Journal of Mathematics Research; Vol. 10, No. 4; August 2018
ISSN 1916-9795 E-ISSN 1916-9809
Published by Canadian Center of Science and Education

Influence of Divisor-ratio to Distribution of Semiprime's Divisor

Xingbo WANG[1]

[1] Department of Mechatronic Engineering, Foshan University, & Guangdong Engineering Center of Information Security for Intelligent Manufacturing System, PRC

Correspondence: Xingbo WANG, Department of Mechatronic Engineering, Foshan University, & Guangdong Engineering Center of Information Security for Intelligent Manufacturing System, PRC.

Received: May 7, 2018 Accepted: May 24, 2018 Online Published: June 4, 2018

doi:10.5539/jmr.v10n4p54 URL: https://doi.org/10.5539/jmr.v10n4p54

Abstract

For a semiprime that consists in two distinct odd prime divisors, this article makes an investigation on the distribution of the small divisor by analyzing the divisor-ratio that is calculated by the big divisor divided by the small one. It proves that, the small divisor must be a divisor of an odd integer lying in an interval that is uniquely determined by the divisor-ratio, and the length of the interval decreases exponentially with the increment of the ratio. Accordingly, a big divisor-ratio means the small divisor can be found in a small interval whereas a small divisor-ratio means it has to find the small divisor in a large interval. The proved theorems and corollaries can provide certain theoretical supports for finding out the small divisor of the semiprime.

Keywords: Semiprime, divisor-ratio, distribution law

1. Introduction

A semiprime is an odd composite number N that has exactly two distinct prime divisors, say p and q, such that $3 \leq p < q$. Factorization of the semiprimes has been an active topic in the world since the RSA challenge was published due to the close relationship between the semiprimes and the RSA numbers, as were introduced books (Surhone, 2011 and 2013). It is believed that, a valid and successful method to factorize a large semiprime rapidly might be a key to open the door of solving the difficult problem of integer factorization. It is known that the GNFS is regarded to be the fastest known general-purpose method to factorize large integers, but the vast amounts of memory that it requires in the computation leaves less chance for an ordinary computer to perform it (Wang Q, 2016). Accordingly, finding an effective approach to factorize a semiprime still remains a research work for researchers all over the world, as stated in (Duta, 2016) and (WANG X,2017 RSA). In fact, there have been many papers to investigate new effective approaches. For example, Silva J (Silva J, 2010) gave an approach to factorize the semiprime of two equal-sized divisors, Wilson K E (Wilson K E, 2011) attempted factoring semiprimes using PG_N^2 prime graph multiagent search, Kloster K (Kloster K, 2011) and Kurzweg U H (Kurzweg U H, 2012) tried to factorize a semiprime n by estimating the Euler's totient $\phi(n)$, Verkhovsky B S (Verkhovsky B S, 2012) attempted to do the factorization of semiprimes based on analysis of a sequence of modular elliptic equations, Grosshans F and his partners (Grosshans F, 2015) imagined to factorize the safe semiprimes with Quantum computer, Khadir (Khadir, 2016) experimented factoring multi-power RSA moduli with primes sharing least or most significant bits, Zhang H (Zhang H, 2013) and Zheng M (Zheng M, 2017) tested respectively factorization with small prime difference. It can see from these literatures that, a better approach is still in need because there has no report to factorize a big semiprime on an ordinary computer except Kurzweg(Kurzweg U H,2018) who factorized a semiprime of 40 decimal digits with the help of MAPLE in April,2018.

In February 2017, WANG X (WANG X, 2017 Genetic) introduced an approach that can exactly locate the divisors of a composite odd number in respectively definite intervals and proposed an algorithm that can factorize composite odd integers. Nevertheless,since the algorithm is still slow in factoring big semiprimes, as stated in (WANG X, 2017 RSA), this article, in order to know clearly the semiprimes and to develop more efficient algorithms to factorize a big semiprime, follows the ideas in (WANG X, 2017 Genetic) and (WANG X, 2017 RSA) to make an investigation on distribution of the semiprime's divisor. By analyzing the divisor-ratio $k = q/p$ of a semiprime $N = pq$ with $3 \leq p < q$, this paper proves several theorems and corollaries to discover p's distribution, as presented in the following sections. Section 2 lists the preliminaries for the later sections; section 3 proves the mathematical foundations.

2. Preliminaries

This section lists the preliminaries that include definitions, symbols and lemmas, which are necessary for later sections.

2.1 Symbols and Notations

In this whole article, a *semiprime* $N = pq$ means p and q are both odd prime numbers and $3 \le p < q$. An *odd interval* $[a, b]$ is a set of consecutive odd numbers that take a as the lower bound and b as the upper bound; for example, $[3, 11] = \{3, 5, 7, 9, 11\}$. Symbol $\lfloor x \rfloor$ is the *floor function*, an integer function of real number x that satisfies $\lfloor x \rfloor \le x < \lfloor x \rfloor + 1$; symbol GCD means the greatest common divisor; symbol T_N means a *valuated binary tree* that is rooted by N and symbol $N_{(k,j)}$ is a node at the j-th position on level k of T_N, as defined in [**?**]; when $m > 0$, $e^b_m = N_{(m+1,2^{m-1}-1)} = 2^m N - 1$ is the *rightmost node on level m in the left branch of* T_N, $e^p_m = 2^m N - p$ and $e^q_m = 2^m N - q$ are respectively the first p's multiple-node and the first q's multiple-node that are left to e^b_m; by default, $e^0_m = e^b_m - 2(\left\lfloor \frac{\sqrt{N}+1}{2} \right\rfloor - 1)$. Symbol $A \triangleq \frac{B}{2}$,which was defined in (WANG X, 2018 Integer Function), means A is half of B.

2.2 Lemmas

Lemma 1 (See in (FU D,2017)) *An odd interval* $[a, b]$ *contains* $\frac{b-a}{2} + 1$ *consecutive odd numbers.*

Lemma 2 (See in (WANG X, 2017 Genetic)) *Let* $N = pq$ *be an odd composite number such that* $2^{\alpha+1} + 1 \le N \le 2^{\alpha+2} - 1$ *, where p, q and* α *are positive integers with* $3 \le p < q$ *and* $\alpha > 2$*; let symbol* e^b_{m+i} *be the rightmost node on level* $m + i$ *in the left branch of* T_N *, symbols* e^p_{m+i} *and* e^q_{m+i} *be respectively the first p's-multiple-node and the first q's multiple-node that are left to* e^b_{m+i}*, where* $m = \lfloor \log_2 N \rfloor - 1$ *and* $i = 0, 1, ...$*; let odd interval* $[e^n_{m+i}, e^b_{m+i}]$ *contains n consecutive odd numbers; then the following statements hold.*
(1). $e^n_{m+i} = e^b_{m+i} - 2(n - 1)$*;*
(2). e^p_{m+i} *lies in odd interval* $[e^0_{m+i}, e^b_{m+i}]$ *and there are* $\frac{p+1}{2}$ *nodes from* e^p_{m+i} *to* e^b_{m+i}*, where* $e^0_{m+i} = e^b_{m+i} - 2(\left\lfloor \frac{\sqrt{N}+1}{2} \right\rfloor - 1)$ *from which to* e^b_{m+i} *there are* $\left\lfloor \frac{\sqrt{N}+1}{2} \right\rfloor$ *nodes, as illustrated in figure 1.*

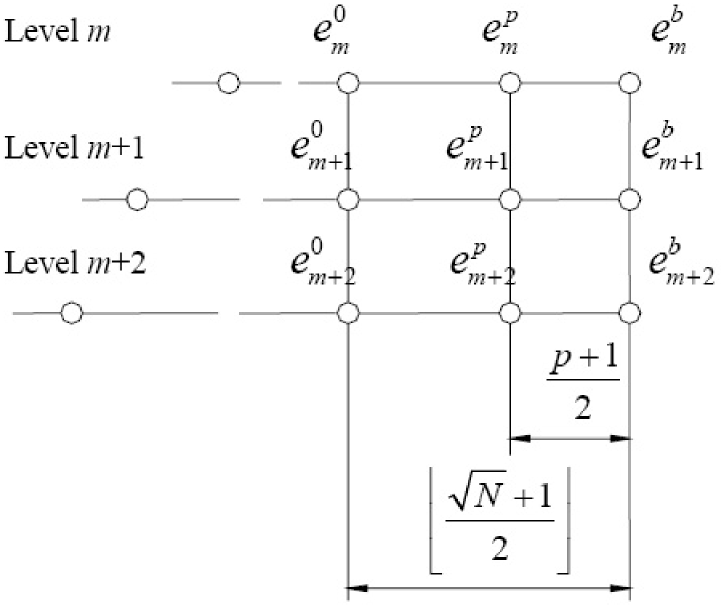

Figure 1. Locations of p's multiple-nodes ($m > 4$)

Lemma 3 (See in (WANG X, 2017 Bound and 2018 Integer Function)) *Let* θ *be a positive real number and* $\Theta(x) = \frac{1}{2}\sqrt{\frac{1}{x}} - \frac{\theta+1}{2}\sqrt{\frac{1}{x+1}} + \frac{\theta}{2}\sqrt{\frac{1}{x+2}}$*; then* $0 < \theta \le 1$ *yields* $\Theta(x) > 0$*, and* $\theta > 1$ *plus* $x > \frac{2}{\sqrt[3]{\theta^2}-1}$ *yields* $\Theta(x) < 0$*. Particularly, when* $x \ge 2$ *, it holds*

$$-\frac{512}{(x+2)\sqrt{x+2}} < \frac{1}{\sqrt{x}} - \frac{3}{\sqrt{x+1}} + \frac{2}{\sqrt{x+2}} < -\frac{1}{512x^3}$$

Lemma 4 (See in (WANG X, 2018 Integer Function)) *Let a be a given positive constant real number and x be a variable on* $(0, \infty)$*. Define* $d(x)$ *and its first order difference* Δ_x *by*

$$d(x) = \left\lfloor \frac{1}{2}(1 + \sqrt{\frac{a}{x}}) \right\rfloor$$

and

$$\Delta_x = d(x) - d(x+1) = \left\lfloor \frac{1}{2}(1 + \sqrt{\frac{a}{x}}) \right\rfloor - \left\lfloor \frac{1}{2}(1 + \sqrt{\frac{a}{x+1}}) \right\rfloor$$

then
(1) It is always holds

$$\left\lfloor \frac{\sqrt{a}}{2((x+1)\sqrt{x} + x\sqrt{x+1})} \right\rfloor \le \Delta_x \le \left\lfloor \frac{\sqrt{a}}{2((x+1)\sqrt{x} + x\sqrt{x+1})} \right\rfloor + 1$$

(2) For a given positive real number ω*, it holds*

$$\Delta_x - \omega\Delta_{x+1} \ge \left\lfloor \frac{1}{2}\sqrt{\frac{a}{x}} - \frac{\omega+1}{2}\sqrt{\frac{a}{x+1}} + \frac{\omega}{2}\sqrt{\frac{a}{x+2}} \right\rfloor$$
$$+ 2\{\omega\}(\left\lfloor \frac{1}{2}\sqrt{\frac{a}{x+1}} - \frac{1}{2}\sqrt{\frac{a}{x+2}} \right\rfloor - \omega - 1$$

and

$$\Delta_x - \omega\Delta_{x+1} \le \left\lfloor \frac{1}{2}\sqrt{\frac{a}{x}} - \frac{\omega+1}{2}\sqrt{\frac{a}{x+1}} + \frac{\omega}{2}\sqrt{\frac{a}{x+2}} \right\rfloor + \omega + 2$$

Furthermore, for given real numbers α*and* β *with* $0 \le \alpha < 1$ *and* $\beta > 1$*, there always exists an* x_0 *such that, when* $x > x_0$ *it holds*

$$\alpha\Delta_{x+1} < \Delta_x < \beta\Delta_{x+1}$$

Lemma 5 (See in (WANG X, 2018 Integer Function)) *Suppose* k_1 *and* k_2 *are positive integers with* $k_1 < k_2$*, a is real with* $a > \max(k_1 + 1, k_2 + 1)$ *and b is a constant real number; let* $s_1 = \left\lfloor \frac{1}{2}(1 + \sqrt{\frac{a}{k_1+1}}) \right\rfloor + 1$*,* $s_2 = \left\lfloor \frac{1}{2}(1 + \sqrt{\frac{a}{k_2+1}}) \right\rfloor + 1$*,* $b_1 = \left\lfloor \frac{1}{2}(1 + \sqrt{\frac{a}{k_1}}) \right\rfloor$ *and* $b_2 = \left\lfloor \frac{1}{2}(1 + \sqrt{\frac{a}{k_2}}) \right\rfloor$*; then it holds*

$$l_1 < r_1 = l_2 < r_2$$

where $l_1 = b - 2(b_1 - 1)$*,* $l_2 = b - 2(b_2 - 1)$*,* $r_1 = b - 2(s_1 - 1)$ *and* $r_2 = b - 2(s_2 - 1)$*.* **Lemma 6** (See in (WANG X, 2018 Integer Function)) *For real number* $a > 0$*, let* $\Delta_0 = \left\lfloor \frac{\sqrt{a}+1}{2} \right\rfloor$*,* $\Delta_1 = \left\lfloor \frac{\sqrt{a}}{4+2\sqrt{2}} \right\rfloor$*,* $\Delta_2 = \left\lfloor \frac{\sqrt{a}}{2(2\sqrt{3}+3\sqrt{2})} \right\rfloor$ *and* $\Delta_3 = \left\lfloor \frac{\sqrt{a}}{2(4\sqrt{3}+3\sqrt{4})} \right\rfloor$*; then* $\Delta_0 \ge 26$ *yields* $\Delta_1 + \Delta_2 > \frac{1}{4}\Delta_0$ *and it always holds* $\Delta_1 + \Delta_2 + \Delta_3 \overset{\Delta}{=} \frac{1}{2}\Delta_0$*.*

3. Main Results and Proofs

Theorem 1 *Suppose* $N = pq$ *is an odd composite number such that* $3 \le p < q$ *and* $kp \le q < (k+1)p$ *for some positive integer k; then p can be found in interval* $[e_m^{kl}, e_m^{kr}]$ *whose length is at most* $1 + \left\lfloor \frac{\sqrt{N}}{2((k+1)\sqrt{k}+k\sqrt{k+1})} \right\rfloor$*, where* $e_m^{kl} = e_m^b - 2(\left\lfloor \frac{1}{2}(1 + \sqrt{\frac{N}{k}}) \right\rfloor - 1)$*,* $e_m^{kr} = e_m^b - 2\left\lfloor \frac{1}{2}(1 + \sqrt{\frac{N}{k+1}}) \right\rfloor$ *and* $e_m^b = 2^m N - 1$*.*

Proof The inequality $kp \le q < (k+1)p$ yields $kp^2 \le N = pq < (k+1)p^2$; namely,

$$\sqrt{\frac{N}{k+1}} < p \le \sqrt{\frac{N}{k}} \tag{1}$$

That is

$$\frac{1}{2}(1 + \sqrt{\frac{N}{k+1}}) < \frac{p+1}{2} \le \frac{1}{2}(1 + \sqrt{\frac{N}{k}}) \tag{2}$$

Referring to the definition of the floor function and its property (**P**13) in (WANG X, 2017 Floor Function), it yields

$$\left\lfloor \frac{1}{2}(1 + \sqrt{\frac{N}{k+1}}) \right\rfloor < \frac{p+1}{2} \le \left\lfloor \frac{1}{2}(1 + \sqrt{\frac{N}{k}}) \right\rfloor$$

namely

$$\left\lfloor \frac{1}{2}(1+\sqrt{\frac{N}{k+1}}) \right\rfloor + 1 \le \frac{p+1}{2} \le \left\lfloor \frac{1}{2}(1+\sqrt{\frac{N}{k}}) \right\rfloor \tag{3}$$

Let $ls = \left\lfloor \frac{1}{2}(1+\sqrt{\frac{N}{k+1}}) \right\rfloor + 1$ and $lb = \left\lfloor \frac{1}{2}(1+\sqrt{\frac{N}{k}}) \right\rfloor$; then (3) is rewritten by

$$ls \le \frac{p+1}{2} \le lb \tag{4}$$

Consider the level m of T_N with $m > 2$. Let $e_m^{kl} = e_m^b - 2(lb-1) = e_m^b - 2(\left\lfloor \frac{1}{2}(1+\sqrt{\frac{N}{k}}) \right\rfloor - 1)$ and $e_m^{kr} = e_m^b - 2(ls-1) = e_m^b - 2\left\lfloor \frac{1}{2}(1+\sqrt{\frac{N}{k+1}}) \right\rfloor$; then by Lemma 2 it knows e_m^p, which has a common divisor p with N, is in the odd interval $[e_m^{kl}, e_m^{kr}]$, as shown in figure 2. Let

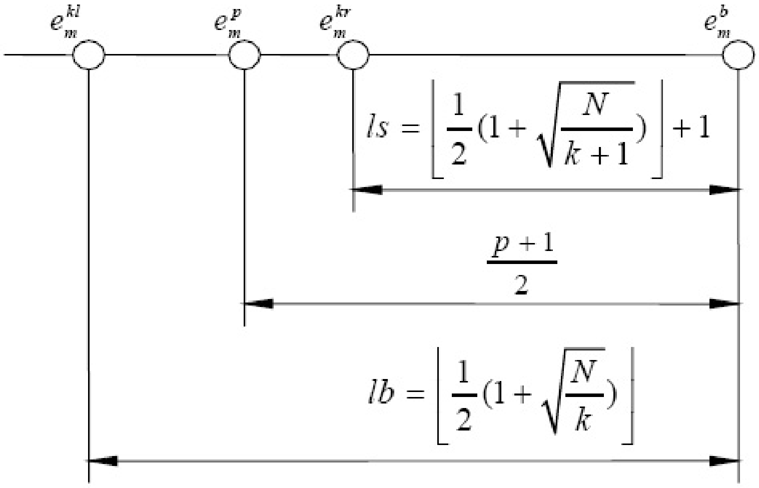
e_m^{kl}
e_m^p
e_m^{kr}
e_m^b
$ls = \left\lfloor \frac{1}{2}(1+\sqrt{\frac{N}{k+1}}) \right\rfloor + 1$
$\frac{p+1}{2}$
$lb = \left\lfloor \frac{1}{2}(1+\sqrt{\frac{N}{k}}) \right\rfloor$

Figure 2. Locations of $e_m^p (m > 2)$

$$\Delta_k = \frac{e_m^{kr} - e_m^{kl}}{2} + 1 = \left\lfloor \frac{1}{2}(1+\sqrt{\frac{N}{k}}) \right\rfloor - \left\lfloor \frac{1}{2}(1+\sqrt{\frac{N}{k+1}}) \right\rfloor \tag{5}$$

then by Lemma 1, Δ_k is the number of nodes contained in the odd interval $[e_m^{kl}, e_m^{kr}]$. By Lemma 5(1), it knows

$$\left\lfloor \frac{\sqrt{N}}{2((k+1)\sqrt{k} + k\sqrt{k+1})} \right\rfloor \le \Delta_k \le \left\lfloor \frac{\sqrt{N}}{2((k+1)\sqrt{k} + k\sqrt{k+1})} \right\rfloor + 1 \tag{6}$$

□

Corollary 1 *Suppose $N = pq$ is an odd composite number; then N can be factorized in at most $1 + \left\lfloor \frac{\sqrt{N}}{4+2\sqrt{2}} \right\rfloor$ steps of searches.*

Proof $k = 1$ is the smallest value of k in Theorem 1; hence it takes at most $1 + \left\lfloor \frac{\sqrt{N}}{4+2\sqrt{2}} \right\rfloor$ steps of searches to find e_m^p that has a common divisor p with N.

□

Corollary 2 *Suppose $N = pq$ is an odd composite number and $k = \left\lfloor \frac{q}{p} \right\rfloor \ge 1$; then $e_m^p \in [e_m^{kl}, e_m^{kr}]$, where $m = \lfloor \log_2 N \rfloor - 1$, $e_m^{kl} = e_m^b - 2(\left\lfloor \frac{1}{2}(1+\sqrt{\frac{N}{k}}) \right\rfloor - 1)$, $e_m^{kr} = e_m^b - 2\left\lfloor \frac{1}{2}(1+\sqrt{\frac{N}{k+1}}) \right\rfloor$ and $e_m^b = 2^m N - 1$.*

Proof (Omitted)

□

Theorem 2 *Suppose $N > 1$ is an odd integer and $k_1 < k_2$ are positive integers. Let $ls_{k_1} = \left\lfloor \frac{1}{2}(1 + \sqrt{\frac{N}{k_1+1}}) \right\rfloor + 1$, $ls_{k_2} = \left\lfloor \frac{1}{2}(1 + \sqrt{\frac{N}{k_2+1}}) \right\rfloor + 1$, $lb_{k_1} = \left\lfloor \frac{1}{2}(1 + \sqrt{\frac{N}{k_1}}) \right\rfloor$ and $lb_{k_2} = \left\lfloor \frac{1}{2}(1 + \sqrt{\frac{N}{k_2}}) \right\rfloor$; then it holds*

$$e_m^{kl_1} < e_m^{kr_1} \leq e_m^{kl_2} < e_m^{kr_2}$$

where $e_m^{kl_1} = e_m^b - 2(lb_{k_1} - 1)$, $e_m^{kl_2} = e_m^b - 2(lb_{k_2} - 1)$, $e_m^{kr_1} = e_m^b - 2(ls_{k_1} - 1)$ and $e_m^{kr_2} = e_m^b - 2(ls_{k_2} - 1)$.
Particularly, when $k_2 = k_1 + 1$ it holds

$$e_m^{kl_1} < e_m^{kr_1} = e_m^{kl_2} < e_m^{kr_2}$$

Proof Taking $a = N$ in Lemma 6 immediately results in the theorem, which can be illustrated with figure 3. as illustrated in figure 3.

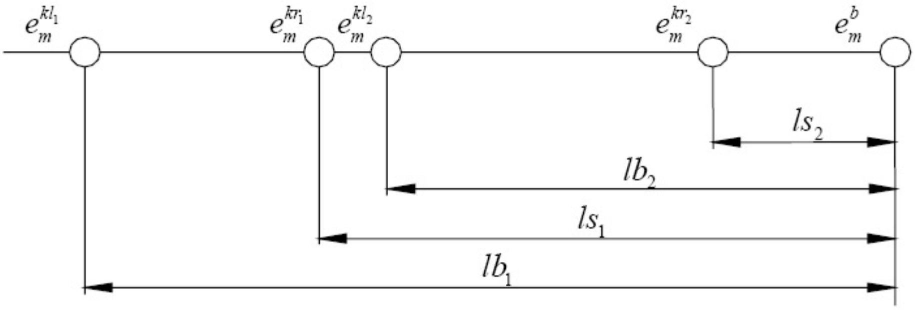

Figure 3. Distribution of $e_m^{kr_2}, e_m^{kr_1}, e_m^{kl_2}$ and $e_m^{kl_1}$

□

Ccorollary 3 *For arbitrary odd number $N > 1$, let $ls_i = \left\lfloor \frac{1}{2}(1 + \sqrt{\frac{N}{i+1}}) \right\rfloor + 1$, $lb_i = \left\lfloor \frac{1}{2}(1 + \sqrt{\frac{N}{i}}) \right\rfloor$,$e_m^{il} = e_m^b - 2(lb_i - 1)$ and $e_m^{ir} = e_m^b - 2(ls_i - 1)$, where $i = 1, 2, ...\omega$ are positive integers; then odd intervals $I_i = [e_m^{il}, e_m^{ir}]$ satisfy*
(1) $I_i \cap I_{i+1} = e_m^{ir}$;
(2) $\bigcup_{i=1}^{i=\omega} I_i = [e_m^0, e_m^{\omega r}]$;
(3) $\bigcup_{i=1}^{i=\infty} I_i = [e_m^0, e_m^b]$; as illustrated in figure 4.

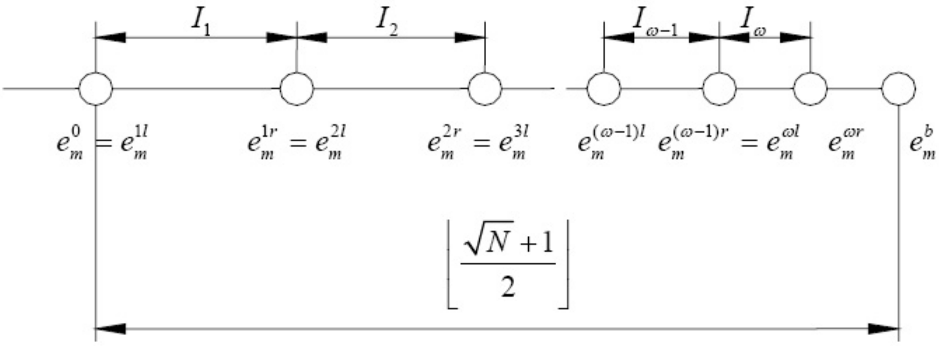

Figure 4. Odd intervals' subdivision and coverage

Proof (Omitted)

□

Corollary 4 *Let* $\Delta_0 = \left\lfloor \frac{\sqrt{N}+1}{2} \right\rfloor$ *be the length of the odd interval* $I_0 = [e_m^0, e_m^b]$, Δ_i *and* Δ_{i+1} *be respectively the lengths of the odd intervals* I_i *and* I_{i+1} *defined in corollaryllary 3; then when* $1 < i \leq \left\lfloor \frac{\sqrt[6]{N}}{16} \right\rfloor$*, it holds* $\frac{1}{2}\Delta_i < \Delta_{i+1} < \Delta_i$*.*

Proof Taking $a = N$, $x = i$, $\alpha = 1$ and $\beta = 2$ in Lemma 4 (2) yields

$$\Delta_i - 2\Delta_{i+1} \leq \left\lfloor \frac{1}{2}\sqrt{\frac{N}{i}} - \frac{3}{2}\sqrt{\frac{N}{i+1}} + \frac{1}{2}\sqrt{\frac{N}{i+2}} \right\rfloor + 4 \tag{7}$$

and

$$\Delta_i - \Delta_{i+1} \geq \left\lfloor \frac{1}{2}\sqrt{\frac{N}{i}} - \sqrt{\frac{N}{i+1}} + \frac{1}{2}\sqrt{\frac{N}{i+2}} \right\rfloor \tag{8}$$

By definition of the floor function, it holds

$$\left\lfloor \frac{1}{2}\sqrt{\frac{N}{i}} - \frac{3}{2}\sqrt{\frac{N}{i+1}} + \frac{1}{2}\sqrt{\frac{N}{i+2}} \right\rfloor \leq \frac{1}{2}\sqrt{\frac{N}{i}} - \frac{3}{2}\sqrt{\frac{N}{i+1}} + \frac{1}{2}\sqrt{\frac{N}{i+2}} \tag{9}$$

By Lemma 3,$\frac{1}{2}\sqrt{\frac{1}{i}} - \frac{3}{2}\sqrt{\frac{1}{i+1}} + \frac{1}{2}\sqrt{\frac{1}{i+2}} < -\frac{1}{1024i^3}$, hence when$-\frac{\sqrt{N}}{1024i^3} + 4 < 0$, namely,$i < \frac{\sqrt[6]{N}}{16}$, it holds$\Delta_i - 2\Delta_{i+1} < 0$. Again by Lemma 3, it always holds $\frac{1}{2}\sqrt{\frac{N}{i}} - \sqrt{\frac{N}{i+1}} + \frac{1}{2}\sqrt{\frac{N}{i+2}} > 0$, hence $i \leq \left\lfloor \frac{\sqrt[6]{N}}{16} \right\rfloor$ yields $\Delta_i - \Delta_{i+1} > 0$.

□

Corollary 5 *Let* $\Delta_0 = \left\lfloor \frac{\sqrt{N}+1}{2} \right\rfloor$ *be the length of the odd interval* $I_0 = [e_m^0, e_m^b]$, Δ_1, Δ_2 *and* Δ_3*, be respectively the lengths of* I_1, I_2 *and* I_3*; then* $\Delta_1 + \Delta_2 + \Delta_3 \triangleq \frac{1}{2}\Delta_0$ *and when* $\Delta_0 \geq 26$ *it holds* $\Delta_1 + \Delta_2 > \frac{1}{4}\Delta_0$*.*

Proof Direct calculation by (5) yields $\Delta_0 = \left\lfloor \frac{\sqrt{a}+1}{2} \right\rfloor$, $\Delta_1 = \left\lfloor \frac{\sqrt{a}}{4+2\sqrt{2}} \right\rfloor$, $\Delta_2 = \left\lfloor \frac{\sqrt{a}}{2(2\sqrt{3}+3\sqrt{2})} \right\rfloor$ and $\Delta_3 = \left\lfloor \frac{\sqrt{a}}{2(4\sqrt{3}+3\sqrt{4})} \right\rfloor$, which is the case of Lemma 6.

□

Corollary 6 *If* $k \geq \left\lfloor \sqrt[3\alpha]{N^\beta} \right\rfloor$ *for some positive integers* $\beta \geq 1$ *and* $\alpha > \beta$*, then* Δ_k *is at most* $\left\lfloor \frac{1}{4}\sqrt[2\alpha]{N^{\alpha-\beta}} \right\rfloor$ *; otherwise it is at least* $\left\lfloor \frac{1}{4}\sqrt[2\alpha]{N^{\alpha-\beta}} \right\rfloor - 1$*. Particularly, arbitrary* $\alpha \geq 2$ *yields* $\Delta_k \leq \left\lfloor \frac{\sqrt[2\alpha]{N}}{4} \right\rfloor$ *for* $k \geq \left\lfloor \sqrt[3\alpha]{N^{\alpha-1}} \right\rfloor$ *and* $\Delta_k \geq \left\lfloor \frac{\sqrt[2\alpha]{N}}{4} \right\rfloor - 1$ *for* $k \leq \left\lfloor \sqrt[3\alpha]{N^{\alpha-1}} \right\rfloor - 1$*.*

Proof Referring to (6) it knows that Δ_k take two possible values given by

$$\Delta_k^b = \left\lfloor \frac{\sqrt{N}}{2((k+1)\sqrt{k} + k\sqrt{k+1})} \right\rfloor + 1$$

and

$$\Delta_k^s = \left\lfloor \frac{\sqrt{N}}{2((k+1)\sqrt{k} + k\sqrt{k+1})} \right\rfloor$$

Then since $2(k+1)\sqrt{k} > 2k\sqrt{k}$ and $2k\sqrt{k+1} > 2k\sqrt{k}$ hold for arbitrary positive number k, it knows

$$\Delta_k^b < \left\lfloor \frac{\sqrt{N}}{4k\sqrt{k}} \right\rfloor + 1 \tag{10}$$

Meanwhile,$2(k+1)\sqrt{k} < 2(k+1)\sqrt{k+1}$ and $2k\sqrt{k+1} < 2(k+1)\sqrt{k+1}$ yields

$$\Delta_k^s > \left\lfloor \frac{\sqrt{N}}{4(k+1)\sqrt{k+1}} \right\rfloor \tag{11}$$

Taking in (10) $k \geq \sqrt[3\alpha]{N^\beta} \geq \left\lfloor \sqrt[3\alpha]{N^\beta} \right\rfloor$ yields $\Delta_k^b < \left\lfloor \frac{\sqrt{N}}{4N^{\frac{3}{2}\times\frac{\beta}{3\alpha}}} \right\rfloor + 1 = \left\lfloor \frac{1}{4}N^{\frac{\alpha-\beta}{2\alpha}} \right\rfloor + 1$, namely,

$$\Delta_k^b \leq \left\lfloor \frac{1}{4}N^{\frac{\alpha-\beta}{2\alpha}} \right\rfloor \tag{12}$$

Taking in (11) $k \leq \left\lfloor \sqrt[3\alpha]{N^\beta} \right\rfloor - 1 \leq \sqrt[3\alpha]{N^\beta} - 1$ leads to $\Delta_k^s > \left\lfloor \frac{\sqrt{N}}{4N^{\frac{3}{2}\times\frac{\beta}{3\alpha}}} \right\rfloor = \left\lfloor \frac{1}{4} N^{\frac{\alpha-\beta}{2\alpha}} \right\rfloor$, namely,

$$\Delta_k^s \geq \left\lfloor \frac{\sqrt{N}}{4N^{\frac{\beta}{2\alpha}}} \right\rfloor - 1 = \left\lfloor \frac{1}{4} N^{\frac{\alpha-\beta}{2\alpha}} \right\rfloor - 1 \tag{13}$$

Obviously, taking $\alpha > 1$ and $\beta = \alpha - 1$ yields $\Delta_k \leq \left\lfloor \frac{\sqrt[2\alpha]{N}}{4} \right\rfloor$ when $k \geq \left\lfloor \sqrt[3\alpha]{N^{\alpha-1}} \right\rfloor$ and $\Delta_k \geq \left\lfloor \frac{\sqrt[2\alpha]{N}}{4} \right\rfloor - 1$ when $k \leq \left\lfloor \sqrt[3\alpha]{N^{\alpha-1}} \right\rfloor - 1$.

□

Corollary 7 *Let $I_1, I_2, ..., I_\omega$ be odd intervals defined in Corollary 3; then there are intervals that contain at most $\left\lfloor \frac{\sqrt[4]{N}}{4} \right\rfloor$ nodes and there are intervals that contain at least $\left\lfloor \frac{\sqrt[4]{N}}{4} \right\rfloor - 1$ nodes.*

Proof This is just the case taking $\alpha = 2$ and $\beta = 1$ in Corollary 3.

□

4. Conclusion and Future Work

Based on the previous lemmas, theorems and corollaries, one can easily draw the following conclusions.

1. If $N = pq$ is a semiprime, then there is a term e_m^p that lies in the odd interval I_0 and satisfies $p = GCD(N, e_m^p)$;

2. If I_0 is subdivided into a series of subintervals that are defined in Corollary 3, then $e_m^p \in I_k$ with $k = \left\lfloor \frac{q}{p} \right\rfloor$, and the bigger k is the fewer nodes are contained in I_k. Among all the subintervals, I_1, I_2 and I_3 dominate half of I_0. Corollary 6 shows that, when $k \leq \left\lfloor \sqrt[3\alpha]{N^\beta} \right\rfloor - 1$ there are at least $\left\lfloor \frac{1}{4} \sqrt[2\alpha]{N^{\alpha-\beta}} \right\rfloor - 1$ nodes in I_k. These provide a guideline for designing new algorithm for integer factorization. We are now working on the work and are sure that new algorithms will soon come into being.

Acknowledgment

The research work is supported by the State Key Laboratory of Mathematical Engineering and Advanced Computing under Open Project Program No.2017A01, Department of Guangdong Science and Technology under project 2015A030401105, Foshan Bureau of Science and Technology under projects 2016AG100311, Project gg040981 from Foshan University. The authors sincerely present thanks to them all.

References

Surhone, L. M., Tennoe, M. T., Henssonow, S. F. (2011). RSA factoring challenge. Springer US.

Surhone, L. M., Tennoe, M. T., Henssonow, S. F. (2013). RSA. Betascript Publishing.

Wang, Q., Fan, X., Zang, H., et al. (2016). The Space Complexity Analysis in the General Number Field Sieve Integer Factorization. *Theoretical Computer Science, 630*(C), 76-94.

Duta, C. L., Gheorghe, L., & Tapus, N. (2016). Framework for evaluation and comparison of integer factorization algorithms. *Sai Computing Conference. IEEE*, 1047-1053.

WANG, X. (2017). Strategy For Algorithm Design in Factoring RSA Numbers. *IOSR Journal of Computer Engineering, 19*(3,ver.2), 1-7. https://doi.org/10.9790/0661-1903020107.

Silva, J. C. L. D. (2010). Factoring semiprimes and possible implications for RSA, The 26-th Convention of Electrical and Electronics Engineers in Israel, Eliat, IEEE, 182-183.

Wilson, K. E. (2011). Factoring Semiprimes Using PG(2N) Prime Graph Multiagent Search. Dissertations & Theses - Gradworks.

Kloster, K. (2011). Factoring a semiprime n by estimating $\phi(n)$. Retrieved from http://www.gregorybard.com /papers/ phi_version _may _7.pdf

Kurzweg, U. H. (2012). More on Factoring Semi-primes. Retrieved from http://www2.mae.ufl.edu/ũhk/MORE-ON-SEMI PRIMES.pdf

Verkhovsky, B. S. (2012). Integer Factorization of Semi-Primes Based on Analysis of a Sequence of Modular Elliptic Equations. *International Journal of Communications Network & System Sciences, 4*(10), 609-615.

Grosshans, F., Lawson, T., Morain, F., et al. (2015). Factoring Safe Semiprimes with a Single Quantum Query. Computer Science, arXiv:1511.04385

Akchiche, K. O. O. (2016). Factoring multi-power RSA moduli with primes sharing least or most significant bits. *Groups Complexity Cryptology, 8*(1), 47-54

Zhang, H., & Takagi, T. (2013). Attacks on Multi-Prime RSA with Small Prime Difference. Australasian Conference on Information Security and Privacy. Springer, Berlin, Heidelberg, 41-56.

Zheng, M., Kunihiro, N., & Hu, H. (2017). Improved Factoring Attacks on Multi-prime RSA with Small Prime Difference. In: Pieprzyk J., Suriadi S. (eds) Information Security and Privacy. ACISP 2017. Lecture Notes in Computer Science, vol 10342. Springer, Cham.

Kurzweg, U. H. (2018). More on Factoring Semi-primes. Retrieved from http://www2.mae. ufl. edu/ uhk/ SEMI- PRIME-FACTORIZATION- VIA-f(N).pdf

WANG, X. (2017). Genetic Traits of Odd Numbers With Applications in Factorization of Integers, *Global Journal of Pure and Applied Mathematics, 13*(1), 318-333.

FU, D. (2017). A Parallel Algorithm for Factorization of Big Odd Numbers, IOSR Journal of Computer Engineering, 19(2, Ver. V), 51-54. https://doi.org/10.9790/0661-1902055154

WANG, X. (2017). Bound Estimation of Two Functions with Proofs of Some New Inequalities. *IOSR Journal of Mathematics, 13*(11), 49-55. https://doi.org/10.9790/5728-1306014955

WANG, X. (2018). Difference Property of An Integer Function. *International Journal of Mathematics Trends and Technology, 55*(3), 236-241.

WANG, X. (2017). Brief Summary of Frequently-Used Properties of the Floor Function. *IOSR Journal of Mathematics, 13*(5), 46-48. https://doi.org/10.9790/5728-1305024648

Copyrights