International Journal of Mathematics and Statistics Studies
Vol.6, No.4, pp.15-32, November 2018
Published by European Centre for Research Training and Development UK (www.eajournals.org)

DIVISORS' DISTRIBUTION OF A RSA MODULUS ON T3 TREE

Xingbo Wang

Department of Mechatronic Engineering, Foshan University, PRC
Guangdong Engineering Centre of Information Security for Intelligent Manufacturing System, PRC
State Key Laboratory of Mathematical Engineering and Advanced Computing, PRC

ABSTRACT: *The article makes an investigation on divisors' distribution of a RSA modulus by means of the T3 tree. Several properties are proved to discover how the divisors distribute on the T3 tree and it is shown that such a distribution is completely determined by the divisor-ratio. Some typical distributions in terms of typical divisor-ratios are investigated in detail mathematical deductions and proofs.*

KEYWORDS: RSA Modulus, Divisor-ratio, T3 Tree

INTRODUCTION

The RSA modulus is a big semiprime composed of two distinct prime divisors, say p and q with $3 \le p < q$ such that $1 < q/p < \sqrt{2}$, according to the American Digital Signature Standard (DSS)(2009). Since the RSA modulus came into being, factorisation of the RSA numbers has been a dream filled with fantasies of researchers and engineers working on information security. Since 2016 when WANG put forward the approach of studying integers on a perfect complete binary tree, as seen in WANG (2016(IJMISR) & 2018(APM)), the T_3 tree approach has aroused a series of studies, as seen WANG's papers list in the bibliography, CHEN (2018) and LI (2018).

The T_3 tree, as a potential tool to study integer, should have known of the RSA modulus. Hence WANG studied the traits of a RSA number on T_3, as seen in WANG (2018-JMR). This paper continues studying the properties of a RSA modulus on the tree and makes clear how the divisors of a RSA modulus are distributed on the tree.

PRELIMINARIES

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

Definitions and Notations

Let S be a set of finite positive integers with s_0 and s_n being the smallest and the biggest nodes respectively; an integer x is said to *be clamped* in S if $s_0 \le x \le s_n$. Symbol $x \triangleq S$ indicates that x is clamped in S. Symbol $\lfloor x \rfloor$ is the floor function, an integer function of real number x that satisfies inequality $x-1 < \lfloor x \rfloor \le x$, or equivalently $\lfloor x \rfloor \le x < \lfloor x \rfloor + 1$. Let $N = pq$ be an odd integer with $1 < p < q$; then $k = \frac{q}{p}$ is called the *divisor-ratio* of *N*.

Print ISSN: 2053-2229, Online ISSN: ISSN 2053-2210

In this whole paper, symbol $\boldsymbol{T}_3$ is the $\boldsymbol{T}_3$ tree that was introduced in WANG (2016 & 2018) and symbol $N_{(k,j)}$ is by default the node at position j on level k of $\boldsymbol{T}_3$, where $k \geq 0$ and $0 \leq j \leq 2^k - 1$. By using the asterisk wildcard *, symbol $N_{(k,*)}$ means a node lying on level k. An integer X is said to *be clamped* on level k of $\boldsymbol{T}_3$ if $2^{k+1} \leq X \leq 2^{k+2} - 1$ and symbol $X \triangleq k$ indicates X is clamped on level k. If a positive integer X is clamped on level k and there is a node Y of $\boldsymbol{T}_3$ satisfying $X = \lfloor \sqrt{Y} \rfloor$, then X is said to be a *floor square root* of the node Y and Y is called a *square source* of X. Symbol $(p \doteq q) = k$ means integers p and q are on the same level k or clamped on the same level k. Symbol $A \otimes B$ means A holds and simultaneously B holds, symbol $A \oplus B$ means A or B holds. Symbol $(a = b) > c$ means a takes the value of b and $a > c$. Symbol $A \Rightarrow B$ means conclusion *B* can be derived from condition *A*.

Lemmas

Lemma 1 (See in WANG (2018, APM)). $\boldsymbol{T}_3$ Tree has the following fundamental properties.

(**P1**). Every node is an odd integer and every odd integer bigger than 1 must be on the $\boldsymbol{T}_3$ tree. Odd integer *N* with $N > 1$ lies on level $\lfloor \log_2 N \rfloor - 1$.

(**P2**). On level *k* with $k = 0,1,\ldots$, there are 2^k nodes starting by $2^{k+1}+1$ and ending by $2^{k+2}-1$, namely, $N_{(k,j)} \in [2^{k+1}+1, 2^{k+2}-1]$ with $j = 0,1,\ldots,2^k - 1$.

(**P3**). $N_{(k,j)}$ is calculated by

$$N_{(k,j)} = 2^{k+1} + 1 + 2j,\ j = 0,1,\ldots,2^k - 1$$

(**P4**) Multiplication of arbitrary two nodes of $\boldsymbol{T}_3$, say $N_{(m,\alpha)}$ and $N_{(n,\beta)}$, is a third node of $\boldsymbol{T}_3$. Let $J = 2^m(1+2\beta) + 2^n(1+2\alpha) + 2\alpha\beta + \alpha + \beta$; the multiplication $N_{(m,\alpha)} \times N_{(n,\beta)}$ is given by

$$N_{(m,\alpha)} \times N_{(n,\beta)} = 2^{m+n+2} + 1 + 2J$$

If $J < 2^{m+n+1}$, then $N_{(m,\alpha)} \times N_{(n,\beta)} = N_{(m+n+1,J)}$ lies on level $m+n+1$ of $\boldsymbol{T}_3$; whereas, if $J \geq 2^{m+n+1}$, $N_{(m,\alpha)} \times N_{(n,\beta)} = N_{(m+n+2,\chi)}$ with $\chi = J - 2^{m+n+1}$ lies on level $m+n+2$ of $\boldsymbol{T}_3$.

(P5) Product $N_{(m,\alpha)} \times N_{(m,\alpha)} = N_{(m,\alpha)}^2$ is a left node of $\boldsymbol{T}_3$, and it lies on level $2m+1$ or $2m+2$

Lemma 2(See WANG (2018,IJMSS)). Let $N > 3$ be an odd integer and $k = \lfloor \log_2 N \rfloor - 1$; then $\lfloor \sqrt{N} \rfloor \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$. Particularly, $\left(\lfloor \sqrt{N} \rfloor \leq \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} \sqrt{2} \right\rfloor\right) \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$ when k is odd, whereas $\left(\left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} \sqrt{2} \right\rfloor \leq \lfloor \sqrt{N} \rfloor\right) \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$ when k is even.

Lemma 3 (See WANG (2018 (no.6), JMR)). Let $N = pq$ be an odd integer with $1 < p < q$ and $1 < \frac{q}{p} < \chi$; then

Print ISSN: 2053-2229, Online ISSN: ISSN 2053-2210

$$\left\lfloor \frac{3-\chi}{2}\sqrt{N} \right\rfloor < p \le \lfloor \sqrt{N} \rfloor \otimes \lfloor \sqrt{N} \rfloor \le q \le \left\lfloor \frac{\chi+1}{2}\sqrt{N} \right\rfloor$$

where $\lfloor x \rfloor = 0$ if $x \le 0$.

Particularly, when $\chi = 2$, it yields

$$\left\lfloor \frac{\sqrt{N}}{2} \right\rfloor < p \le \lfloor \sqrt{N} \rfloor \otimes \lfloor \sqrt{N} \rfloor \le q \le \left\lfloor \frac{3}{2}\sqrt{N} \right\rfloor$$

when $\chi = \frac{3}{2}$, it yields

$$\left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor < p \le \lfloor \sqrt{N} \rfloor \otimes \lfloor \sqrt{N} \rfloor \le q \le \left\lfloor \frac{5}{4}\sqrt{N} \right\rfloor$$

and when $\chi = \sqrt{2}$ it holds

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

Lemma 4 (See in WANG (2017, IOSR-JM)). For real numbers x, y and positive integer i, it holds

(**P13**) $x \le y \Rightarrow \lfloor x \rfloor \le \lfloor y \rfloor$.

(**P14**) $\lfloor n + x \rfloor = n + \lfloor x \rfloor$.

(**P17**) $\lfloor x \rfloor + \left\lfloor x + \frac{1}{2} \right\rfloor = \lfloor 2x \rfloor$ and $\left\lfloor \frac{x}{2} \right\rfloor + \left\lfloor \frac{x+1}{2} \right\rfloor = \lfloor x \rfloor$.

Lemma 5 (See in WANG (2018(no.3), JMR)). Let α and x be a positive real numbers; then it holds

$$\alpha \lfloor x \rfloor - 1 < \lfloor \alpha x \rfloor < \alpha(\lfloor x \rfloor + 1)$$

Particularly, if α is a positive integer, say $\alpha = n$, then it yields

$$n \lfloor x \rfloor \le \lfloor nx \rfloor \le n(\lfloor x \rfloor + 1) - 1$$

MAIN RESULTS AND PROOFS

Proposition 1. Let $N > 16$ be an odd integer and $k = \lfloor \log_2 N \rfloor - 1$; then

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} \le \left\lfloor \frac{\sqrt{N}}{2} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} \quad (1)$$

when *k* is odd., whereas

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} \le \left\lfloor \frac{\sqrt{N}}{2} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} \quad (2)$$

when *k* is even.

Print ISSN: 2053-2229, Online ISSN: ISSN 2053-2210

Proof. Direct calculation yields

$$2^{k+1} < N < 2^{k+2} \Rightarrow 2^{\frac{k+1}{2}} < \sqrt{N} < 2^{\frac{k+2}{2}}$$
$$\Rightarrow 2^{\frac{k+1}{2}-1} < \frac{\sqrt{N}}{2} < 2^{\frac{k+2}{2}-1}$$

By Lemma 4 (P13) it holds

$$\left\lfloor 2^{\frac{k+1}{2}-1} \right\rfloor \le \left\lfloor \frac{\sqrt{N}}{2} \right\rfloor \le \left\lfloor 2^{\frac{k+2}{2}-1} \right\rfloor$$

Let $2^{\frac{k+1}{2}-1} = B$; then $2^{\frac{k+2}{2}-1} = B\sqrt{2}$ and thus

$$\lfloor B \rfloor \le \left\lfloor \frac{\sqrt{N}}{2} \right\rfloor \le \lfloor B\sqrt{2} \rfloor \tag{3}$$

Let $\frac{k+1}{2} - \left\lfloor \frac{k+1}{2} \right\rfloor = \varepsilon$; then $\varepsilon = 0$ when k is odd and $\varepsilon = 0.5$ when k is even. By Lemma 4 (P14), it holds

$$\lfloor B \rfloor - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} = \left\lfloor B - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} \right\rfloor = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} (2^{\varepsilon-1} - 1) \right\rfloor \tag{4}$$

and

$$\lfloor B\sqrt{2} \rfloor - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} = \left\lfloor B\sqrt{2} - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} \right\rfloor = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} (2^{\varepsilon-\frac{1}{2}} - 1) \right\rfloor \tag{5}$$

Now suppose k is even; then (4) becomes

$$\lfloor B \rfloor - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} (2^{0.5-1} - 1) \right\rfloor = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} (\frac{\sqrt{2}}{2} - 1) \right\rfloor \ge \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} (\frac{1}{2} - 1) \right\rfloor = -2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1}$$

and (5) becomes

$$\lfloor B\sqrt{2} \rfloor - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} (2^{\frac{1}{2}-\frac{1}{2}} - 1) \right\rfloor = 0$$

which says an even k yields

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} \le \left\lfloor \frac{\sqrt{N}}{2} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} \tag{6}$$

If k is odd; then (4) becomes

$$\lfloor B \rfloor - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} (2^{0-1} - 1) \right\rfloor = -2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} \tag{7}$$

Print ISSN: 2053-2229, Online ISSN: ISSN 2053-2210

and (5) becomes

$$\left\lfloor B\sqrt{2}\right\rfloor - 2^{\left\lfloor\frac{k+1}{2}\right\rfloor} = \left\lfloor 2^{\left\lfloor\frac{k+1}{2}\right\rfloor}(2^{0-\frac{1}{2}}-1)\right\rfloor = \left\lfloor 2^{\left\lfloor\frac{k+1}{2}\right\rfloor}(\frac{\sqrt{2}}{2}-1)\right\rfloor \le \left\lfloor 2^{\left\lfloor\frac{k+1}{2}\right\rfloor}(\frac{3}{4}-1)\right\rfloor = -2^{\left\lfloor\frac{k+1}{2}\right\rfloor-2} \tag{8}$$

That is, an odd *k* leads to

$$2^{\left\lfloor\frac{k+1}{2}\right\rfloor} - 2^{\left\lfloor\frac{k+1}{2}\right\rfloor-1} \le \left\lfloor\frac{\sqrt{N}}{2}\right\rfloor \le 2^{\left\lfloor\frac{k+1}{2}\right\rfloor} - 2^{\left\lfloor\frac{k+1}{2}\right\rfloor-2} \tag{9}$$

Since $N>16$, it knows that $(k=\lfloor\log_2 N\rfloor-1)>3$ and thus $\left\lfloor\frac{k+1}{2}\right\rfloor-2\ge 0$, ensuring (8) and (9) meaningful.

□

Proposition 2. Let $N>3$ be an odd integer and $k=\lfloor\log_2 N\rfloor-1$; then

$$2^{\left\lfloor\frac{k+1}{2}\right\rfloor} + 2^{\left\lfloor\frac{k+1}{2}\right\rfloor-1} \le \left\lfloor\frac{3\sqrt{N}}{2}\right\rfloor \le 2^{\left\lfloor\frac{k+1}{2}\right\rfloor+1} + 2^{\left\lfloor\frac{k+1}{2}\right\rfloor-1} < 2^{\left\lfloor\frac{k+1}{2}\right\rfloor+2} \tag{10}$$

when *k* is odd, whereas

$$2^{\left\lfloor\frac{k+1}{2}\right\rfloor+1} \le \left\lfloor\frac{3\sqrt{N}}{2}\right\rfloor \le 2^{\left\lfloor\frac{k+1}{2}\right\rfloor+1} + 2^{\left\lfloor\frac{k+1}{2}\right\rfloor} < 2^{\left\lfloor\frac{k+1}{2}\right\rfloor+2} \tag{11}$$

when *k* is even.

Proof. Direct calculation yields

$$\begin{aligned} &2^{k+1}<N<2^{k+2} \Rightarrow 2^{\frac{k+1}{2}} < \sqrt{N} < 2^{\frac{k+2}{2}} \\ &\Rightarrow 2^{\frac{k+1}{2}-1} < \frac{\sqrt{N}}{2} < 2^{\frac{k+2}{2}-1} \\ &\Rightarrow 2^{\frac{k+1}{2}} + 2^{\frac{k+1}{2}-1} < \frac{3\sqrt{N}}{2} < 2^{\frac{k+2}{2}} + 2^{\frac{k+2}{2}-1} \end{aligned}$$

By Lemma 4 (P17), $\left\lfloor\frac{k+2}{2}\right\rfloor = k+1-\left\lfloor\frac{k+1}{2}\right\rfloor$; referring to the proof of Proposition 1,it yields

$$2^{\left\lfloor\frac{k+1}{2}\right\rfloor+\varepsilon} + 2^{\left\lfloor\frac{k+1}{2}\right\rfloor+\varepsilon-1} < \frac{3\sqrt{N}}{2} < 2^{\left\lfloor\frac{k+1}{2}\right\rfloor+\varepsilon+\frac{1}{2}} + 2^{\left\lfloor\frac{k+1}{2}\right\rfloor+\varepsilon-\frac{1}{2}}$$

thus

$$\left\lfloor 2^{\left\lfloor\frac{k+1}{2}\right\rfloor+\varepsilon} + 2^{\left\lfloor\frac{k+1}{2}\right\rfloor+\varepsilon-1}\right\rfloor \le \left\lfloor\frac{3\sqrt{N}}{2}\right\rfloor \le \left\lfloor 2^{\left\lfloor\frac{k+1}{2}\right\rfloor+\varepsilon+\frac{1}{2}} + 2^{\left\lfloor\frac{k+1}{2}\right\rfloor+\varepsilon-\frac{1}{2}}\right\rfloor \tag{12}$$

Consequently, for an odd k, it holds

Print ISSN: 2053-2229, Online ISSN: ISSN 2053-2210

$$2^{\left\lfloor\frac{k+1}{2}\right\rfloor}+2^{\left\lfloor\frac{k+1}{2}\right\rfloor-1}\le\left\lfloor\frac{3\sqrt{N}}{2}\right\rfloor\le\left\lfloor 2^{\left\lfloor\frac{k+1}{2}\right\rfloor}(\sqrt{2}+\frac{1}{\sqrt{2}})\right\rfloor\le\left\lfloor 2^{\left\lfloor\frac{k+1}{2}\right\rfloor}(\frac{3}{2}+1)\right\rfloor=\left\lfloor 2^{\left\lfloor\frac{k+1}{2}\right\rfloor}(2+\frac{1}{2})\right\rfloor=2^{\left\lfloor\frac{k+1}{2}\right\rfloor+1}+2^{\left\lfloor\frac{k+1}{2}\right\rfloor-1}$$

whereas for an even k

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

Since $2^{\left\lfloor\frac{k+1}{2}\right\rfloor+1}+2^{\left\lfloor\frac{k+1}{2}\right\rfloor-1}=2^{\left\lfloor\frac{k+1}{2}\right\rfloor+1}(1+\frac{1}{4})<2^{\left\lfloor\frac{k+1}{2}\right\rfloor+2}$, it holds

$$2^{\left\lfloor\frac{k+1}{2}\right\rfloor}+2^{\left\lfloor\frac{k+1}{2}\right\rfloor-1}\le\left\lfloor\frac{3\sqrt{N}}{2}\right\rfloor\le 2^{\left\lfloor\frac{k+1}{2}\right\rfloor+1}+2^{\left\lfloor\frac{k+1}{2}\right\rfloor-1}<2^{\left\lfloor\frac{k+1}{2}\right\rfloor+2}$$

Since $N>3$, it knows that $(k=\lfloor\log_2 N\rfloor-1)>1$ and thus $\left\lfloor\frac{k+1}{2}\right\rfloor-1\ge 0$ is a valid quantity ensuring (10) and (11) meaningful.

□

Corollary 1. Let $(N=pq)>16$ be an odd integer with $1<\frac{q}{p}<2$ and $k=\lfloor\log_2 N\rfloor-1$; then

$$2^{\left\lfloor\frac{k+1}{2}\right\rfloor}-2^{\left\lfloor\frac{k+1}{2}\right\rfloor-1}+1\le p\le\lfloor\sqrt{N}\rfloor \tag{13}$$

$$\lfloor\sqrt{N}\rfloor\le q\le 2^{\left\lfloor\frac{k+1}{2}\right\rfloor+1}+2^{\left\lfloor\frac{k+1}{2}\right\rfloor-1}-1 \tag{14}$$

if k is odd, whereas

$$\lfloor\sqrt{N}\rfloor\le q\le 2^{\left\lfloor\frac{k+1}{2}\right\rfloor+1}+2^{\left\lfloor\frac{k+1}{2}\right\rfloor}-1 \tag{15}$$

if k is even.

Consequently,

$$p\triangleq\left\lfloor\frac{k+1}{2}\right\rfloor-2\oplus p\triangleq\left\lfloor\frac{k+1}{2}\right\rfloor-1 \tag{16}$$

and

$$q\triangleq\left\lfloor\frac{k+1}{2}\right\rfloor-1\oplus q\triangleq\left\lfloor\frac{k+1}{2}\right\rfloor \tag{17}$$

Proof. By Lemma 2, it always holds $\lfloor\sqrt{N}\rfloor\triangleq\left\lfloor\frac{k+1}{2}\right\rfloor-1$. By Lemma 3, $\left\lfloor\frac{\sqrt{N}}{2}\right\rfloor<p\le\lfloor\sqrt{N}\rfloor$ and $\lfloor\sqrt{N}\rfloor\le q\le\left\lfloor\frac{3\sqrt{N}}{2}\right\rfloor$ when $1<\frac{q}{p}<2$. By Proposition 1, the inequality (13) holds and thus

Print ISSN: 2053-2229, Online ISSN: ISSN 2053-2210

$\left\lfloor \frac{\sqrt{N}}{2} \right\rfloor \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2$, which indicates that $p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2 \oplus p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$ holds. By Proposition 2 it knows the inequalities (14) and (15) hold and $q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1 \oplus q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor$ by referring to (10) and (11).

□

Proposition 3. Let $N > 1024$ be an odd integer and $k = \lfloor \log_2 N \rfloor - 1$; then

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} \le \left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 4} < 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} \tag{18}$$

when k is odd, whereas

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 5} \le \left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} < 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} \tag{19}$$

when k is even.

Proof. Direct calculation yields

$$\begin{aligned} & 2^{k+1} < N < 2^{k+2} \Rightarrow 2^{\frac{k+1}{2}} < \sqrt{N} < 2^{\frac{k+2}{2}} \\ & \Rightarrow 2^{\frac{k+1}{2}-2}(2+1) < \frac{3}{4}\sqrt{N} < 2^{\frac{k+2}{2}-2}(2+1) \\ & \Rightarrow 2^{\frac{k+1}{2}-1} + 2^{\frac{k+1}{2}-2} < \frac{3}{4}\sqrt{N} < 2^{\frac{k+2}{2}-1} + 2^{\frac{k+2}{2}-2} \end{aligned}$$

By Lemma 4 (P13) it holds

$$\left\lfloor 2^{\frac{k+1}{2}-1} + 2^{\frac{k+1}{2}-2} \right\rfloor \le \left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor \le \left\lfloor 2^{\frac{k+2}{2}-1} + 2^{\frac{k+2}{2}-2} \right\rfloor$$

Let $2^{\frac{k+1}{2}-1} + 2^{\frac{k+1}{2}-2} = \Lambda$; then $2^{\frac{k+2}{2}-1} + 2^{\frac{k+2}{2}-2} = \Lambda\sqrt{2}$ and thus

$$\lfloor \Lambda \rfloor \le \left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor \le \lfloor \Lambda\sqrt{2} \rfloor \tag{20}$$

Note that, by Lemma 4 (P14), it holds

$$\lfloor \Lambda \rfloor - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} = \left\lfloor \Lambda - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} \right\rfloor = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}(2^{\varepsilon-1} + 2^{\varepsilon-2} - 1) \right\rfloor \tag{21}$$

and

Print ISSN: 2053-2229, Online ISSN: ISSN 2053-2210

$$\left\lfloor \Lambda\sqrt{2} \right\rfloor - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} = \left\lfloor \Lambda\sqrt{2} - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} \right\rfloor = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}(2^{\varepsilon-\frac{1}{2}} + 2^{\varepsilon-\frac{3}{2}} - 1) \right\rfloor \tag{22}$$

By $\frac{3\sqrt{2}}{4} - 1 > \frac{1}{32}$, it can see by Lemma 5 that, when $k > 0$ is even

$$\lfloor \Lambda \rfloor - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}(2^{0.5-1} + 2^{0.5-2} - 1) \right\rfloor = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}(\frac{1}{\sqrt{2}} + \frac{1}{2\sqrt{2}} - 1) \right\rfloor = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}(\frac{3\sqrt{2}}{4} - 1) \right\rfloor \geq 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 5}$$

and

$$\left\lfloor \Lambda\sqrt{2} \right\rfloor - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}(2^{\frac{1}{2}-\frac{1}{2}} + 2^{\frac{1}{2}-\frac{3}{2}} - 1) \right\rfloor = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}(1 + \frac{1}{2} - 1) \right\rfloor = 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1}$$

Thereby an even *k* yields

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 5} \leq \left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor \leq 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} \tag{23}$$

On the other hand, when $k > 2$ is odd

$$\lfloor \Lambda \rfloor - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}(2^{0-1} + 2^{0-2} - 1) \right\rfloor = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}(\frac{1}{2} + \frac{1}{4} - 1) \right\rfloor = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}(\frac{3}{4} - 1) \right\rfloor = -2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2}$$

and

$$\left\lfloor \Lambda\sqrt{2} \right\rfloor - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}(2^{0-\frac{1}{2}} + 2^{0-\frac{3}{2}} - 1) \right\rfloor = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}(\frac{1}{\sqrt{2}} + \frac{1}{2\sqrt{2}} - 1) \right\rfloor = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}(\frac{3\sqrt{2}}{4} - 1) \right\rfloor$$

Since $\frac{1}{32} < \frac{3\sqrt{2}}{4} - 1 < \frac{1}{16}$, it holds

$$\left\lfloor \Lambda\sqrt{2} \right\rfloor - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} \leq 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 4}$$

Accordingly an odd *k* yields

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} \leq \left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor \leq 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 4} \tag{24}$$

Since $N > 1024$, it knows that $(k = \lfloor \log_2 N \rfloor - 1) > 9$ and thus $\left\lfloor \frac{k+1}{2} \right\rfloor - 5 \geq 0$ is a valid quantity ensuring (23) and (24) meaningful.

□

Proposition 4. Let $N > 16$ be an odd integer and $k = \lfloor \log_2 N \rfloor - 1$; then

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} \leq \left\lfloor \frac{5}{4}\sqrt{N} \right\rfloor \leq 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} \tag{25}$$

Print ISSN: 2053-2229, Online ISSN: ISSN 2053-2210

when k is odd, whereas

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} \le \left\lfloor \frac{5}{4}\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} \tag{26}$$

when k is even.

Proof. Referring to the proof of Proposition 2, direct calculation yields

$$\begin{aligned}
&2^{k+1} < N < 2^{k+2} \Rightarrow 2^{\frac{k+1}{2}} < \sqrt{N} < 2^{\frac{k+2}{2}} \\
&\Rightarrow 2^{\frac{k+1}{2}-2}(4+1) < \frac{5}{4}\sqrt{N} < 2^{\frac{k+2}{2}-2}(4+1) \\
&\Rightarrow 2^{\frac{k+1}{2}} + 2^{\frac{k+1}{2}-2} < \frac{5}{4}\sqrt{N} < 2^{\frac{k+2}{2}} + 2^{\frac{k+2}{2}-2} \\
&\Rightarrow \left\lfloor 2^{\frac{k+1}{2}} + 2^{\frac{k+1}{2}-2} \right\rfloor \le \left\lfloor \frac{5}{4}\sqrt{N} \right\rfloor \le \left\lfloor 2^{\frac{k+2}{2}} + 2^{\frac{k+2}{2}-2} \right\rfloor \\
&\Rightarrow \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + \varepsilon} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + \varepsilon - 2} \right\rfloor \le \left\lfloor \frac{5}{4}\sqrt{N} \right\rfloor \le \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + \varepsilon + \frac{1}{2}} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + \varepsilon - \frac{3}{2}} \right\rfloor
\end{aligned}$$

Hence it holds

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} \le \left\lfloor \frac{5}{4}\sqrt{N} \right\rfloor \le \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}\left(\sqrt{2} + \frac{1}{\sqrt{8}}\right) \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1}$$

when k is odd, whereas

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} \le \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} \times \frac{3}{2} \right\rfloor \le \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}\left(\sqrt{2} + \frac{1}{\sqrt{8}}\right) \right\rfloor = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + \frac{1}{2}} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - \frac{3}{2}} \right\rfloor \le \left\lfloor \frac{5}{4}\sqrt{N} \right\rfloor \le \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} \right\rfloor = 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1}$$

when k is even.

Since $N > 16$, it knows that $(k = \lfloor \log_2 N \rfloor - 1) \ge 3$ and thus $\left\lfloor \frac{k+1}{2} \right\rfloor - 2 \ge 0$ is a valid quantity ensuring (25) and (26) meaningful.

□

Corollary 2. Let $(N = pq) > 1024$ be an odd integer with $1 < \frac{q}{p} < \frac{3}{2}$ and $k = \lfloor \log_2 N \rfloor - 1$; then

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} + 1 \le p \le \left\lfloor \sqrt{N} \right\rfloor \tag{27}$$

$$\left\lfloor \sqrt{N} \right\rfloor \le q \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} - 1 \tag{28}$$

if k is odd, whereas

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 5} + 1 \le p \le \left\lfloor \sqrt{N} \right\rfloor \tag{29}$$

Print ISSN: 2053-2229, Online ISSN: ISSN 2053-2210

$$\left\lfloor \sqrt{N} \right\rfloor \le q \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} - 1 \tag{30}$$

if *k* is even.

Consequently,

$$(p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2 \oplus p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \tag{31}$$

if *k* is odd, whereas

$$(p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1 \oplus q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor) \tag{32}$$

if *k* is even.

Proof. (Omitted)

□

Proposition 5. Let $N > 256$ be an odd integer and $k = \lfloor \log_2 N \rfloor - 1$; then

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 3} \le \left\lfloor \frac{7}{8}\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 4} \tag{33}$$

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 3} \le \left\lfloor \frac{9}{8}\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} \tag{34}$$

when k is odd, whereas

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 3} \le \left\lfloor \frac{7}{8}\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} \tag{35}$$

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} \le \left\lfloor \frac{9}{8}\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} \tag{36}$$

when k is even.

Proof. Direct calculation yields

$$2^{k+1} < N < 2^{k+2} \Rightarrow 2^{\frac{k+1}{2}} < \sqrt{N} < 2^{\frac{k+2}{2}}$$

$$\Rightarrow 2^{\frac{k+1}{2}-3}(2^2+2+1) < \frac{7}{8}\sqrt{N} < 2^{\frac{k+2}{2}-3}(2^2+2+1)$$

$$\Rightarrow 2^{\frac{k+1}{2}-1} + 2^{\frac{k+1}{2}-2} + 2^{\frac{k+1}{2}-3} < \frac{7}{8}\sqrt{N} < 2^{\frac{k+2}{2}-1} + 2^{\frac{k+2}{2}-2} + +2^{\frac{k+2}{2}-3}$$

$$\Rightarrow \left\lfloor 2^{\frac{k+1}{2}-1} + 2^{\frac{k+1}{2}-2} + 2^{\frac{k+1}{2}-3} \right\rfloor \le \left\lfloor \frac{7}{8}\sqrt{N} \right\rfloor \le \left\lfloor 2^{\frac{k+2}{2}-1} + 2^{\frac{k+2}{2}-2} + 2^{\frac{k+2}{2}-3} \right\rfloor$$

Print ISSN: 2053-2229, Online ISSN: ISSN 2053-2210

$$\left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor+\varepsilon-1}+2^{\left\lfloor \frac{k+1}{2} \right\rfloor+\varepsilon-2}+2^{\left\lfloor \frac{k+1}{2} \right\rfloor+\varepsilon-3} \right\rfloor \le \left\lfloor \frac{7}{8}\sqrt{N} \right\rfloor \le \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor+\varepsilon-\frac{1}{2}}+2^{\left\lfloor \frac{k+1}{2} \right\rfloor+\varepsilon-\frac{3}{2}}+2^{\left\lfloor \frac{k+1}{2} \right\rfloor+\varepsilon-\frac{5}{2}} \right\rfloor$$

Let $2^{\frac{k+1}{2}-1}+2^{\frac{k+1}{2}-2}+2^{\frac{k+1}{2}-3}=\Pi$; then $2^{\frac{k+2}{2}-1}+2^{\frac{k+2}{2}-2}+2^{\frac{k+2}{2}-3}=\Pi\sqrt{2}$ and thus

$$\lfloor \Pi \rfloor \le \left\lfloor \frac{7}{8}\sqrt{N} \right\rfloor \le \lfloor \Pi\sqrt{2} \rfloor \tag{37}$$

Letting $\frac{k+1}{2}-\left\lfloor \frac{k+1}{2} \right\rfloor=\varepsilon$ yields

$$\lfloor \Pi \rfloor - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} = \left\lfloor \Pi - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} \right\rfloor = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}(2^{\varepsilon-1}+2^{\varepsilon-2}+2^{\varepsilon-3}-1) \right\rfloor \tag{38}$$

and

$$\lfloor \Pi\sqrt{2} \rfloor - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} = \left\lfloor \Pi\sqrt{2} - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} \right\rfloor = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}(2^{\varepsilon-\frac{1}{2}}+2^{\varepsilon-\frac{3}{2}}+2^{\varepsilon-\frac{5}{2}}-1) \right\rfloor \tag{39}$$

By $\frac{1}{8}<\frac{7\sqrt{2}}{8}-1<\frac{1}{4}$, it can see by Lemma 4 (P13) that, when $k>0$ is even

$$\lfloor \Pi \rfloor - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}(2^{0.5-1}+2^{0.5-2}+2^{0.5-3}-1) \right\rfloor = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}\left(\frac{1}{\sqrt{2}}+\frac{1}{2\sqrt{2}}+\frac{1}{2^2\sqrt{2}}-1\right) \right\rfloor = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}\left(\frac{7\sqrt{2}}{8}-1\right) \right\rfloor \ge 2^{\left\lfloor \frac{k+1}{2} \right\rfloor-3}$$

and

$$\lfloor \Pi\sqrt{2} \rfloor - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}(2^{\frac{1}{2}-\frac{1}{2}}+2^{\frac{1}{2}-\frac{3}{2}}+2^{\frac{1}{2}-\frac{5}{2}}-1) \right\rfloor = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}\left(\frac{1}{2}+\frac{1}{4}\right) \right\rfloor = 2^{\left\lfloor \frac{k+1}{2} \right\rfloor-1}+2^{\left\lfloor \frac{k+1}{2} \right\rfloor-2}$$

which says,

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor}+2^{\left\lfloor \frac{k+1}{2} \right\rfloor-3} \le \left\lfloor \frac{7}{8}\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}+2^{\left\lfloor \frac{k+1}{2} \right\rfloor-1}+2^{\left\lfloor \frac{k+1}{2} \right\rfloor-2} \tag{40}$$

When $k>4$ is odd

$$\lfloor \Pi \rfloor - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}(2^{0-1}+2^{0-2}+2^{0-3}-1) \right\rfloor = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}\left(\frac{1}{2}+\frac{1}{4}+\frac{1}{8}-1\right) \right\rfloor = -2^{\left\lfloor \frac{k+1}{2} \right\rfloor-3}$$

and

$$\lfloor \Pi\sqrt{2} \rfloor - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}(2^{0-\frac{1}{2}}+2^{0-\frac{3}{2}}+2^{0-\frac{5}{2}}-1) \right\rfloor = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}\left(\frac{1}{\sqrt{2}}+\frac{1}{2\sqrt{2}}+\frac{1}{2^2\sqrt{2}}-1\right) \right\rfloor = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}\left(\frac{7\sqrt{2}}{8}-1\right) \right\rfloor$$

By $\frac{1}{8}<\frac{7\sqrt{2}}{8}-1<\frac{1}{4}$, it knows

$$\lfloor \Pi\sqrt{2} \rfloor - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor-2}$$

Print ISSN: 2053-2229, Online ISSN: ISSN 2053-2210

Accordingly an odd *k* yields

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 3} \le \left\lfloor \frac{7}{8}\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} \tag{41}$$

Now it is up to see the bound of $\left\lfloor \frac{7}{8}\sqrt{N} \right\rfloor$. Seeing from the following deductions in (42),

$$\begin{aligned}
&2^{k+1} < N < 2^{k+2} \Rightarrow 2^{\frac{k+1}{2}} < \sqrt{N} < 2^{\frac{k+2}{2}} \\
&\Rightarrow 2^{\frac{k+1}{2}-3}(2^3+1) < \frac{9}{8}\sqrt{N} < 2^{\frac{k+2}{2}-3}(2^3+1) \\
&\Rightarrow 2^{\frac{k+1}{2}} + 2^{\frac{k+1}{2}-3} < \frac{9}{8}\sqrt{N} < 2^{\frac{k+2}{2}} + 2^{\frac{k+2}{2}-3} \\
&\Rightarrow \left\lfloor 2^{\frac{k+1}{2}} + 2^{\frac{k+1}{2}-3} \right\rfloor \le \left\lfloor \frac{9}{8}\sqrt{N} \right\rfloor \le \left\lfloor 2^{\frac{k+2}{2}} + 2^{\frac{k+2}{2}-3} \right\rfloor \\
&\Rightarrow \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + \varepsilon} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + \varepsilon - 3} \right\rfloor \le \left\lfloor \frac{9}{8}\sqrt{N} \right\rfloor \le \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + \varepsilon + \frac{1}{2}} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + \varepsilon - \frac{5}{2}} \right\rfloor
\end{aligned} \tag{42}$$

it knows that, when $k > 4$ is odd

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 3} = \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 3} \right\rfloor \le \left\lfloor \frac{9}{8}\sqrt{N} \right\rfloor \le \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor}(\sqrt{2} + \frac{1}{\sqrt{32}}) \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1}$$

whereas when *k* is even

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} \le \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + \frac{1}{2}} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - \frac{5}{2}} \right\rfloor \le \left\lfloor \frac{9}{8}\sqrt{N} \right\rfloor \le \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} \right\rfloor = 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2}$$

Since $N > 256$, it knows that $(k = \lfloor \log_2 N \rfloor - 1) \ge 7$ and thus $\left\lfloor \frac{k+1}{2} \right\rfloor - 4 \ge 0$ is a valid quantity ensuring (33), (34), (35) and (36) meaningful.

□

Corollary 3. Let $(N = pq) > 64$ be an odd integer with $1 < \frac{q}{p} < \frac{5}{4}$ and $k = \lfloor \log_2 N \rfloor - 1$; then

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 3} + 1 \le p \le \left\lfloor \sqrt{N} \right\rfloor \tag{43}$$

$$\left\lfloor \sqrt{N} \right\rfloor \le q \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} - 1 \tag{44}$$

when k is odd, whereas

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 3} + 1 \le p \le \left\lfloor \sqrt{N} \right\rfloor \tag{45}$$

$$\left\lfloor \sqrt{N} \right\rfloor \le q \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} - 1 \tag{46}$$

Print ISSN: 2053-2229, Online ISSN: ISSN 2053-2210

when k is even.

Consequently,

$$(p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2 \oplus p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \tag{47}$$

when k is odd, whereas

$$(p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1 \oplus q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor) \tag{48}$$

when k is even.

Proof. (Omitted).

□

Proposition 6. Let $N > 1024$ be an odd integer and $k = \lfloor \log_2 N \rfloor - 1$ be an odd integer; then then

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} \le \left\lfloor (1 - \frac{\sqrt{2}-1}{2})\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} \tag{49}$$

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 3} \le \left\lfloor \frac{\sqrt{2}+1}{2}\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} \tag{50}$$

when k is odd, whereas

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 5} \le \left\lfloor (1 - \frac{\sqrt{2}-1}{2})\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} \tag{51}$$

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} \le \left\lfloor \frac{\sqrt{2}+1}{2}\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} \tag{52}$$

when k is even.

Proof. The inequality $\frac{3}{4} < 1 - \frac{\sqrt{2}-1}{2} < \frac{7}{8}$ immediately yields

$$\left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor \le \left\lfloor (1 - \frac{\sqrt{2}-1}{2})\sqrt{N} \right\rfloor \le \left\lfloor \frac{7}{8}\sqrt{N} \right\rfloor \tag{53}$$

When *k* is even, referring to (18) and (33), it leads to

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 5} \le \left\lfloor (1 - \frac{\sqrt{2}-1}{2})\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} \tag{55}$$

and when *k* is odd, referring to (19) and (35), it leads to

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} \le \left\lfloor (1 - \frac{\sqrt{2}-1}{2})\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} \tag{56}$$

Print ISSN: 2053-2229, Online ISSN: ISSN 2053-2210

Now considering

$$2^{k+1} < N < 2^{k+2} \Rightarrow 2^{\frac{k+1}{2}} < \sqrt{N} < 2^{\frac{k+2}{2}}$$
$$\Rightarrow 2^{\frac{k+1}{2}}(2^{-\frac{1}{2}} + 2^{-1}) < \frac{\sqrt{2}+1}{2}\sqrt{N} < 2^{\frac{k+2}{2}}(2^{-\frac{1}{2}} + 2^{-1})$$
$$\Rightarrow 2^{\frac{k+1}{2}-\frac{1}{2}} + 2^{\frac{k+1}{2}-1} < \frac{\sqrt{2}+1}{2}\sqrt{N} < 2^{\frac{k+1}{2}} + 2^{\frac{k+1}{2}-\frac{1}{2}}$$
$$\Rightarrow \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + \varepsilon - \frac{1}{2}} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + \varepsilon - 1} \right\rfloor \le \left\lfloor \frac{\sqrt{2}+1}{2}\sqrt{N} \right\rfloor \le \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + \varepsilon} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + \varepsilon - \frac{1}{2}} \right\rfloor$$

it knows

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} \le \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - \frac{1}{2}} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} \right\rfloor \le \left\lfloor \frac{\sqrt{2}+1}{2}\sqrt{N} \right\rfloor \le \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - \frac{1}{2}} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} \tag{57}$$

when *k* is odd, whereas

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} \le \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - \frac{1}{2}} \right\rfloor \le \left\lfloor \frac{\sqrt{2}+1}{2}\sqrt{N} \right\rfloor \le \left\lfloor 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + \frac{1}{2}} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor} \tag{58}$$

when *k* is even.

Meanwhile, since $\frac{9}{8}\sqrt{N} < \frac{\sqrt{2}+1}{2}\sqrt{N} < \frac{10}{8}\sqrt{N}$, by (25), (26), (34) and (36), it also lead to

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 3} \le \left\lfloor \frac{\sqrt{2}+1}{2}\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} \tag{59}$$

when k is odd, whereas

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} \le \left\lfloor \frac{\sqrt{2}+1}{2}\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} \tag{60}$$

when k is even.

Comparing (57) with (59), (58) with (60), it knows

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 3} \le \left\lfloor \frac{\sqrt{2}+1}{2}\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} \tag{61}$$

when k is odd, whereas

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} \le \left\lfloor \frac{\sqrt{2}+1}{2}\sqrt{N} \right\rfloor \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} \tag{62}$$

Referring to previous proofs, it knows that $N > 1024$ ensures the validation of (49), (50), (51) and (52).

□

Print ISSN: 2053-2229, Online ISSN: ISSN 2053-2210

Corollary 4. Let $(N = pq) > 1024$ be an odd integer with $1 < \frac{q}{p} < \sqrt{2}$ and $k = \lfloor \log_2 N \rfloor - 1$; then

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} - 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 2} + 1 \le p \le \left\lfloor \sqrt{N} \right\rfloor \tag{63}$$

$$\left\lfloor \sqrt{N} \right\rfloor \le q \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} \tag{64}$$

when k is odd, whereas

$$2^{\left\lfloor \frac{k+1}{2} \right\rfloor} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 5} + 1 \le p \le \left\lfloor \sqrt{N} \right\rfloor \tag{65}$$

$$\left\lfloor \sqrt{N} \right\rfloor \le q \le 2^{\left\lfloor \frac{k+1}{2} \right\rfloor + 1} + 2^{\left\lfloor \frac{k+1}{2} \right\rfloor - 1} \tag{66}$$

when k is even.

Consequently,

$$(p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2 \oplus p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \tag{67}$$

when k is odd, whereas

$$(p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1 \oplus q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor) \tag{68}$$

when k is even.

Proof. (Omitted).

□

Theorem 1. For a RSA modulus $N = pq$ with $1 < p < q$, the distribution of divisor p in $\boldsymbol{T}_3$ tree is completely determined by the divisor-ratio $1 < \frac{q}{p} = \chi < 2$ and integer $k = \lfloor \log_2 N \rfloor - 1$. When k is even, there is a χ_0 with $\frac{3}{2} < \chi_0 < 2$ such that $(p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1 \oplus q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor)$ when $1 < \frac{q}{p} \le \chi_0$ whereas $p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2$ when $\chi_0 < \frac{q}{p} < 2$. When k is odd, $(p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2 \oplus p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1)$ and the smaller χ is the closer p and q are to $\lfloor \sqrt{N} \rfloor$.

Proof. A simple summarization of the cases proved in Corollary 1, Corollary 2, Corollary 3 and Corollary 4 immediately conclusions of the theorem.

□

Print ISSN: 2053-2229, Online ISSN: ISSN 2053-2210

NUMERICAL EXPERIMENTS IN MATHEMATICA

To test the proved conclusions, numerical experiment was made with Mathematica. The experiment first chose randomly semiprime N from the semiprime table, e.g., from *The On-Line Encyclopedia of Integer Sequences (OEIS)*, then located N's level by $k_1 = \lfloor \log_2 N \rfloor - 1$, calculated $\lfloor \sqrt{N} \rfloor$ and its level $k_2 = \left\lfloor \log_2 \lfloor \sqrt{N} \rfloor \right\rfloor - 1$, calculate the possible bound of N's smaller divisor p and its level by $k_p = \lfloor \log_2 p \rfloor - 1$, calculate the possible bound of N's bigger divisor q and its level by $k_q = \lfloor \log_2 q \rfloor - 1$, checked the divisor-ratio and judge the consistency to Corollary 1, Corollary 2 and Theorem 1. Mathematica programs are list as follows.

```
flsqrt[N_] := Floor[Sqrt[N]];
kn[N_] := Floor[Log[N]/Log[2]] - 1; (*levelofN*)
ksn[N_] := Floor[Log[Floor[Sqrt[N]] + 0.01]/Log[2]] - 1; (*levelofSqrt[N]*)
kp[p_] := Floor[Log[p]/Log[2]] - 1; (*levelofp*)
ratio[N_, p_] := N/p^2;
(*p'sleftboundforoddkwhenq / p < 1.5*)
Lpo[N_] = 2^Floor[Log[N]/Log[2]/2] - 2^(Floor[Log[N]/Log[2]/2] - 2) + 1;
(*p'sleftboundforevenkwhenq / p < 1.5*)
Lpe[N_] = 2^Floor[Log[N]/Log[2]/2] + 2^(Floor[Log[N]/Log[2]/2] - 5) + 1;
(*q'srightboundforoddkwhenq / p < 1.5*)
Rqo[N_] = 2^(Floor[Log[N]/Log[2]/2] + 1) - 1;
(*q'srightboundforevenkwhenq / p < 1.5*)
Rqe[N_] = 2^(Floor[Log[N]/Log[2]/2] + 1) + 2^(Floor[Log[N]/Log[2]/2] - 1) - 1;
inDataN = {72593, 386757, 489779, 753041, 2350553, 4538873, 8772041};
inDataP = {229, 441, 647, 739, 1259, 2029, 2659};
r1 = Table[inDataN[[i]], {i, 7}]; (*N*)
r2 = Table[kn[inDataN[[i]]], {i, 7}]; (*N'slevel*)
r3 = Table[ksn[inDataN[[i]]], {i, 7}]; (*sqrtN'slevel*)
r4 = Table[ flsqrt[inDataN[[i]]], {i, 7}]; (*Sqrt(N)*)
r5 = Table[Lpo[inDataN[[i]]], {i, 7}]; (*p'sleftbound,oddk*)
r6 = Table[Lpe[inDataN[[i]]], {i, 7}]; (*p'sleftbound,evenk*)
r7 = Table[Rqo[inDataN[[i]]], {i, 7}]; (*q'sleftbound,oddk*)
```


Print ISSN: 2053-2229, Online ISSN: ISSN 2053-2210

$r8 = Table[Rqe[inDataN[[i]]],\{i,7\}];(*q'sleftbound, evenk*)$
$r9 = Table[inDataP[[i]],\{i,7\}];(*p*)$
$r10 = Table[inDataN[[i]]/inDataP[[i]],\{i,7\}];(*N/pp*)$
$r11 = Table[kp[inDataP[[i]]],\{i,7\}];(*p'slevel*)$
$r12 = Table[kp[inDataN[[i]]/inDataP[[i]]],\{i,7\}];(*q'slevel*)$
$r13 = Table[ratio[inDataN[[i]], inDataP[[i]]]//N,\{i,7\}];$
$t = \{r1,r2,r3,r4,r5,r6,r7,r8,r9,r10,r11,r12,r13\}//MatrixForm$

The computations of running the programs are shown with a matrix form in Figure 1. In the matrix, row 1 contains the seven input data $N = \{72593, 386757, 489779, 753041, 2350553, 4538873, 8772041\}$, row 2 means the level k for each N, row 3 shows the level for each $\lfloor\sqrt{N}\rfloor$, row 4 shows the value for each $\lfloor\sqrt{N}\rfloor$, row 5 shows the left bound of N's smaller divisor p in the case k is odd, row 6 shows the left bound of p in the case k is even, row 7 shows the right bound of N's bigger divisor q in the case k is odd, row 8 shows the right bound of q in the case k is even, row 9 shows N's smaller divisor p, row 10 shows N's bigger divisor q, row 11 shows p's level, row 12 shows q's level and row 13 shows the ratio q/p. Take 386757 as an example. It can see that, $386757 \triangleq 17$ thus $k = 17$ is odd. By Theorem 1, the smaller divisor of 386757 possibly lies on level $\left\lfloor\frac{17+1}{2}\right\rfloor - 2 = 7$ or $\left\lfloor\frac{17+1}{2}\right\rfloor - 1 = 8$. By Corollary 1, $2^{\left\lfloor\frac{k+1}{2}\right\rfloor} - 2^{\left\lfloor\frac{k+1}{2}\right\rfloor-1} + 1 \le p \le \lfloor\sqrt{N}\rfloor$ and $\lfloor\sqrt{N}\rfloor \le q \le 2^{\left\lfloor\frac{k+1}{2}\right\rfloor+1} + 2^{\left\lfloor\frac{k+1}{2}\right\rfloor-1} - 1$. By calculation, it yields, $p \ge 2^{\left\lfloor\frac{k+1}{2}\right\rfloor} - 2^{\left\lfloor\frac{k+1}{2}\right\rfloor-1} + 1 = 385$, $\lfloor\sqrt{386757}\rfloor = 621$ and $q \le 2^{\left\lfloor\frac{k+1}{2}\right\rfloor+1} + 2^{\left\lfloor\frac{k+1}{2}\right\rfloor-1} - 1 = 1023$. The results fact match to the fact that $p = 441 \triangleq 7$, $q = 887 \triangleq 8$ and $\chi = 1.98866 > 1.5$. Checking the other numbers one by one, it can see that all the calculated results match the corollaries and the theorem as expected.

72 593	386 757	489 779	753 041	2 350 553	4 538 873	8 772 041
15	17	17	18	20	21	22
7	8	8	8	9	10	10
269	621	699	867	1533	2130	2961
193	385	385	385	769	1537	1537
265	529	529	529	1057	2113	2113
511	1023	1023	1023	2047	4095	4095
639	1279	1279	1279	2559	5119	5119
229	441	647	739	1259	2029	2659
317	877	757	1019	1867	2237	3299
6	7	8	8	9	9	10
7	8	8	8	9	10	10
1.38428	1.98866	1.17002	1.37889	1.48292	1.10251	1.24069

Figure 1. Screenshot of the program's output

CONCLUSION

It is undoubtedly meaningful to know the divisors' range of a RSA modulus. The investigation in this paper discloses the deep relationship between the divisor-ratio and the distribution of the small divisor. The propositions and theorem proved in this paper indicate that, factorisation of the RSA numbers may be achieved via a small search on specific level of $\boldsymbol{T}_3$ tree, and the smaller the divisor-ratio is the easier the search will be done. This discovers an opposite direction to the classics thoughts that the smaller the divisor-ratio is the harder is the factorisation. Hope future work would be successful in the related researches.

Print ISSN: 2053-2229, Online ISSN: ISSN 2053-2210

Acknowledgement

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 2015A010104011, Foshan Bureau of Science and Technology under projects 2016AG100311, Project gg040981 from Foshan University. The author sincerely present thanks to them all.

REFERENCES

CHEN G., LI J. (2018) *Brief Investigation on Square Root of a Node of T3 Tree*, Advances in Pure Mathematics,8(7) 666-671

LI J., (2018) *A Parallel Probabilistic Approach to Factorize a Semiprime*, American Journal of Computational Mathematics, vol. 8, no. 2, pp.153-162, 2018

National Institute of Standards and Technology (NIST). (2009) Digital signature standard (DSS), FIPS publication 186-3.

WANG X. (2016) *Valuated Binary Tree: A New Approach in Study of Integers*. International Journal of Scientific and Innovative Mathematical Research (IJSIMR), 4(3) 63-67

WANG X., (2016) *Amusing Properties of Odd Numbers Derived From Valuated Binary Tree*, IOSR Journal of Mathematics (IOSR-JM), 12(6) 53-57

WANG X. (2017) *Brief Summary of Frequently-Used Properties of the Floor Function*, IOSR Journal of Mathematics (IOSR-JM), 13(5) 46-48

WANG X., (2017) *Strategy For Algorithm Design in Factoring RSA Numbers*, IOSR Journal of Computer Engineering (IOSR-JCE), 19(3,ver. II)1-7

WANG X., (2017) *Genetic Traits of Odd Numbers With Applications in Factorization of Integers*, Global Journal of Pure and Applied Mathematics (GJPAM), 13(2) 493-517

WANG X., (2017) *Two More Symmetric Properties of Odd Numbers*, IOSR Journal of Mathematics (IOSR-JM), 13(3ver. II) 37-40

WANG X. (2018) *T3 Tree and Its Traits in Understanding Integers*, Advances in Pure Mathematics (APM), 8(5) 494-507

WANG X., (2018) *Some Inequalities on T3 Tree*, Advances in Pure Mathematics (APM), 8(8) 711-719

WANG X., (2018) *More on Square and Square Root of a Node on T3 Tree*, International Journal of Mathematics and Statistics Study (IJMSS), 6(3) 1-7

WANG X., (2018) *Some New Inequalities With Proofs and Comments on Applications*, Journal of Mathematics Research (JMR), 10(3) 15-19

WANG X., (2018) *Influence of Divisor-ratio to Distribution of Semiprime's Divisor*, Journal of Mathematics Research (JMR), 10(4) 54-61

WANG X., (2018) *Traits of a RSA Modulus on T3 Tree*, Journal of Mathematics Research (JMR), 10(6) 10-20

Print ISSN: 2053-2229, Online ISSN: ISSN 2053-2210