pt_0'$ for some prime P dividing m and $t_0' \in \mathcal{D}_z(m)$. It is now clear that we can apply Lemmas 6 and 5 by trying $A' := AQu$ with Q running through the set of prime divisors of m, and u the set $\mathcal{D}_z(m)$. The corresponding algorithm will find d' at least for the choice $Q = P, u = t_0'$. □

Although we will not use the following theorem, we include it for the sake of comparison with Lemma 7.

Theorem 8. *Let $A, d, m, z \in \mathbb{N}$ be given, m together with its factorization $m = P_1^{e_1} \cdot \cdots \cdot P_l^{e_l}$ into primes P_i, $P_1 < \cdots < P_l$. Suppose that d has a divisor $d' = Ax+1$ with $x \mid m$, $x \leq z$, and that $d > AP_l z + 1$. Then a nontrivial factor of d can be found deterministically in $O\left(\psi(\sqrt{z}, p_l) \ln^{C_3}(d+m)\right)$ time for some constant C_3, and using $O(\psi(\sqrt{z}, p_l))$ space.*

Proof. We can assume that $x > \sqrt{z}$, for otherwise $x \in \mathcal{D}_{\sqrt{z}}(m)$ and the conclusion follows from Lemma 5. The set $\{t \in \mathbb{N} : t \mid x \wedge t > \sqrt{z}\}$ is therefore nonempty; let t_0 be its minimal element. Let us write $t_0 = P_i t_0'$ for some i, $1 \leq i \leq l$, and thus $x = P_i t_0' x'$ with $t_0', x' \in \mathcal{D}_{\sqrt{z}}(m)$. For every j, $1 \leq j \leq l$, consider the polynomial

$$W_j = \prod_{u \in \mathcal{D}_{\sqrt{z}}(m)} (AP_j u X + 1) \in \mathbb{Z}_d[X].$$

Using fast arithmetic methods from [12], we compute $W_j(y)$ and then $\mathrm{GCD}(W_j(y), d)$ for all j and $y \in \mathcal{D}_{\sqrt{z}}(m)$. At least one of these greatest common divisors must be larger than 1 (in particular for $j = i$ and $y = x'$), say $\mathrm{GCD}(W_{j_0}(y_0), d) > 1$. Hence also $\mathrm{GCD}(AP_{j_0} u_0 y_0 + 1, d) > 1$ for some $u_0 \in \mathcal{D}_{\sqrt{z}}(m)$. Furthermore, the assumption $d > AP_l z + 1$ ensures that this last GCD is not equal to d. □

Denote by $P_-(d)$ (respectively $P_+(d)$) the smallest (respectively largest) prime divisor of d. For a subset $\mathcal{S}$ of the group $\mathbb{Z}_d^*$ the notation $\langle \mathcal{S} \rangle$ stands for the subgroup generated by $\mathcal{S}$.

Lemma 9. *Let $d \in \mathbb{N}$, c_1, c_2 be positive constants, $\mathcal{B}_d = \left\{2, 3, \ldots, \left\lfloor L\left(d, \frac{1}{3}\right)^{c_1} \right\rfloor\right\} \bmod d$, $p = P_-(d)$, $q = P_+(d)$. Suppose that $p > L\left(d, \frac{1}{3}\right)^{c_1}$, that there is no Fermat–Euclid witness in $\mathcal{B}_d$, and that $\omega(d) \geq c_2 \left(\frac{\ln d}{\ln \ln d}\right)^{\frac{1}{3}}$. Define A as $LCM_{b \in \mathcal{B}_d} ord_d(b)$. Then $A \geq qL\left(d, \frac{1}{3}\right)^{-\frac{1}{3c_1c_2} + o(1)}$.*

Proof. Since $\mathcal{B}_d$ does not contain any Fermat–Euclid witness and $\mathbb{Z}_q^*$ is cyclic, we get

$$\begin{aligned} A = \mathrm{LCM}_{b \in \mathcal{B}_q} \mathrm{ord}_q(b) &= \#\langle \mathcal{B}_q \rangle \\ &\geq \psi\left(q, L\left(q, \frac{1}{3}\right)^{c_1}\right). \end{aligned}$$

By Theorem 3 this gives $A \geq qL\left(q, \frac{2}{3}\right)^{-\frac{2}{3c_1} + o(1)}$, i.e., $A \geq q^{1-\varepsilon}$, where $\varepsilon = \left(\frac{2}{3c_1} + o(1)\right)\left(\frac{\ln \ln q}{\ln q}\right)^{\frac{1}{3}} \xrightarrow[d \to \infty]{} 0$. Moreover, $A = \mathrm{LCM}_{b \in \mathcal{B}_p} \mathrm{ord}_p(b)$. Therefore $A \mid p-1$ and $p > q^{1-\varepsilon}$. Now let us find a function c for which $L\left(q, \frac{1}{2}\right)^c \leq L\left(d, \frac{1}{3}\right)^{c_1}$. We have:

$$L\left(q, \frac{1}{2}\right)^c \leq L\left(p, \frac{1}{2}\right)^{c(1+o(1))} \leq \exp\left(c(1+o(1))\left(\ln d^{\frac{1}{\omega(d)}}\right)^{\frac{1}{2}}\left(\ln \ln d^{\frac{1}{\omega(d)}}\right)^{\frac{1}{2}}\right)$$

with $\ln d^{\frac{1}{\omega(d)}} \leq \frac{1}{c_2}(\ln d)^{\frac{2}{3}}(\ln \ln d)^{\frac{1}{3}}$, $\ln \ln d^{\frac{1}{\omega(d)}} \leq \left(\frac{2}{3} + o(1)\right) \ln \ln d$. Hence

$$L\left(q, \frac{1}{2}\right)^c \leq L\left(d, \frac{1}{3}\right)^{\frac{c\sqrt{2}}{\sqrt{3c_2}}(1+o(1))}. \tag{2}$$

We can thus take c such that $c_1 = \frac{c\sqrt{2}}{\sqrt{3c_2}}(1+o(1))$, i.e., $c = \frac{c_1\sqrt{3c_2}}{\sqrt{2}} + o(1)$. Following the same lines as above, we obtain $A = \#\langle \mathcal{B}_q \rangle \geq \psi\left(q, L\left(q, \frac{1}{2}\right)^c\right)$, so

that $A \geq qL\left(q, \frac{1}{2}\right)^{-\frac{1}{2c}+o(1)}$. Using again inequality (2), we get $L\left(q, \frac{1}{2}\right)^{\frac{1}{2c}+o(1)} \leq L\left(d, \frac{1}{3}\right)^{\frac{1}{c\sqrt{6c_2}}+o(1)}$. We plug the chosen value of c to prove the desired result. □

Lemma 10. *Let $d \in \mathbb{N}$ and $\varphi(d)$ be given, $\varphi(d)$ in completely factorized form. Let c_1, a_1, a_2 be positive constants, $\mathcal{B}_d = \left\{2, 3, \ldots, \left[L\left(d, \frac{1}{3}\right)^{c_1}\right]\right\} \mod d$, $p = P_-(d)$. Assume that $GCD(\varphi(d), d) = 1$, $p > L\left(d, \frac{1}{3}\right)^{c_1}$, $\mathcal{B}_d$ contains no Fermat–Euclid witness, and that $\omega(d) = c_2\left(\frac{\ln d}{\ln\ln d}\right)^{\frac{1}{3}}$ with $a_1 \leq c_2 \leq a_2$. Then p can be found deterministically in at most $L\left(d, \frac{1}{3}\right)^{\max\left(c_1, \frac{1}{6c_1c_2}-\frac{1}{2c_2^2}\right)+o(1)}$ time, using $O(\ln^2 d)$ space.*

Proof. We compute $A := \mathrm{LCM}_{b\in\mathcal{B}_d}\mathrm{ord}_d(b)$ and apply Lemma 7 with $m = \frac{\varphi(d)}{A^{\omega(d)}}$, $d' = p$. The sequence (h_k) can be chosen so that $d > 1 + \left[\left(2^{(h_d-1)/4}\sqrt{h_d}\right)^{16h_d}\right]$ for sufficiently large d, and to fit the complexity requirement: $\delta_k = \left[(\ln\ln k)^{\frac{1}{3}}\right] + \frac{1}{2}$ will do. First we bound $p_{\omega(m)}$ and z from above. By the Chinese remainder theorem, the group $\mathbb{Z}_d^*$ is isomorphic to the product of $\omega(d)$ cyclic groups (assuming $p \neq 2$). It follows that for every prime s dividing $\#\langle\mathcal{B}_d\rangle$ the Sylow s-subgroup of $\langle\mathcal{B}_d\rangle$ is the internal direct product of at most $\omega(d)$ cyclic subgroups whose order is a power of s. Consequently, $A^{\omega(d)} \geq \#\langle\mathcal{B}_d\rangle$. Using Theorem 3, we thus obtain

$$A^{\omega(d)} \geq \psi\left(d, L\left(d, \frac{1}{3}\right)^{c_1}\right) \geq dL\left(d, \frac{2}{3}\right)^{-\frac{2}{3c_1}+o(1)}.$$

Since

$$\omega(m) \leq \ln_2\left(\frac{d}{A^{\omega(d)}}\right) \leq c_3(\ln d)^{\frac{2}{3}}(\ln\ln d)^{\frac{1}{3}},$$

we get (by Chebyshev's theorem)

$$p_{\omega(m)} \leq c_4\omega(m)\ln\omega(m) \leq c_5(\ln d)^{\frac{2}{3}}(\ln\ln d)^{\frac{4}{3}},$$

where c_3, c_4, c_5 are some positive constants. Lemma 9 yields

$$A \geq d^{\frac{1}{\omega(d)}}L\left(d, \frac{1}{3}\right)^{-\frac{1}{3c_1c_2}+o(1)}.$$

Noting that $d^{\frac{1}{\omega(d)^2}} = L\left(d, \frac{1}{3}\right)^{\frac{1}{c_2^2}}$, we thus have

$$z = d^{\frac{1}{\omega(d)}-\frac{1+o(1)}{\omega(d)^2}}A^{-1} \leq L\left(d, \frac{1}{3}\right)^{\frac{1}{3c_1c_2}-\frac{1}{c_2^2}+o(1)}. \tag{3}$$

These upper bounds give the inequality

$$\psi\left(z, p_{\omega(m)}\right) \leq \psi\left(L\left(d, \frac{1}{3}\right)^{\frac{1}{3c_1c_2}-\frac{1}{c_2^2}+o(1)}, c_5(\ln d)^{\frac{2}{3}}(\ln\ln d)^{\frac{4}{3}}\right)$$

We appeal to Theorem 3 to evaluate the last expression. In this case $u = \left(\frac{3}{2}+o(1)\right)\left(\frac{1}{3c_1c_2}-\frac{1}{c_2^2}+o(1)\right)\left(\frac{\ln d}{\ln\ln d}\right)^{\frac{1}{3}}$ and $\ln u = \left(\frac{1}{3}+o(1)\right)\ln\ln d$. The aforementioned expression therefore equals $L\left(d, \frac{1}{3}\right)^{\frac{1}{3c_1c_2}-\frac{1}{c_2^2}+o(1)}u^{-u(1+o(1))}$ which is easily seen to be $L\left(d, \frac{1}{3}\right)^{\frac{1}{6c_1c_2}-\frac{1}{2c_2^2}+o(1)}$. □

Lemma 11. *Let $d \in \mathbb{N}$, $p = P_-(d)$, c_1 and c_2 be positive constants, $\mathcal{B}_d = \left\{2, 3, \ldots, \left[L\left(d, \frac{1}{3}\right)^{c_1}\right]\right\} \bmod d$, $A = LCM_{b \in \mathcal{B}_d} ord_d(b)$. Suppose that $\frac{c_1}{c_2} > \frac{2}{3}$, $\omega(d) \leq c_2 \left(\frac{\ln d}{\ln\ln d}\right)^{\frac{1}{3}}$, $p > L\left(d, \frac{1}{3}\right)^{c_1}$, and that there is no Fermat–Euclid witness in $\mathcal{B}_d$. Then $A^{\omega(d)+1} > d \cdot 2^{\omega(d)}$ for d larger than some effective constant $C = C(c_1, c_2)$.*

Proof. As it was shown in the proof of Lemma 10, $A^{\omega(d)} \geq dL\left(d, \frac{2}{3}\right)^{-\frac{2}{3c_1}(1+o(1))}$. Hence, assuming that d is sufficiently large,

$$\begin{aligned} A^{\omega(d)+1} &\geq d \cdot d^{\frac{1}{\omega(d)}} L\left(d, \frac{2}{3}\right)^{-\frac{2(\omega(d)+1)}{3c_1\omega(d)}(1+o(1))} \\ &\geq d \cdot L\left(d, \frac{2}{3}\right)^{\frac{1}{c_2}+\frac{\omega(d)+1}{c_1\omega(d)}\left(-\frac{2}{3}-\frac{\eta}{3}\right)}, \end{aligned} \tag{4}$$

where $\eta = \frac{c_1}{c_2} - \frac{2}{3}$. Two cases are to be considered. If $\frac{\omega(d)+1}{\omega(d)}\left(-\frac{2}{3} - \frac{\eta}{3}\right) \leq -\frac{2}{3} - \frac{2\eta}{3}$, then $\omega(d)$ is bounded from above; by looking at the first inequality in (4) we see that the assertion holds. Suppose on the contrary that $\frac{\omega(d)+1}{\omega(d)}\left(-\frac{2}{3} - \frac{\eta}{3}\right) > -\frac{2}{3} - \frac{2\eta}{3}$. Then $A^{\omega(d)+1} \geq d \cdot L\left(d, \frac{2}{3}\right)^{\frac{1}{c_2}+\frac{1}{c_1}\left(-\frac{2}{3}-\frac{2\eta}{3}\right)}$. Since the exponent $\frac{1}{c_2} + \frac{1}{c_1}\left(-\frac{2}{3} - \frac{2\eta}{3}\right)$ is positive by assumption, the second factor of the right-hand side for large d exceeds $\exp\left(c_2\left(\frac{\ln d}{\ln\ln d}\right)^{\frac{1}{3}} \ln 2\right)$ and thus also $2^{\omega(d)}$. □

Lemma 12. *Let a positive, composite integer d, and the prime factorization of $\varphi(d)$ be given. Let a_1, a_2 be positive constants. Assume that $a_1\left(\frac{\ln d}{\ln\ln d}\right)^{\frac{1}{3}} \leq \omega(d) \leq a_2\left(\frac{\ln d}{\ln\ln d}\right)^{\frac{1}{3}}$. Then a nontrivial factor of d can be computed deterministically in at most $L\left(d, \frac{1}{3}\right)^{\frac{1}{\sqrt[3]{72}}+o(1)}$ time with space complexity $O(\ln^2 d)$.*

Proof. By Lemma 10 the task can be done in at most $L\left(d, \frac{1}{3}\right)^{\max\left(c_1, \frac{1}{6c_1c_2} - \frac{1}{2c_2^2}\right)+o(1)}$ time for positive, constant c_1 and $\omega(d) = c_2\left(\frac{\ln d}{\ln\ln d}\right)^{\frac{1}{3}}$. Consider c_1 as a parameter and put $f(c_2) = \frac{1}{6c_1c_2} - \frac{1}{2c_2^2}$. We easily check that the function f attains its maximum when $c_2 = 6c_1$. Consequently, the minimum of $\max(c_1, f(c_2))$ is reached for $c_1 = f(6c_1) = \frac{1}{72c_1^2}$ i.e., $c_1 = 72^{-\frac{1}{3}}$. □

Lemma 13. *Let a_1, a_2 be positive constants and $n \in \mathbb{N}$. Let a composite divisor d of n be given and let $\varphi(n)$ together with its complete factorization be known. Assume that $\omega(d) \leq a_1\left(\frac{\ln d}{\ln\ln d}\right)^{\frac{1}{3}}$ or $\omega(d) \geq a_2\left(\frac{\ln d}{\ln\ln d}\right)^{\frac{1}{3}}$. Then we can find a nontrivial factor of d deterministically in at most $\max\left(L\left(d, \frac{1}{3}\right)^{c+o(1)}, \ln^{C_4} n\right)$ time, where $c = \max\left(\frac{3a_1}{4}, \frac{1}{\sqrt{3a_2}}\right)$ and C_4 is a constant.*

Proof. Write $\omega(d) = c_2\left(\frac{\ln d}{\ln\ln d}\right)^{\frac{1}{3}}$ and consider two cases. If $c_2 \leq a_1$, the desired time bound is obtained by taking $c_1 = \frac{3a_1}{4}$ in Lemma 11 and using Lemma 8.5. from [13]. For $c_2 \geq a_2$ it is sufficient to appeal to Lemma 9 and note that $\min\left\{\max\left(c_1, \frac{1}{3c_1c_2}\right) : c_1 > 0, c_2 \geq a_2\right\} = \frac{1}{\sqrt{3a_2}}$. □

Lemma 14. *Let a positive, composite integer n be given, as well as $\varphi(n)$ in completely factorized form. Then a nontrivial factor of n can be computed deterministically in at most $L\left(n, \frac{1}{3}\right)^{\frac{1}{\sqrt[3]{72}}+o(1)}$ time with space complexity $O(\ln^2 n)$.*

Proof. The result follows from Lemmas 12 and 13 with $d = n$ and a_1, a_2 satisfying $\frac{3a_1}{4} = \frac{1}{\sqrt{3a_2}} = \frac{1}{\sqrt[3]{72}}$. That gives $a_1 = 2 \cdot 3^{-\frac{5}{3}}$, $a_2 = 4 \cdot 3^{\frac{1}{3}}$. □

Lemma 15. *Let $n \in \mathbb{N}$. Assume that $\varphi(n)$ is known and completely factored. Then the prime factorization of any given divisor d of n can be found deterministically in at most $\max\left(L\left(d, \frac{1}{3}\right)^{\frac{1}{\sqrt[3]{4}}+o(1)}, \ln^{C_5} n\right)$ time for some constant C_5.*

Proof. Choose $a_1 = a_2$ in Lemma 13, which we use recursively. It remains to observe that $\min\left\{\max\left(\frac{3a_1}{4}, \frac{1}{\sqrt{3a_1}}\right) : a_1 > 0\right\} = \frac{1}{\sqrt[3]{4}}$. □

Lemma 16. *Let $\mathcal{A}(d)$ be an abstract algorithm which outputs $\varphi(d)$ for input $d \in \mathbb{N}$. Let $n \in \mathbb{N}$ and $\varphi(n)$ be given, $\varphi(n)$ in completely factorized form. Having access to no more than 17 chosen outputs of $\mathcal{A}$ (with inputs less than n), we can compute deterministically the prime factorization of n in at most $L\left(n, \frac{1}{3}\right)^{\frac{1}{\sqrt[3]{72}}+o(1)}$ time with space complexity $O(\ln^2 n)$.*

Proof. Suppose that n is composite, moreover that it is squarefree; for if the square of a prime p divides n, then p also divides $\varphi(n)$, so the appropriate factors (of the form p^α in n and $p^{\alpha-1}(p-1)$ in $\varphi(n)$) could be easily removed. By Lemma 14 we can split n nontrivially in the asserted time. We proceed further by recursion. Let us assume that for some composite d dividing n, a nontrivial factorization $d = d_1 d_2$, $d_1 < d_2$, has been found and that the complete factorization of $\varphi(d)$ is known. Consider first the case $d_1 \le n^{\frac{1}{18}}$. Then according to Lemma 15, we can completely factor d_1 in at most $L\left(n, \frac{1}{3}\right)^{\frac{1}{\sqrt[3]{72}}+o(1)}$ time, hence compute—without algorithm $\mathcal{A}$—the value of $\varphi(d_1)$. This in turn allows us to find the prime factorization of $\varphi(d_2)$ as of the quotient $\frac{\varphi(d)}{\varphi(d_1)}$ and apply Lemma 14 to d_2. Now assume that the other, pessimistic case $d_1 > n^{\frac{1}{18}}$ holds. Obviously this scenario can occur at most 17 times. We then call $\mathcal{A}(d_1)$. Next, we easily obtain the complete factorizations of $\varphi(d_1)$ and $\varphi(d_2)$ from the prime factorization of their product $\varphi(d)$. Finally, we apply Lemma 14 to both d_1, d_2. □

Lemma 17. *Let $n \in \mathbb{N}$ and $\varphi(n)$ be given, $\varphi(n)$ completely factored. Suppose that $\omega(n) \le 2^{\frac{2}{3}} 3^{-\frac{7}{3}} \left(\frac{\ln n}{\ln\ln n}\right)^{\frac{1}{3}}$. Then the prime factorization of n can be computed deterministically in at most $L\left(n, \frac{1}{3}\right)^{\frac{1}{\sqrt[3]{72}}+o(1)}$ time.*

Proof. We factor n recursively; so assume that a composite divisor d of n has been found and we further want to split d. If $d \le n^{\frac{1}{18}}$, then Lemma 15 can be applied. Otherwise we get $\omega(d) \le \omega(n) < 2 \cdot 3^{-\frac{5}{3}} \left(\frac{\ln d}{\ln\ln d}\right)^{\frac{1}{3}}$. Lemma 13 proves to be sufficient in this case. □

Proof of Theorem 1. We proceed by induction on n. Fix $N \in \mathbb{N}$ such that $\frac{\ln n}{\ln\ln n} \ge 2 \cdot 3^{16}$ whenever $n > N$. The theorem clearly holds for all $n \le N$, since these can be factored by trial division. Take therefore $n > N$, and assume that the assertion is valid for every integer less than n. Let $n = 2^{k_1} n_1$ with $2 \nmid n_1$. Call $\mathcal{A}(n_1)$ and write $\varphi(n_1) = 2^{k_2} n_2$, $2 \nmid n_2$. If $k_2 \le 2$, then $\omega(n_1) \le 2$. It is well known that in

this case factoring n_1 simply reduces to computing $\mathrm{GCD}(n_1, \varphi(n_1))$ and possibly solving a real quadratic equation (see for example [13]). We can thus assume that $k_2 \geq 3$. Use the induction hypothesis to completely factor n_2 within the allotted time. Suppose that $\ln_8 n_2 \leq \ln_8 n - 18$. We then apply Lemma 16 to n. The total number of times algorithm $\mathcal{A}$ is called would not exceed $1 + \ln_8 n_2 + 17$, which is less than or equal to $\ln_8 n$. Finally, suppose that $\ln_8 n_2 > \ln_8 n - 18$. Then a basic calculation yields $\omega(n) \leq 2^{\frac{2}{3}} 3^{-\frac{7}{3}} \left(\frac{\ln n}{\ln \ln n}\right)^{\frac{1}{3}}$, allowing us to apply Lemma 17 to n. Algorithm $\mathcal{A}$ would be called for a total number of times not greater than $1+\ln_8 n_2$, hence less than or equal to $\ln_8 n$. □

Sketch of proof of Theorem 2. As discussed in the introduction, we can assume that the prime factorization of $\varphi(n)$ is already given. If n is composite, a nontrivial factorization $n = d_1 d_2$ will be found using the method attached to Lemma 14. The next step is similar to the proof of Lemma 16. Without loss of generality, d_1 and d_2 are coprime, $d_1 \leq \sqrt{n}$, and if we manage to completely factor d_1, then the procedure can be repeated with d_2 in place of n. This time, also the method for splitting each successively found divisor d of d_1 (starting with $d = d_1$) is chosen according to whether or not $\omega(d)$ belongs to an interval $\left(a_1 \left(\frac{\ln d}{\ln \ln d}\right)^{\frac{1}{3}}, a_2 \left(\frac{\ln d}{\ln \ln d}\right)^{\frac{1}{3}}\right)$. Here a_1 and a_2 are constants from Lemma 13. In the case when $\omega(d)$ lies indeed in the above interval, if we do not find any Fermat–Euclid witness among the elements $2, 3, \ldots, \left[L\left(d, \frac{1}{3}\right)^{c_1}\right] \bmod d$ for some positive constant c_1, then we will try to apply Lemma 6 directly with A' equal to the LCM of their orders in $\mathbb{Z}_d^*$. We will succeed provided that $\frac{1}{3c_1c_2} - \frac{1}{c_2^2} < 0$, i.e., $c_1 > \frac{c_2}{3}$ (see equation (3)) for $\omega(d) = c_2 \left(\frac{\ln d}{\ln \ln d}\right)^{\frac{1}{3}}$. Since $\min\left\{\max\left(\frac{a_2}{3}, \frac{1}{\sqrt{3a_2}}\right) : a_2 > 0\right\} = \frac{1}{\sqrt[3]{9}}$ and $d \leq d_1 \leq \sqrt{n}$, the theorem follows. □

3. Discussion of related results

Theorem 1 can be easily extended to the Carmichael function λ. However, because of the lack of multiplicativity, more values of λ are needed: at most $\ln_2 n$. To limit their number we need a deterministic primality test. Computing and factoring orders of elements is easy in this set-up, so even Fürer's test [5] (see also Fellows-Koblitz test [4]) will do. Apart from that the proof goes the same way. Only in the proof of Lemma 10 it should be noted that $\frac{\lambda(d)}{A} \mid \frac{\varphi(d)}{A^{\omega(d)}}$. Hence $m = \frac{\lambda(d)}{A}$ can be taken there.

Generalization of Theorem 1 to other functions such as the sum of divisors function σ is much more problematic. One of the main obstacles seems to be that we would have to work with ring of integers of varying number fields instead of the fixed ring $\mathbb{Z}$. Unfortunately, the greater the class number, the fewer smooth integers of bounded norm (i.e., elements which can be written as a product of integers with "small" norm).

Perhaps interestingly, the very basic ideas from Lemmas 5 and 7 can be carried over to the ordinary integer factorization problem, where no extra knowledge in the form of an abstract oracle is available. Recall a result analogous to Lemma 6 and best suited for integers with exactly two prime factors.

Theorem 18 (Coppersmith, Howgrave-Graham, Nagaraj [3])**.** *Let $n, r, A' \in \mathbb{N}$ and $\eta \in \mathbb{R}$ be given, $0 < \eta < \frac{3}{4}$. Suppose that $A' > n^{\frac{1}{4}+\eta}$ and $GCD(A', n) = 1$. Then*

all the divisors d of n, satisfying $d \equiv r\ (A')$, can be found deterministically in time polynomial in $\ln n$ and η^{-1}, with space complexity $O\left(\eta^{-\frac{9}{2}} \ln n\right)$, whenever n is larger than some effective constant depending only on η.

The following method exploits the possibility of n having a shifted divisor with a large smooth factor.

Theorem 19. *Let $n \in \mathbb{N}$, $r \in \mathbb{Z}$ and $M, S, \eta \in \mathbb{R}$ be given, $0 < \eta < \frac{3}{4}$, $M \le n^{\frac{1}{4}+\eta}$, $S \le n$. Assume that n has no prime divisor less than or equal to S. Suppose also n is divisible by an integer d such $d - r$ has a S-smooth factor F greater than M. Then d can be found deterministically in $O\left(\frac{n^{\frac{1}{4}+\eta}}{M}\psi(M,S) \cdot S\left(\eta^{-1}\ln n\right)^C\right)$ time with space complexity $O\left(\eta^{-\frac{9}{2}}\ln n + S\right)$ for some constant C, whenever n is larger than some effectively computable integer depending only on η.*

Proof. First we construct all the primes less than or equal to S using Eratosthenes' sieve (which consumes $O(S \ln\ln S)$ arithmetic operations and $O(S)$ space). Then, for every S-smooth integer u, $u \le M$, and each prime Q, $Q \le S$, we compute $T := Qu$ whenever $T > M$. Similarly, as in Lemma 5, the elements u are enumerated here one at time to save space. Let 2^e be the largest power of 2 dividing T. If $\frac{T}{2^e} \le n^{\frac{1}{4}+\eta}$, we define i as the least integer such that $2^{i-e}T > n^{\frac{1}{4}+\eta}$. Otherwise we just put $i = 0$. We now appeal to Theorem 18 with $A' = \frac{T}{2^e} \cdot 2^i$ to try to find via the Chinese remainder theorem all the divisors d' of n which are solutions of the system of congruences

$$\begin{cases} d' \equiv r\ \left(\frac{T}{2^e}\right), \\ d' \equiv r + k \cdot 2^e\ (2^i), \end{cases}$$

where k runs through the set $\{0, 1, \ldots, 2^{i-e} - 1\}$ if $i > e$ or, in the contrary case, $k = 0$. By the familiar argument (cf. the proof of Lemma 7 or Theorem 8), among the integers T computed there is the minimum t_0 of $\{t \in \mathbb{N} : t \mid F \wedge t > M\}$. The whole search will therefore output d (and possibly other divisors of n). Finally, when $i > e$, the minimality of i yields $2^{i-e} \le 2 \cdot \frac{n^{\frac{1}{4}+\eta}}{T} < 2 \cdot \frac{n^{\frac{1}{4}+\eta}}{M}$, thus the algorithm's complexity fits the given time and space bounds. □

As an example, for $M = n^\theta$, $S = \ln^\alpha n$ (θ, α fixed, $0 < \theta \le \frac{1}{4} + \eta$, $\alpha > \theta$) the algorithm needs at most $n^{\frac{1}{4}-\frac{\theta}{\alpha}+\eta-C\frac{\ln\eta}{\ln n}+o_\alpha(1)}$ bit operations by Theorem 3. For a lower bound on the number of shifted primes with a large smooth factor see Theorem 5.2 in the article of Konyagin and Pomerance [7].

It is easy to generalize this approach to more, say k, shifts of d, assuming that each integer $d - r_i$ has a S_i-smooth factor greater than M_i, $\prod_{1\le i\le k} M_i \le n^{\frac{1}{4}+\eta}$. The time complexity would be $O_{b,k}\left(n^{\frac{1}{4}+\eta} \cdot \left(\eta^{-1}\ln n\right)^C \cdot \prod_{1\le i\le k} \frac{\psi(M_i,S_i)S_i}{M_i}\right)$, where $b = \max_{1\le i,j\le k} |r_i - r_j|$, C is the same constant as in Theorem 19 ($C \ge 2$). We would also need $O\left(\eta^{-\frac{9}{2}}\ln n + \max_{1\le i\le k} S_i\right)$ space.

References

[1] E. Bach, G. Miller, and J. Shallit, *Sums of divisors, perfect numbers and factoring*, SIAM J. Comput. **15** (1986), no. 4, 1143–1154, DOI 10.1137/0215083. MR861378

[2] E. R. Canfield, P. Erdős, and C. Pomerance, *On a problem of Oppenheim concerning "factorisatio numerorum"*, J. Number Theory **17** (1983), no. 1, 1–28, DOI 10.1016/0022-314X(83)90002-1. MR712964

[3] D. Coppersmith, N. Howgrave-Graham, and S. V. Nagaraj, *Divisors in residue classes, constructively*, Math. Comp. **77** (2008), no. 261, 531–545, DOI 10.1090/S0025-5718-07-02007-8. MR2353965

[4] M. R. Fellows and N. Koblitz, *Self-witnessing polynomial-time complexity and prime factorization*, Des. Codes Cryptogr. **2** (1992), no. 3, 231–235, DOI 10.1007/BF00141967. MR1181730

[5] M. Fürer, *Deterministic and Las Vegas primality testing algorithms*, Automata, languages and programming (Nafplion, 1985), Lecture Notes in Comput. Sci., vol. 194, Springer, Berlin, 1985, pp. 199–209, DOI 10.1007/BFb0015745. MR819255

[6] A. Ivić and G. Tenenbaum, *Local densities over integers free of large prime factors*, Quart. J. Math. Oxford Ser. (2) **37** (1986), no. 148, 401–417, DOI 10.1093/qmath/37.4.401. MR868616

[7] S. Konyagin and C. Pomerance, *On primes recognizable in deterministic polynomial time*, The mathematics of Paul Erdős, I, Algorithms Combin., vol. 13, Springer, Berlin, 1997, pp. 176–198, DOI 10.1007/978-3-642-60408-9_15. MR1425185

[8] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), no. 4, 515–534, DOI 10.1007/BF01457454. MR682664

[9] D. Long, *Random Equivalence of Factorization and Computation of Orders*, Princeton University, Department of Electrical Engineering and Computer Science, Technical Report 284 (1981).

[10] G. L. Miller, *Riemann's hypothesis and tests for primality*, J. Comput. System Sci. **13** (1976), no. 3, 300–317, DOI 10.1016/S0022-0000(76)80043-8. MR0480295

[11] J. M. Pollard, *Theorems on factorization and primality testing*, Proc. Cambridge Philos. Soc. **76** (1974), 521–528. MR0354514

[12] V. Strassen, *Einige Resultate über Berechnungskomplexität*, Jber. Deutsch. Math.-Verein. **78** (1976/77), no. 1, 1–8. MR0438807

[13] B. Źrałek, *A deterministic version of Pollard's $p-1$ algorithm*, Math. Comp. **79** (2010), no. 269, 513–533, DOI 10.1090/S0025-5718-09-02262-5. MR2552238

Institute of Mathematics, Warsaw University, Banacha 2, 02-097 Warszawa, Poland
Email address: b.zralek@mimuw.edu.pl