Traits of a RSA Modulus on T_3 Tree

Xingbo WANG[1,2,3], Zhen SHEN[1]

[1] Department of Mechatronic Engineering, Foshan University, Foshan City, PRC

[2] Guangdong Engineering Center of Information Security for Intelligent Manufacturing System, Foshan City, PRC

[3] State Key Laboratory of Mathematical Engineering and Advanced Computing, Wuxi City, PRC

Correspondence: Xingbo WANG, Department of Mechatronic Engineering, Foshan University, Foshan City, PRC.
Email: dr.xbwang@qq.com; xbwang@fosu.edu.cn

Received: September 11, 2018 Accepted: October 7, 2018 Online Published: October 15, 2018
doi:10.5539/jmr.v10n6p15 URL: https://doi.org/10.5539/jmr.v10n6p15

Abstract

The article investigates how the two divisors of a RSA modulus distribute in the T3 tree. It proves that, the two divisors of a RSA modulus lie on the same level or on two adjacent levels and at least one of them is clamped on the same level where the square root of the RSA modulus lies. Then the paper proposes three interval-subdivisions that can indicate which subinterval the two divisors lie in. Mathematical deductions are showed in detail, which can be a reference to design algorithm of RSA factorization.

Keywords: RSA modulus, divisor distribution, binary tree, subdivision

1. Introduction

The RSA modulus, which is also called a RSA number, is a big semiprime composed of two distinct prime divisors, say p and q with $3 \leq p < q$ such that $1 < q/p < \sqrt{2}$, according to the American Digital Signature Standard (DSS)(NIST, 2009). As stated in WANG's paper(WANG, 2017: Strategy RSA), the RSA numbers have been essentially important in cryptography ever since the RSA public cryptosystem was established. It is believed that, a systematic theory or method that can factorize the RSA numbers means the failure of the RSA public cryptosystem. Thus factorization of the RSA numbers has been a dream filled with fantasies of researchers and engineers working on information security. Nevertheless, the list of unfactroized RSA numbers gets longer and longer on the bulletin.

In August 2016, WANG introduced a new approach, called T_3 tree, to study integers in article (WANG, 2016: Valuated Binary Tree). Through the approach, many new properties of integers were disclosed, as introduced in papers list in the references of WANG's papers (WANG, 2016, 2017, 2018) and CHEN's paper (CHEN, 2018), and even new approaches to factorize integers were found, as claimed in FU's paper (FU, 2017) and LI's paper (LI, 2018).

Due to the importance of RSA numbers, it is necessary to investigate them on the T_3 tree. Accordingly, this article makes a brief investigation on the trait of the RSA modulus on the $T3$ tree. The research in this article may provide certain foundation for knowing the RSA modulus.

2. Preliminaries

2.1 Definitions and Notations

Let S be a set of finite positive integers with s_0 and s_n being the smallest and the biggest terms respectively; an integer x is said to *be clamped* in S if $s_0 \leq x \leq s_n$. Symbol $x \stackrel{\triangle}{=} S$ 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 $x-1 < \lfloor x \rfloor \leq x$, or equivalently $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$. Let $N = pq$ be an odd integer with $1 < p < q$; then $k = \frac{q}{p}$ is called the *divisor-ratio* of N.

In this whole paper, symbol T_3 is the T_3 tree that was introduced in WANG's papers (WANG, 2016 & 2018: T_3 Tree) and symbol $N_{(k,j)}$ is by default the node at position j on level k of 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 of T_3. An integer X is said to be clamped on level k of T_3 if $2^{k+1} \leq X \leq 2^{k+2} - 1$ and symbol $X \stackrel{\triangle}{=} k$ indicates X is clamped on level k. An odd integer O satisfying $2^{k+1} + 1 \leq O \leq 2^{k+2} - 1$ is said to be on level k of T_3, and use symbol $O \stackrel{\Delta}{=} k$ to express it. Symbol $(p \stackrel{\circ}{=} q) = k$ 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 $A \Rightarrow B$ means conclusion B can be derived from condition A. Symbol $(a = b) > c$ means a takes the value of c and $a > c$. The union symbol $\cup$ of the set operation is also used in this paper.

2.2 Lemmas

Lemma 1(**See in (WANG, 2016 & 2018: T_3 Tree)**). *The 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 T_3 tree. Odd integer N with $N > 1$ lies on level $\lfloor \log_2 N \rfloor - 1$.*
***(P2)**. $N_{(k,j)}$ is calculated by*

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

and thus

$$2^{k+1} + 1 \le N_{(k,j)} \le 2^{k+2} - 1 \tag{2}$$

***(P3)**. The biggest node on level k of left branch is $2^{k+1} + 2^k - 1$ whose position is $j = 2^{k-1} - 1$, and the smallest node on level k of right branch is $2^{k+1} + 2^k + 1$ whose position is $j = 2^{k-1}$. On the same level, there is not a node that is a multiple of another one.*
***(P4)**. Multiplication of arbitrary two nodes of T_3, say $N_{(m,\alpha)}$ and $N_{(n,\beta)}$, is a third node of 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*

$$N_{(m,\alpha)} \times N_{(n,\beta)} = 2^{m+n+2} + 1 + 2J \tag{3}$$

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 T_3; whereas, if $J \ge 2^{m+n+1}$, $N_{(m,\alpha)} \times N_{(n,\beta)} = N_{(m+n+2,\chi)}$ with $\chi = J - 2^{m+n+1}$ lies on level $m + n + 2$ of T_3.

Lemma 2(**See in (WANG, 2018: Square root)**). *Let $N > 3$ be an odd integer and $k = \lfloor \log_2 N \rfloor - 1$; then $(\lfloor \sqrt{N} \rfloor \le \lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \rfloor) \triangleq \lfloor \frac{k-1}{2} \rfloor$ when k is odd whereas $(\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \rfloor \le \lfloor \sqrt{N} \rfloor) \triangleq \lfloor \frac{k-1}{2} \rfloor$ when k is even.*

Lemma 3(**See in (WANG, 2017: Summary floor function)**). *For real numbers x and y, it holds*
***(P2)**. $\lfloor x \rfloor - \lfloor y \rfloor - 1 \le \lfloor x - y \rfloor \le \lfloor x \rfloor - \lfloor y \rfloor < \lfloor x \rfloor - \lfloor y \rfloor + 1$*
***(P6)**. $\lfloor xy \rfloor \ge \lfloor x \rfloor \lfloor y \rfloor$ with $x, y \ge 0$.*
***(P7)**. $\lfloor \frac{y}{x} \rfloor \le \frac{\lfloor y \rfloor}{\lfloor x \rfloor}$ with $x \ge 1$ and $y > 0$.*
***(P13)**. $x \le y \Rightarrow \lfloor x \rfloor \le \lfloor y \rfloor$.*
***(P15)**. $\lfloor \frac{\lfloor x \rfloor}{m} \rfloor = \lfloor \frac{x}{m} \rfloor$ with $m \ge 1$.*
***(P28)**. $N - \lfloor \sqrt{N} \rfloor^2 \ge 0$ with N being a positive integer.*
***(P31)**. $i - 1 \le 2\lfloor \frac{i}{2} \rfloor \le i$ with i being a positive integer.*

Lemma 4(**See in (WANG, 2018: Inequalities)**). *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

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

Lemma 5. *Let n be a positive odd integer; then $n = \lfloor \sqrt{n} \rfloor^2$ or $n = \lfloor \sqrt{n} \rfloor (\lfloor \sqrt{n} \rfloor + 2)$ if $\lfloor \sqrt{n} \rfloor | n$.*

Proof. Since $\lfloor \sqrt{n} \rfloor | n$, it knows that there is a positive integer k such that $n = k \lfloor \sqrt{n} \rfloor$. By definition of the floor function, $\lfloor \sqrt{n} \rfloor \le \sqrt{n} < \lfloor \sqrt{n} \rfloor + 1$; hence

$$\begin{aligned}
&\lfloor \sqrt{n} \rfloor^2 \le n < (\lfloor \sqrt{n} \rfloor + 1)^2 = \lfloor \sqrt{n} \rfloor^2 + 2\lfloor \sqrt{n} \rfloor + 1 \\
&\Rightarrow \lfloor \sqrt{n} \rfloor^2 \le k \lfloor \sqrt{n} \rfloor < \lfloor \sqrt{n} \rfloor^2 + 2\lfloor \sqrt{n} \rfloor + 1 \\
&\Rightarrow \lfloor \sqrt{n} \rfloor \le k < \lfloor \sqrt{n} \rfloor + 2 + \tfrac{1}{\lfloor \sqrt{n} \rfloor} \\
&\Rightarrow \lfloor \sqrt{n} \rfloor \le k \le \lfloor \sqrt{n} \rfloor + 2
\end{aligned}$$

which means k takes one of $\lfloor \sqrt{n} \rfloor$,$\lfloor \sqrt{n} \rfloor + 1$ and $\lfloor \sqrt{n} \rfloor + 2$.

Obviously the case $k = \lfloor \sqrt{n} \rfloor + 1$ is impossible because n is odd. Hence $k = \lfloor \sqrt{n} \rfloor$ or $k = \lfloor \sqrt{n} \rfloor + 2$. □

3. Main Results

Proposition 1. *Let $N = pq$ be an odd integer with $1 < p < q$ and $1 < \frac{q}{p} < k$; then*

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

where k is real, $\lfloor x \rfloor = 0$ if $x \le 0$.
Particularly, when $k = 2$, it yields

$$\left\lfloor \frac{\sqrt{N}}{2} \right\rfloor < p \le \left\lfloor \sqrt{N} \right\rfloor \otimes \left\lfloor \sqrt{N} \right\rfloor \le q \le \left\lfloor \frac{3}{2}\sqrt{N} \right\rfloor \tag{5}$$

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

$$\left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor < p \le \left\lfloor \sqrt{N} \right\rfloor \otimes \left\lfloor \sqrt{N} \right\rfloor \le q \le \left\lfloor \frac{5}{4}\sqrt{N} \right\rfloor \tag{6}$$

when $k = \sqrt{2}$, it yields

$$\left\lfloor (1 - \frac{\sqrt{2}-1}{2})\sqrt{N} \right\rfloor < p \le \left\lfloor \sqrt{N} \right\rfloor \otimes \left\lfloor \sqrt{N} \right\rfloor \le q \le \left\lfloor \frac{\sqrt{2}+1}{2}\sqrt{N} \right\rfloor \tag{7}$$

Proof. By $1 < p < q$, it knows

$$p \le \sqrt{N} \otimes q \ge \sqrt{N}$$

Then the conditions $1 < p < q$ and $1 < \frac{q}{p} < k$ directly yield

$$\begin{aligned}
&q + p > 2\sqrt{pq} \otimes p < q < kp \\
&\Rightarrow -q - p < -2\sqrt{N} \otimes 0 < q - p < (k-1)p \le (k-1)\sqrt{N} \\
&\Rightarrow -2p < (k-3)\sqrt{N} \otimes 2q < (k+1)\sqrt{N} \\
&\Rightarrow \tfrac{3-k}{2}\sqrt{N} < p \le \sqrt{N} \otimes \sqrt{N} \le q < \tfrac{k+1}{2}\sqrt{N} \\
&\Rightarrow \left\lfloor \tfrac{3-k}{2}\sqrt{N} \right\rfloor < p \le \left\lfloor \sqrt{N} \right\rfloor \otimes \left\lfloor \sqrt{N} \right\rfloor \le q \le \left\lfloor \tfrac{k+1}{2}\sqrt{N} \right\rfloor
\end{aligned}$$

□

Proposition 2. *Let $N = pq$ be an odd integer with $1 < p < q$ and $1 < \frac{q}{p} < k$; then*

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

Proof. Use proof by contradiction. Assume $kp \le \left\lfloor \sqrt{N} \right\rfloor$; then by $1 < \frac{q}{p} < k$ it yields $p < q < kp \le \sqrt{N}$ which is contradictory to $q \ge \sqrt{N}$. Likewise, by $1 < \frac{q}{p} < k$, assuming $\frac{q}{k} \ge \left\lfloor \sqrt{N} \right\rfloor$ results in a contradiction of $\left\lfloor \sqrt{N} \right\rfloor \le \frac{q}{k} < p$. □

Proposition 3. *Let N and k be positive integers with $k > 2$; then it holds*

$$\left\lfloor \sqrt{N} \right\rfloor \overset{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1 \Rightarrow \left\lfloor \frac{\sqrt{N}}{2} \right\rfloor \overset{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 2$$

$$\left\lfloor \sqrt{N} \right\rfloor \overset{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1 \Rightarrow \left(\left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor \overset{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1\right) \oplus \left(\left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor \overset{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 2\right)$$

and

$$\left\lfloor \sqrt{N} \right\rfloor \overset{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1 \Rightarrow \left(\left\lfloor (1 - \frac{\sqrt{2}-1}{2})\sqrt{N} \right\rfloor \overset{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1\right) \oplus \left(\left\lfloor (1 - \frac{\sqrt{2}-1}{2})\sqrt{N} \right\rfloor \overset{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 2\right)$$

In general, for arbitrary positive integer M and $k > 0$ it holds

$$M \overset{\wedge}{=} k \Rightarrow \begin{cases} \left\lfloor \frac{M}{2} \right\rfloor \overset{\wedge}{=} k - 1 \\ 2M \overset{\wedge}{=} k + 1 \end{cases}$$

Proof. $k > 2$ is mandatory because $k \leq 2$ yields $\left\lfloor \frac{k+1}{2} \right\rfloor - 2 < 0$ losses its meaning. By definition,

$$\left\lfloor \sqrt{N} \right\rfloor \stackrel{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1 \Rightarrow 2^{\lfloor \frac{k+1}{2} \rfloor} \leq \left\lfloor \sqrt{N} \right\rfloor \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1 < 2^{\lfloor \frac{k+1}{2} \rfloor + 1} \tag{8}$$

Then simple deduction with the help of the inequality (8) yields

$$\begin{aligned} &\left\lfloor \sqrt{N} \right\rfloor \stackrel{\wedge}{=} \left\lfloor \tfrac{k+1}{2} \right\rfloor - 1 \Rightarrow 2^{\lfloor \frac{k+1}{2} \rfloor} \leq \left\lfloor \sqrt{N} \right\rfloor < 2^{\lfloor \frac{k+1}{2} \rfloor + 1} \\ &\Rightarrow 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \leq \frac{\lfloor \sqrt{N} \rfloor}{2} < 2^{\lfloor \frac{k+1}{2} \rfloor} \Rightarrow 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \leq \left\lfloor \frac{\lfloor \sqrt{N} \rfloor}{2} \right\rfloor < 2^{\lfloor \frac{k+1}{2} \rfloor} \end{aligned}$$

$$M \stackrel{\wedge}{=} k \Rightarrow 2^{k+1} \leq M < 2^{k+2} \Rightarrow 2^k \leq \frac{M}{2} < 2^{k+1} \Rightarrow 2^k \leq \left\lfloor \frac{M}{2} \right\rfloor < 2^{k+1}$$

and

$$M \stackrel{\wedge}{=} k \Rightarrow 2^{k+1} \leq M < 2^{k+2} \Rightarrow 2^{k+2} \leq 2M < 2^{k+3} \Rightarrow 2^{k+2} \leq 2M < 2^{k+3}$$

By Lemma 2(**P15**), $\left\lfloor \frac{\lfloor \sqrt{N} \rfloor}{2} \right\rfloor = \left\lfloor \frac{\sqrt{N}}{2} \right\rfloor$ and thus $\left\lfloor \sqrt{N} \right\rfloor \stackrel{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1 \Rightarrow \left\lfloor \frac{\sqrt{N}}{2} \right\rfloor \stackrel{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 2$, $M \stackrel{\wedge}{=} k \Rightarrow \begin{cases} \left\lfloor \frac{M}{2} \right\rfloor \stackrel{\wedge}{=} k-1 \\ 2M \stackrel{\wedge}{=} k+1 \end{cases}$.

By Lemma 4, it knows

$$\left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor < \frac{3}{4}(\left\lfloor \sqrt{N} \right\rfloor + 1) = \left\lfloor \sqrt{N} \right\rfloor - \frac{1}{4}\left\lfloor \sqrt{N} \right\rfloor + \frac{3}{4}$$

and

$$\left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor > \frac{3}{4}\left\lfloor \sqrt{N} \right\rfloor - 1 = \frac{1}{2}\left\lfloor \sqrt{N} \right\rfloor + \frac{1}{4}\left\lfloor \sqrt{N} \right\rfloor - 1$$

Thus $\left\lfloor \sqrt{N} \right\rfloor \geq 3$ yields $\left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor < \left\lfloor \sqrt{N} \right\rfloor$, and $\left\lfloor \sqrt{N} \right\rfloor \geq 4$ yields $\left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor > \frac{1}{2}\left\lfloor \sqrt{N} \right\rfloor \geq \left\lfloor \frac{\sqrt{N}}{2} \right\rfloor$. Note that, the conditions $k > 2$ and $\left\lfloor \sqrt{N} \right\rfloor \stackrel{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1$ indicate $\left\lfloor \sqrt{N} \right\rfloor \geq 4$, accordingly

$$\left\lfloor \frac{\sqrt{N}}{2} \right\rfloor < \left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor < \left\lfloor \sqrt{N} \right\rfloor$$

Similarly, it can show

$$\left\lfloor \frac{\sqrt{N}}{2} \right\rfloor < \left\lfloor (1 - \frac{\sqrt{2}-1}{2})\sqrt{N} \right\rfloor < \left\lfloor \sqrt{N} \right\rfloor$$

Since $\left\lfloor \sqrt{N} \right\rfloor \stackrel{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1 \Rightarrow \left\lfloor \frac{\sqrt{N}}{2} \right\rfloor \stackrel{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 2$, it surely holds

$$\left\lfloor \sqrt{N} \right\rfloor \stackrel{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1 \Rightarrow (\left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor \stackrel{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \oplus (\left\lfloor \frac{3}{4}\sqrt{N} \right\rfloor \stackrel{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 2)$$

and

$$\left\lfloor \sqrt{N} \right\rfloor \stackrel{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1 \Rightarrow (\left\lfloor (1 - \frac{\sqrt{2}-1}{2})\sqrt{N} \right\rfloor \stackrel{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \oplus (\left\lfloor (1 - \frac{\sqrt{2}-1}{2})\sqrt{N} \right\rfloor \stackrel{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 2)$$

□

Proposition 4. *Let $N = pq$ be a node of T_3 with $1 < p < q$ and $1 < \frac{q}{p} < 2$; then*
(1) p and q lie on the same level or on two adjacent levels.
(2) At least one of p and q lies on the same level as where $\left\lfloor \sqrt{N} \right\rfloor$ is clamped.

Proof. Without loss of generality, let $p = N_{(m,*)}$ and $q = N_{(n,*)}$ with $n \geq m \geq 0$. Use proof by contradiction.

To prove the assertion (1), assume $n - m \geq 2$. Then p and q satisfy $p \leq 2^{m+2} - 1 \leq 2^n - 1$ and $q \geq 2^{n+1} + 1$. Consequently

$$\frac{q}{p} > \frac{2^{n+1}+1}{2^n - 1} = \frac{2^{n+1} - 2 + 3}{2^n - 1} = 2 + \frac{3}{2^n - 1} > 2$$

This is contradictory to the condition $1 < \frac{q}{p} < 2$. Hence it must hold $0 \leq n - m < 2$, which says the assertion (1) holds.

To prove the assertion (2), let $k = \lfloor \log_2 N \rfloor - 1$. By Lemma 2, $\left\lfloor \sqrt{N} \right\rfloor \stackrel{\wedge}{=} \left\lfloor \frac{k-1}{2} \right\rfloor = \left\lfloor \frac{k+1}{2} \right\rfloor - 1$. Assume the neither of p and q is clamped on level $\left\lfloor \frac{k+1}{2} \right\rfloor - 1$; then $p < 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \otimes q < 2^{\lfloor \frac{k+1}{2} \rfloor - 1}$ holds or $p > 2^{\lfloor \frac{k+1}{2} \rfloor + 1} \otimes q > 2^{\lfloor \frac{k+1}{2} \rfloor + 1}$ holds. By Lemma 3(**P31**), $2\left\lfloor \frac{k+1}{2} \right\rfloor - 2 \leq k - 1$ and $2\left\lfloor \frac{k+1}{2} \right\rfloor + 2 \geq k + 2$, it knows

$$p < 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \otimes q < 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \Rightarrow N = pq < 2^{2\lfloor \frac{k+1}{2} \rfloor - 2} \leq 2^{k-1}$$

and

$$p > 2^{\lfloor \frac{k+1}{2} \rfloor + 1} \otimes q > 2^{\lfloor \frac{k+1}{2} \rfloor + 1} \Rightarrow N = pq > 2^{2\lfloor \frac{k+1}{2} \rfloor + 2} \geq 2^{k+2}$$

Either case is contradictory to $2^{k+1} < N < 2^{k+2}$. □

Corollary 1. *Let $N = pq$ be a node of T_3 and $(k = \lfloor \log_2 N \rfloor - 1) > 2$, where $1 < p < q$ and $1 < \frac{q}{p} < 2$. Then*

$$\begin{aligned} &(\left\lfloor \sqrt{N} \right\rfloor < 2^{\lfloor \frac{k+1}{2} \rfloor} + 1) \oplus ((\left\lfloor \sqrt{N} \right\rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor} + 1) \otimes (\left\lfloor \sqrt{N} \right\rfloor \nmid N)) \\ &\Rightarrow p \stackrel{\Delta}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 2 \otimes q \stackrel{\Delta}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1 \end{aligned} \tag{9}$$

$$\begin{aligned} &(\left\lfloor \sqrt{N} \right\rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor} + 1) \otimes (\left\lfloor \sqrt{N} \right\rfloor | N) \\ &\Rightarrow (p = 2^{\lfloor \frac{k+1}{2} \rfloor} + 1) \otimes ((q = 2^{\lfloor \frac{k+1}{2} \rfloor} + 1) \oplus (q = 2^{\lfloor \frac{k+1}{2} \rfloor} + 3)) \stackrel{\Delta}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1 \end{aligned} \tag{10}$$

$$\begin{aligned} &(\left\lfloor \sqrt{N} \right\rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1) \otimes (\left\lfloor \sqrt{N} \right\rfloor | N) \\ &\Rightarrow (p = 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1) \stackrel{\Delta}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes ((q = 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1) \oplus (q = 2^{\lfloor \frac{k+1}{2} \rfloor + 1} + 1)) \stackrel{\Delta}{=} \left\lfloor \frac{k+1}{2} \right\rfloor \end{aligned} \tag{11}$$

$$\begin{aligned} &(2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1 < \left\lfloor \sqrt{N} \right\rfloor) \oplus ((\left\lfloor \sqrt{N} \right\rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1) \otimes (\left\lfloor \sqrt{N} \right\rfloor \nmid N)) \\ &\Rightarrow q \stackrel{\Delta}{=} \left\lfloor \frac{k+1}{2} \right\rfloor \otimes p \stackrel{\Delta}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1 \end{aligned} \tag{12}$$

Proof. Since $p \leq \left\lfloor \sqrt{N} \right\rfloor \leq \sqrt{N} \leq q$, it knows $\left\lfloor \sqrt{N} \right\rfloor < 2^{\lfloor \frac{k+1}{2} \rfloor} + 1 \Rightarrow p \leq 2^{\lfloor \frac{k+1}{2} \rfloor}$. Considering that p is odd and $2^{\lfloor \frac{k+1}{2} \rfloor} + 1$ is the smallest node on level $\left\lfloor \frac{k+1}{2} \right\rfloor - 1$, $p \leq 2^{\lfloor \frac{k+1}{2} \rfloor}$ means that p is on level $\left\lfloor \frac{k+1}{2} \right\rfloor - 2$ or higher. By Lemma 2 , $\left\lfloor \sqrt{N} \right\rfloor \stackrel{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1$. This fact and Proposition 4 indicate that q and $\left\lfloor \sqrt{N} \right\rfloor$ are clamped on level $\left\lfloor \frac{k+1}{2} \right\rfloor - 1$, and it must fit $p \stackrel{\Delta}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 2$.

Now consider the case $(\left\lfloor \sqrt{N} \right\rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor} + 1) \otimes (\left\lfloor \sqrt{N} \right\rfloor \nmid N)$. Obviously, the following deduction (13) is surely valid.

$$\begin{aligned} &(p|N) \otimes (p \leq \left\lfloor \sqrt{N} \right\rfloor) \otimes (\left\lfloor \sqrt{N} \right\rfloor \nmid N) \\ &\Rightarrow p < \left\lfloor \sqrt{N} \right\rfloor \Rightarrow p \stackrel{\Delta}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 2 \end{aligned} \tag{13}$$

For the case $\left\lfloor \sqrt{N} \right\rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor} + 1) \otimes (\left\lfloor \sqrt{N} \right\rfloor | N)$, it immediately knows by Lemma 4

$$((q = 2^{\lfloor \frac{k+1}{2} \rfloor} + 1) \stackrel{\Delta}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \oplus ((q = 2^{\lfloor \frac{k+1}{2} \rfloor} + 3) \stackrel{\Delta}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1)$$

Likewise, by Lemma 4 , the case $(\left\lfloor \sqrt{N} \right\rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1) \otimes (\left\lfloor \sqrt{N} \right\rfloor | N)$ yields

$$((p = 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1) \stackrel{\Delta}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \oplus ((q = 2^{\lfloor \frac{k+1}{2} \rfloor + 1} + 1) \stackrel{\Delta}{=} \left\lfloor \frac{k+1}{2} \right\rfloor)$$

For the case $\left\lfloor \sqrt{N} \right\rfloor > 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1$, it knows $q \geq \left\lfloor \sqrt{N} \right\rfloor \geq 2^{\lfloor \frac{k+1}{2} \rfloor + 1}$ that means q is clamped on level $\left\lfloor \frac{k+1}{2} \right\rfloor$ or lower. This time, by Proposition 4 it knows that p and $\left\lfloor \sqrt{N} \right\rfloor$ are clamped on level $\left\lfloor \frac{k+1}{2} \right\rfloor - 1$, and thus $q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor$.

For the case $(\left\lfloor \sqrt{N} \right\rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1) \otimes (\left\lfloor \sqrt{N} \right\rfloor \nmid N)$, the following deduction (14) is surely valid.

$$(q|N) \otimes (p \geq \left\lfloor \sqrt{N} \right\rfloor) \otimes (\left\lfloor \sqrt{N} \right\rfloor \nmid N) \Rightarrow q > \left\lfloor \sqrt{N} \right\rfloor \Rightarrow q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor \tag{14}$$

□

Example 1. Let $N = 4331$; then $k = \lfloor \log_2 N \rfloor - 1 = \lfloor \log_2(4331) \rfloor - 1 = 11$, $\left\lfloor \sqrt{N} \right\rfloor = \left\lfloor \sqrt{4331} \right\rfloor = 65$ and $2^{\lfloor \frac{k+1}{2} \rfloor} + 1 = 2^6 + 1 = 65$. Since $\left\lfloor \sqrt{N} \right\rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor} + 1$ and $\left\lfloor \sqrt{N} \right\rfloor \nmid (N = 4331)$, it yields $p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2 = 4$. Actually, $p = 61 = 2^5 + 2 \times 14 + 1 = N_{(4,14)}$ is a divisor of $N = 4331$.

Example 2. Let $N = 4087$; then $k = \lfloor \log_2 N \rfloor - 1 = \lfloor \log_2(4087) \rfloor - 1 = 10$, $\left\lfloor \sqrt{N} \right\rfloor = \left\lfloor \sqrt{4087} \right\rfloor = 63$ and $2^{\lfloor \frac{k+1}{2} \rfloor} + 1 = 2^6 - 1 = 63$. Since $\left\lfloor \sqrt{N} \right\rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor} + 1$ and $\left\lfloor \sqrt{N} \right\rfloor \nmid (N = 4087)$, it yields $q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor = 5$. Actually, $p = 67 = 2^6 + 2 \times 1 + 1 = N_{(5,1)}$ is a divisor of $N = 4087$.

Example 3. Let $N = 16637$; then $k = \lfloor \log_2 N \rfloor - 1 = \lfloor \log_2(16637) \rfloor - 1 = 13$, $\left\lfloor \sqrt{N} \right\rfloor = \left\lfloor \sqrt{16637} \right\rfloor = 128$ and $2^{\lfloor \frac{k+1}{2} \rfloor} + 1 = 2^7 + 1 = 129$. Since $\left\lfloor \sqrt{N} \right\rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor} + 1$ and $\left\lfloor \sqrt{N} \right\rfloor \nmid (N = 16637)$, it yields $p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2 = 5$. Actually, $p = 127 = 2^6 + 2 \times 31 + 1 = N_{(5,31)}$ is a divisor of $N = 16637$.

Example 4. Let $N = 66049$; then $k = \lfloor \log_2 N \rfloor - 1 = \lfloor \log_2(66049) \rfloor - 1 = 15$, $\left\lfloor \sqrt{N} \right\rfloor = \left\lfloor \sqrt{66049} \right\rfloor = 257$ and $2^{\lfloor \frac{k+1}{2} \rfloor} + 1 = 2^8 + 1 = 257$. Since $\left\lfloor \sqrt{N} \right\rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor} + 1$ and $\left\lfloor \sqrt{N} \right\rfloor | (N = 66049)$, it yields $p = 257$ and $q = 257$.

Example 5. Let $N = 66563$; then $k = \lfloor \log_2 N \rfloor - 1 = \lfloor \log_2(66563) \rfloor - 1 = 15$, $\left\lfloor \sqrt{N} \right\rfloor = \left\lfloor \sqrt{66563} \right\rfloor = 257$ and $2^{\lfloor \frac{k+1}{2} \rfloor} + 1 = 2^8 + 1 = 257$. Since $\left\lfloor \sqrt{N} \right\rfloor = 2^{\lfloor \frac{k+1}{2} \rfloor} + 1$ and $\left\lfloor \sqrt{N} \right\rfloor | (N = 66563)$, it yields $p = 257$ and $q = 259$.

Corollary 2. *Let $N = pq$ be an odd integer and $k = \lfloor \log_2 N \rfloor - 1$, where divisors p and q satisfy $1 < p < q$ and $1 < \frac{q}{p} < 2$; then there are 3 possible cases in term of the levels on which p and q lie, which are given by (15)*

$$\begin{cases} (p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2) \otimes (q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \\ (p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \\ (p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor) \end{cases} \tag{15}$$

Proof. (omit) □

Proposition 5. *Let $N = pq$ be an odd integer and $k = \lfloor \log_2 N \rfloor - 1$, where divisors p and q satisfy $1 < p < q$ and $1 < \frac{q}{p} < \sqrt{2}$; then p and q lie on at most 2 levels of T_3, as shown in (15). Subdivide the interval $[2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 1]$ into 6 subintervals by*

$$\begin{aligned} I_1 &= [2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1, \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \sqrt{2} \right\rfloor + 1) \\ I_2 &= [\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \sqrt{2} \right\rfloor + 1, 2^{\lfloor \frac{k+1}{2} \rfloor} - 1] \\ I_3 &= [2^{\lfloor \frac{k+1}{2} \rfloor} + 1, \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor + 1) \\ I_4 &= [\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1] \\ I_5 &= [2^{\lfloor \frac{k+1}{2} \rfloor + 1} + 1, \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor + 1} \sqrt{2} \right\rfloor + 1) \\ I_6 &= [\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor + 1} \sqrt{2} \right\rfloor + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 1] \end{aligned} \tag{16}$$

then $p \stackrel{\wedge}{=} I_2 \otimes (q \stackrel{\wedge}{=} I_3 \oplus q \stackrel{\wedge}{=} I_4)$ in the case $(p \stackrel{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 2) \otimes (q \stackrel{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1)$, $(p < q) \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$ in the case $(p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1)$ and $p \stackrel{\wedge}{=} I_4 \otimes (q \stackrel{\wedge}{=} I_5 \oplus q \stackrel{\wedge}{=} I_6)$ in the case $(p \stackrel{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (q \stackrel{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor)$.

Proof. Since $1 < \frac{q}{p} < \sqrt{2} < 2$, the first conclusion is directly derived from Corollary 2 . Next is to prove the second conclusion. By Lemma 1(**P3**), it is sure that $(p < q) \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1$ in the case $(p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1)$, thus next is for the other two conditions.

(1). If $(p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2) \otimes (q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1)$, it possibly yields $p \in I_1 \oplus p \in I_2$ and $q \in I_3 \oplus q \in I_4$. The cases $p \in I_1 \otimes q \in I_3$, $p \in I_1 \otimes q \in I_4$, $p \in I_2 \otimes q \in I_3$ and $p \in I_2 \otimes q \in I_4$ are to be checked.

For the case $p \in I_1 \otimes q \in I_3$, $2^{\lfloor \frac{k+1}{2} \rfloor - 1} < p \leq \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \sqrt{2} \right\rfloor$ and $2^{\lfloor \frac{k+1}{2} \rfloor} < q \leq \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor$ lead to

$$\frac{q}{p} > \frac{2^{\lfloor \frac{k+1}{2} \rfloor}}{\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \sqrt{2} \right\rfloor} \geq \frac{2^{\lfloor \frac{k+1}{2} \rfloor}}{2^{\lfloor \frac{k+1}{2} \rfloor - 1} \sqrt{2}} = \sqrt{2}$$

which is contradictory to $1 < \frac{q}{p} < \sqrt{2}$.

For the case $p \in I_1 \otimes q \in I_4$, $2^{\lfloor \frac{k+1}{2} \rfloor - 1} < p \leq \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \sqrt{2} \right\rfloor$ and $\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor < q < 2^{\lfloor \frac{k+1}{2} \rfloor + 1}$ lead to a contradiction to $1 < \frac{q}{p} < \sqrt{2}$ by

$$\frac{q}{p} > \frac{\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor}{\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \sqrt{2} \right\rfloor} \geq \left\lfloor \frac{2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2}}{2^{\lfloor \frac{k+1}{2} \rfloor - 1} \sqrt{2}} \right\rfloor = 2$$

For the case $p \in I_2 \otimes q \in I_3$, $\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \sqrt{2} \right\rfloor < p \leq 2^{\lfloor \frac{k+1}{2} \rfloor}$ and $2^{\lfloor \frac{k+1}{2} \rfloor} < q \leq \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor + 1$ lead to

$$\frac{q}{p} > \frac{2^{\lfloor \frac{k+1}{2} \rfloor}}{2^{\lfloor \frac{k+1}{2} \rfloor}} = 1$$

and

$$\frac{q}{p} < \frac{\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor + 1}{\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \sqrt{2} \right\rfloor} \leq \frac{2^{\lfloor \frac{k+1}{2} \rfloor} (\left\lfloor \sqrt{2} \right\rfloor + 1)}{2^{\lfloor \frac{k+1}{2} \rfloor - 1} \left\lfloor \sqrt{2} \right\rfloor} = 4$$

For the case $p \in I_2 \otimes q \in I_4$, $\left\lfloor 2^{\lfloor \frac{k-1}{2} \rfloor} \sqrt{2} \right\rfloor < p \leq 2^{\lfloor \frac{k-1}{2} \rfloor + 1}$ and $\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor < q < 2^{\lfloor \frac{k+1}{2} \rfloor + 1}$ yield

$$\frac{q}{p} > \frac{\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor}{2^{\lfloor \frac{k+1}{2} \rfloor}} > \frac{2^{\lfloor \frac{k+1}{2} \rfloor} \left\lfloor \sqrt{2} \right\rfloor}{2^{\lfloor \frac{k+1}{2} \rfloor}} = 1$$

and

$$\frac{q}{p} < \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 1}}{\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \sqrt{2} \right\rfloor} \leq \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 1}}{2^{\lfloor \frac{k+1}{2} \rfloor - 1} \left\lfloor \sqrt{2} \right\rfloor} = 4$$

(2). If $(p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor)$, it possibly yields $p \in I_3 \oplus p \in I_4$ and $q \in I_5 \oplus q \in I_6$. The cases $p \in I_3 \otimes q \in I_5$, $p \in I_3 \otimes q \in I_6$, $p \in I_4 \otimes q \in I_5$ and $p \in I_4 \otimes q \in I_6$ are to be checked.

For the case $p \in I_3 \otimes q \in I_5$, $2^{\lfloor \frac{k+1}{2} \rfloor} < p \leq \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor$ and $2^{\lfloor \frac{k+1}{2} \rfloor + 1} < q \leq \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor + 1} \sqrt{2} \right\rfloor$ yield a contradiction to $1 < \frac{q}{p} < \sqrt{2}$ by

$$\frac{q}{p} > \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 1}}{\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor} \geq \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 1}}{2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2}} = \sqrt{2}$$

For the case $p \in I_3 \otimes q \in I_6$, $2^{\lfloor \frac{k+1}{2} \rfloor} < p \leq \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor$ and $\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor + 1} \sqrt{2} \right\rfloor < q < 2^{\lfloor \frac{k+1}{2} \rfloor + 2}$ also yield a contradiction to $1 < \frac{q}{p} < \sqrt{2}$ by

$$\frac{q}{p} > \frac{\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor + 1} \sqrt{2} \right\rfloor}{\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor} \geq \left\lfloor \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 1} \sqrt{2}}{2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2}} \right\rfloor = 2$$

For the case $p \in I_4 \otimes q \in I_5$, $\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor < p < 2^{\lfloor \frac{k+1}{2} \rfloor + 1}$ and $2^{\lfloor \frac{k+1}{2} \rfloor + 1} < q \leq \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor + 1} \sqrt{2} \right\rfloor$ yield

$$\frac{q}{p} > \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 1}}{2^{\lfloor \frac{k+1}{2} \rfloor + 1}} = 1$$

and

$$\frac{q}{p} < \frac{\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor + 1} \sqrt{2} \right\rfloor}{\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor} \leq \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 1} \sqrt{2}}{2^{\lfloor \frac{k+1}{2} \rfloor} \left\lfloor \sqrt{2} \right\rfloor} = 2\sqrt{2}$$

For the case $p \in I_4 \otimes q \in I_6$, $\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor + 1 \leq p < 2^{\lfloor \frac{k+1}{2} \rfloor + 1}$ and $\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor + 1} \sqrt{2} \right\rfloor < q \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 1$ yield

$$\frac{q}{p} > \frac{\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor + 1} \sqrt{2} \right\rfloor}{2^{\lfloor \frac{k+1}{2} \rfloor + 1}} \geq 1$$

and

$$\frac{q}{p} < \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 2}}{\left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor + 1} \leq \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 2}}{2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2}} = 2\sqrt{2}$$

Consequently, $p \triangleq I_2 \otimes (q \in I_3 \oplus q \in I_4)$ fits the condition $(p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 2) \otimes (q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1)$ and $p \triangleq I_4 \otimes (q \triangleq I_5 \oplus q \triangleq I_6)$ fits the condition $(p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor)$.

□

Example 7. Let $N = 4331$, then $k = \lfloor \log_2 N \rfloor - 1 = \lfloor \log_2(4331) \rfloor - 1 = 11$. Subdivision (16) is instanced by

$$\begin{aligned} &I_1 = [33, 45], I_2 = [46, 63], \\ &I_3 = [65, 90], I_4 = [91, 127], \\ &I_5 = [129, 181], I_6 = [182, 255] \end{aligned}$$

By Example 1 it knows $p = 61 \in I_2$ and $q = 71 \in I_3$.

Example 8. Let $N = 16637$, then $k = \lfloor \log_2 N \rfloor - 1 = \lfloor \log_2(16637) \rfloor - 1 = 13$. Subdivision (16) is instanced by

$$\begin{aligned} &I_1 = [65, 90], I_2 = [91, 127], \\ &I_3 = [129, 181], I_4 = [182, 255], \\ &I_5 = [257, 362], I_6 = [363, 511] \end{aligned}$$

By Example 3 it knows $p = 127 \in I_2$ and $q = 131 \in I_3$.

Remark 1. With the help of Mathematica, the subdivision is easily implemented by the following program. When running in Mathematica, changing the parameter k immediately obtains the expected subdivision.

$$\begin{aligned} &I1l[k\_] := 2^{Floor[\frac{k+1}{2}]-1} + 1; \\ &I1r[k\_] := Floor[\sqrt{2} \times 2^{Floor[\frac{k+1}{2}]-1}]; \\ &I2r[k\_] := Floor[\sqrt{2} \times 2^{Floor[\frac{k+1}{2}]-1}] + 1; \\ &I2r[k\_] := 2^{Floor[\frac{k+1}{2}]} - 1; \\ &I3r[k\_] := 2^{Floor[\frac{k+1}{2}]} + 1; \\ &I3r[k\_] := Floor[\sqrt{2} \times 2^{Floor[\frac{k+1}{2}]}]; \\ &I4r[k\_] := Floor[\sqrt{2} \times 2^{Floor[\frac{k+1}{2}]}] + 1; \\ &I4r[k\_] := 2^{Floor[\frac{k+1}{2}]+1} - 1; \\ &I5l[k\_] := 2^{Floor[\frac{k+1}{2}]+1} + 1; \\ &I5r[k\_] := Floor[\sqrt{2} \times 2^{Floor[\frac{k+1}{2}]+1}]; \\ &I6r[k\_] := Floor[\sqrt{2} \times 2^{Floor[\frac{k+1}{2}]+1}] + 1; \\ &I6r[k\_] := 2^{Floor[\frac{k+1}{2}]+2} - 1; \\ &/* the - number - 13 - in - bracket - [] - is - the - k */ \\ &l1 = \{I1l[13], I1r[13]\}; \\ &l2 = \{I2l[13], I2r[13]\}; \\ &l3 = \{I3l[13], I3r[13]\}; \\ &l4 = \{I4l[13], I4r[13]\}; \\ &l5 = \{I5l[13], I5r[13]\}; \\ &l6 = \{I6l[13], I6r[13]\}; \\ &T = \{l1, l2, l3, l4, l5, l6\}//MatrixForm \end{aligned}$$

Proposition 6. *Let* $(N = pq) > 64$ *be an odd integer and* $k = \lfloor \log_2 N \rfloor - 1$*, where divisors* p *and* q *satisfy* $1 < p < q$ *and*

$1 < \frac{q}{p} < \frac{3}{2}$; *Subdivide the interval* $[2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 1]$ *into 6 subintervals by*

$$\begin{aligned} I_1 &= [2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3} + 1) \\ I_2 &= [2^{\lfloor \frac{k+1}{2} \rfloor} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor} - 1] \\ I_3 &= [2^{\lfloor \frac{k+1}{2} \rfloor} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} + 1) \\ I_4 &= [2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1] \\ I_5 &= [2^{\lfloor \frac{k+1}{2} \rfloor + 1} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1) \\ I_6 &= [2^{\lfloor \frac{k+1}{2} \rfloor + 3} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 1] \end{aligned} \tag{17}$$

then $p \triangleq I_2 \otimes (q \triangleq I_3 \oplus q \triangleq I_4)$ *in the case* $(p \triangleq \lfloor \frac{k+1}{2} \rfloor - 2) \otimes (q \triangleq \lfloor \frac{k+1}{2} \rfloor - 1)$, $(p < q) \triangleq \lfloor \frac{k+1}{2} \rfloor - 1$ *in the case* $(p \triangleq \lfloor \frac{k+1}{2} \rfloor - 1) \otimes (q \triangleq \lfloor \frac{k+1}{2} \rfloor - 1)$ *and* $p \triangleq I_4 \otimes (q \triangleq I_5 \oplus q \triangleq I_6)$ *in the case* $(p \triangleq \lfloor \frac{k+1}{2} \rfloor - 1) \otimes (q \triangleq \lfloor \frac{k+1}{2} \rfloor)$.

Proof. $N > 64$ yields $k > 5$ and $\lfloor \frac{k+1}{2} \rfloor - 3 \geq 0$, which is meaningful. Like the proof of Proposition 5 , here merely prove the case $(p \triangleq \lfloor \frac{k+1}{2} \rfloor - 2) \otimes (q \triangleq \lfloor \frac{k+1}{2} \rfloor - 1)$ and case $(p \triangleq \lfloor \frac{k+1}{2} \rfloor - 1) \otimes (q \triangleq \lfloor \frac{k+1}{2} \rfloor)$.

(1). If $(p \triangleq \lfloor \frac{k+1}{2} \rfloor - 2) \otimes (q \triangleq \lfloor \frac{k+1}{2} \rfloor - 1)$, it possibly yields $p \in I_1 \oplus p \in I_2$ and $q \in I_3 \oplus q \in I_4$. The cases $p \in I_1 \otimes q \in I_3$, $p \in I_1 \otimes q \in I_4$, $p \in I_2 \otimes q \in I_3$ and $p \in I_2 \otimes q \in I_4$ are to be checked.

For the case $p \in I_1 \otimes q \in I_3$, $2^{\lfloor \frac{k+1}{2} \rfloor - 1} < p \leq 2^{\lfloor \frac{k+1}{2} \rfloor} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3}$ and $2^{\lfloor \frac{k+1}{2} \rfloor} \leq q < 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2}$ lead to

$$\frac{q}{p} > \frac{2^{\lfloor \frac{k+1}{2} \rfloor}}{2^{\lfloor \frac{k+1}{2} \rfloor} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3}} = \frac{1}{1 - \frac{3}{8}} = \frac{8}{5} > \frac{3}{2}$$

which is contradictory to $1 < \frac{q}{p} < \frac{3}{2}$.

For the case $p \in I_1 \otimes q \in I_4$, $2^{\lfloor \frac{k+1}{2} \rfloor - 1} < p \leq 2^{\lfloor \frac{k+1}{2} \rfloor} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3}$ and $2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} < q < 2^{\lfloor \frac{k+1}{2} \rfloor + 1}$ lead to

$$\frac{q}{p} > \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2}}{2^{\lfloor \frac{k+1}{2} \rfloor} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3}} = 2$$

which is contradictory to $1 < \frac{q}{p} < \frac{3}{2}$, either.

For the case $p \in I_2 \otimes q \in I_3$, $2^{\lfloor \frac{k+1}{2} \rfloor} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3} < p < 2^{\lfloor \frac{k+1}{2} \rfloor}$ and $2^{\lfloor \frac{k+1}{2} \rfloor} < q \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2}$ lead to

$$\frac{q}{p} > \frac{2^{\lfloor \frac{k+1}{2} \rfloor}}{2^{\lfloor \frac{k+1}{2} \rfloor}} = 1$$

and

$$\frac{q}{p} < \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2}}{2^{\lfloor \frac{k+1}{2} \rfloor} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3}} = 2$$

For the case $p \in I_2 \otimes q \in I_4$, $2^{\lfloor \frac{k+1}{2} \rfloor} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3} < p < 2^{\lfloor \frac{k+1}{2} \rfloor}$ and $2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} < q \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1}$ lead to

$$\frac{q}{p} > \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2}}{2^{\lfloor \frac{k+1}{2} \rfloor}} = 2 - 3 \times \frac{1}{4} = \frac{5}{4} > 1$$

and

$$\frac{q}{p} < \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 1}}{2^{\lfloor \frac{k+1}{2} \rfloor} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3}} = \frac{2}{1 - \frac{3}{8}} = \frac{16}{5} = 3.2$$

(2). If $(p \triangleq \lfloor \frac{k+1}{2} \rfloor - 1) \otimes (q \triangleq \lfloor \frac{k+1}{2} \rfloor)$, it possibly yields $p \in I_3 \oplus p \in I_4$ and $q \in I_5 \oplus q \in I_6$. The cases $p \in I_3 \otimes q \in I_5$, $p \in I_3 \otimes q \in I_6$, $p \in I_4 \otimes q \in I_5$ and $p \in I_4 \otimes q \in I_6$ are to be checked.

For the case $p \in I_3 \otimes q \in I_5$, $2^{\lfloor \frac{k+1}{2} \rfloor} < p \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2}$ and $2^{\lfloor \frac{k+1}{2} \rfloor + 1} < q \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1}$ lead to

$$\frac{q}{p} > \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 1}}{2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2}} = \frac{2}{2 - \frac{3}{4}} = \frac{8}{5} > \frac{3}{2}$$

which is contradictory to $1 < \frac{q}{p} < \frac{3}{2}$.

For the case $p \in I_3 \otimes q \in I_6$, $2^{\lfloor \frac{k+1}{2} \rfloor} < p \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2}$ and $2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1} < q < 2^{\lfloor \frac{k+1}{2} \rfloor + 2}$ lead to

$$\frac{q}{p} > \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1}}{2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2}} = 2$$

contradictory to $1 < \frac{q}{p} < \frac{3}{2}$.

For the case $p \in I_4 \otimes q \in I_5$, $2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} < p \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1}$ and $2^{\lfloor \frac{k+1}{2} \rfloor + 1} < q \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1}$ lead to

$$\frac{q}{p} > \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 1}}{2^{\lfloor \frac{k+1}{2} \rfloor + 1}} = 1$$

and

$$\frac{q}{p} < \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1}}{2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2}} = 2$$

For the case $p \in I_4 \otimes q \in I_6$, $2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} < p \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1}$ and $2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1} < q < 2^{\lfloor \frac{k+1}{2} \rfloor + 2}$ lead to

$$\frac{q}{p} > \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1}}{2^{\lfloor \frac{k+1}{2} \rfloor + 1}} = \frac{2 - \frac{3}{4}}{2} = \frac{5}{8}$$

and

$$\frac{q}{p} < \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 2}}{2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1}} = \frac{4}{4 - \frac{3}{2}} = \frac{8}{5}$$

□

Proposition 7. *Let* $(N = pq) > 64$ *be an odd integer and* $k = \lfloor \log_2 N \rfloor - 1$*, where divisors* p *and* q *satisfy* $1 < p < q$ *and* $1 < \frac{q}{p} < 2$*; Subdivide the interval* $[2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 1]$ *into 6 subintervals by*

$$\begin{aligned}
I_1 &= [2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3} + 1) \\
I_2 &= [2^{\lfloor \frac{k+1}{2} \rfloor} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor} - 1] \\
I_3 &= [2^{\lfloor \frac{k+1}{2} \rfloor} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} + 1) \\
I_4 &= [2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1] \\
I_5 &= [2^{\lfloor \frac{k+1}{2} \rfloor + 1} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1) \\
I_6 &= [2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 1]
\end{aligned} \tag{18}$$

then $p \overset{\wedge}{=} I_2 \otimes (q \overset{\wedge}{=} I_3 \oplus q \overset{\wedge}{=} I_4)$ *in the case* $(p \overset{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 2) \otimes (q \overset{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1)$*,* $(p < q) \overset{\Delta}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1$ *in the case* $(p \overset{\Delta}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (q \overset{\Delta}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1)$ *and* $p \overset{\wedge}{=} I_4 \otimes (q \overset{\wedge}{=} I_5 \oplus q \overset{\wedge}{=} I_6)$ *in the case* $(p \overset{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (q \overset{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor)$.

Proof. Like the proof of Proposition 6, here merely prove the case $(p \overset{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 2) \otimes (q \overset{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1)$ and case $(p \overset{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (q \overset{\wedge}{=} \left\lfloor \frac{k+1}{2} \right\rfloor)$.

(1). If $(p \overset{\Delta}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 2) \otimes (q \overset{\Delta}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1)$, it possibly yields $p \in I_1 \oplus p \in I_2$ and $q \in I_3 \oplus q \in I_4$. The cases $p \in I_1 \otimes q \in I_3$, $p \in I_1 \otimes q \in I_4$, $p \in I_2 \otimes q \in I_3$ and $p \in I_2 \otimes q \in I_4$ are to be checked.

For the case $p \in I_1 \otimes q \in I_3$, $2^{\lfloor \frac{k+1}{2} \rfloor - 1} < p \leq 2^{\lfloor \frac{k+1}{2} \rfloor} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3}$ and $2^{\lfloor \frac{k+1}{2} \rfloor} < q \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2}$ lead to

$$\frac{q}{p} > \frac{2^{\lfloor \frac{k+1}{2} \rfloor}}{2^{\lfloor \frac{k+1}{2} \rfloor} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3}} = \frac{1}{1 - \frac{5}{8}} = \frac{8}{3}$$

which is contradictory to $1 < \frac{q}{p} < 2$.

For the case $p \in I_1 \otimes q \in I_4$, $2^{\lfloor \frac{k+1}{2} \rfloor - 1} < p \leq 2^{\lfloor \frac{k+1}{2} \rfloor} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3}$ and $2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} < q < 2^{\lfloor \frac{k+1}{2} \rfloor + 1}$ lead to

$$\frac{q}{p} > \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2}}{2^{\lfloor \frac{k+1}{2} \rfloor} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3}} = 2$$

which is contradictory to $1 < \frac{q}{p} < 2$, either.

For the case $p \in I_2 \otimes q \in I_3$, $2^{\lfloor \frac{k+1}{2} \rfloor} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3} < p < 2^{\lfloor \frac{k+1}{2} \rfloor}$ and $2^{\lfloor \frac{k+1}{2} \rfloor} < q \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2}$ lead to

$$\frac{q}{p} > \frac{2^{\lfloor \frac{k+1}{2} \rfloor}}{2^{\lfloor \frac{k+1}{2} \rfloor}} = 1$$

and

$$\frac{q}{p} < \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2}}{2^{\lfloor \frac{k+1}{2} \rfloor} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3}} = 2$$

For the case $p \in I_2 \otimes q \in I_4$, $2^{\lfloor \frac{k+1}{2} \rfloor} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3} < p < 2^{\lfloor \frac{k+1}{2} \rfloor}$ and $2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} < q < 2^{\lfloor \frac{k+1}{2} \rfloor + 1}$ lead to

$$\frac{q}{p} > \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2}}{2^{\lfloor \frac{k+1}{2} \rfloor}} = 2 - 5 \times \frac{1}{4} = \frac{3}{4}$$

and

$$\frac{q}{p} < \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 1}}{2^{\lfloor \frac{k+1}{2} \rfloor} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3}} = \frac{2}{1 - 5 \times \frac{1}{8}} = \frac{16}{3}$$

(2). If $(p \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor - 1) \otimes (q \triangleq \left\lfloor \frac{k+1}{2} \right\rfloor)$, it possibly yields $p \in I_3 \oplus p \in I_4$ and $q \in I_5 \oplus q \in I_6$. The cases $p \in I_3 \otimes q \in I_5$, $p \in I_3 \otimes q \in I_6$, $p \in I_4 \otimes q \in I_5$ and $p \in I_4 \otimes q \in I_6$ are to be checked.

For the case $p \in I_3 \otimes q \in I_5$, $2^{\lfloor \frac{k+1}{2} \rfloor} < p \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2}$ and $2^{\lfloor \frac{k+1}{2} \rfloor + 1} < q \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1}$ lead to

$$\frac{q}{p} > \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 1}}{2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2}} = \frac{2}{2 - \frac{5}{4}} = \frac{8}{3}$$

which is contradictory to $1 < \frac{q}{p} < 2$.

For the case $p \in I_3 \otimes q \in I_6$, $2^{\lfloor \frac{k+1}{2} \rfloor} < p \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2}$ and $2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1} < q < 2^{\lfloor \frac{k+1}{2} \rfloor + 2}$ lead to

$$\frac{q}{p} > \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1}}{2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2}} = 2$$

contradictory to $1 < \frac{q}{p} < 2$.

For the case $p \in I_4 \otimes q \in I_5$, $2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} < p \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1}$ and $2^{\lfloor \frac{k+1}{2} \rfloor + 1} < q \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1}$ lead to

$$\frac{q}{p} > \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 1}}{2^{\lfloor \frac{k+1}{2} \rfloor + 1}} = 1$$

and

$$\frac{q}{p} < \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1}}{2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2}} = 2$$

For the case $p \in I_4 \otimes q \in I_6$, $2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} < p \leq 2^{\lfloor \frac{k+1}{2} \rfloor + 1}$ and $2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1} < q < 2^{\lfloor \frac{k+1}{2} \rfloor + 2}$ lead to

$$\frac{q}{p} > \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 1}}{2^{\lfloor \frac{k+1}{2} \rfloor + 1}} = 2 - \frac{5}{4} = \frac{3}{4}$$

and

$$\frac{q}{p} < \frac{2^{\lfloor \frac{k+1}{2} \rfloor + 2}}{2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2}} = \frac{4}{2 - \frac{5}{4}} = \frac{16}{3}$$

□

Remark 2. It can prove that the following subdivision (19) is also subordinate to the Proposition 7.

$$\begin{aligned}
I_1 &= [2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor} - 2^{\lfloor \frac{k+1}{2} \rfloor - 2} - 2^{\lfloor \frac{k+1}{2} \rfloor - 3} + 1) \\
I_2 &= [2^{\lfloor \frac{k+1}{2} \rfloor} - 2^{\lfloor \frac{k+1}{2} \rfloor - 2} - 2^{\lfloor \frac{k+1}{2} \rfloor - 3} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor} - 1] \\
I_3 &= [2^{\lfloor \frac{k+1}{2} \rfloor} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 2^{\lfloor \frac{k+1}{2} \rfloor - 1} - 2^{\lfloor \frac{k+1}{2} \rfloor - 2} + 1) \\
I_4 &= [2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 2^{\lfloor \frac{k+1}{2} \rfloor - 1} - 2^{\lfloor \frac{k+1}{2} \rfloor - 2} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 1] \\
I_5 &= [2^{\lfloor \frac{k+1}{2} \rfloor + 1} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 2^{\lfloor \frac{k+1}{2} \rfloor} - 2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1) \\
I_6 &= [2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 2^{\lfloor \frac{k+1}{2} \rfloor} - 2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 1]
\end{aligned} \tag{19}$$

Proposition 8. *Let* $k > 6$, $eI_2^{\sqrt{2}} = \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \sqrt{2} \right\rfloor + 1$, $eI_2^{1.5} = 2^{\lfloor \frac{k+1}{2} \rfloor} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3} + 1$, $eI_2^2 = 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3} + 1$,$eI_4^{\sqrt{2}} = \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor + 1$, $eI_4^{1.5} = 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} + 1$ *and* $eI_4^2 = 2^{\lfloor \frac{k+1}{2} \rfloor + 1} - 5 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} + 1$*; then*

$$\begin{cases} eI_2^{\sqrt{2}} \geq 2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 2^{\lfloor \frac{k+1}{2} \rfloor - 3} + 1 = N_{(\lfloor \frac{k+1}{2} \rfloor - 2, 2\lfloor \frac{k+1}{2} \rfloor - 4)} \\ eI_4^{\sqrt{2}} \geq 2^{\lfloor \frac{k+1}{2} \rfloor} + 2^{\lfloor \frac{k+1}{2} \rfloor - 2} + 1 = N_{(\lfloor \frac{k+1}{2} \rfloor - 1, 2\lfloor \frac{k+1}{2} \rfloor - 3)} \end{cases} \tag{20}$$

and

$$\begin{cases} eI_2^{\sqrt{2}} > eI_2^{1.5} > eI_2^2 \\ eI_4^{\sqrt{2}} > eI_4^{1.5} > eI_4^2 \end{cases} \tag{21}$$

Proof. Direct calculations yields

$$\begin{aligned}
eI_2^{\sqrt{2}} &= \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \sqrt{2} \right\rfloor + 1 \\
&= 2^{\lfloor \frac{k+1}{2} \rfloor - 1} + \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor - 1} (\sqrt{2} - 1) \right\rfloor + 1 \\
&= 2^{\lfloor \frac{k+1}{2} \rfloor - 1} + \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor - 3} \times 4(\sqrt{2} - 1) \right\rfloor + 1 \\
&\geq 2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 2^{\lfloor \frac{k+1}{2} \rfloor - 3} \times \left\lfloor 4(\sqrt{2} - 1) \right\rfloor + 1 \\
&= 2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 2^{\lfloor \frac{k+1}{2} \rfloor - 3} + 1 = N_{(\lfloor \frac{k+1}{2} \rfloor - 2, 2\lfloor \frac{k+1}{2} \rfloor - 4)}
\end{aligned}$$

and

$$\begin{aligned}
eI_4^{\sqrt{2}} &= \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} \sqrt{2} \right\rfloor + 1 \\
&= 2^{\lfloor \frac{k+1}{2} \rfloor} + \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor} (\sqrt{2} - 1) \right\rfloor + 1 \\
&= 2^{\lfloor \frac{k+1}{2} \rfloor} + \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor - 2} \times 4(\sqrt{2} - 1) \right\rfloor + 1 \\
&\geq 2^{\lfloor \frac{k+1}{2} \rfloor} + 2^{\lfloor \frac{k+1}{2} \rfloor - 2} \times \left\lfloor 4(\sqrt{2} - 1) \right\rfloor + 1 \\
&= 2^{\lfloor \frac{k+1}{2} \rfloor} + 2^{\lfloor \frac{k+1}{2} \rfloor - 2} + 1 = N_{(\lfloor \frac{k+1}{2} \rfloor - 1, 2\lfloor \frac{k+1}{2} \rfloor - 3)}
\end{aligned}$$

Hence (20) holds. It is obvious that $\begin{cases} eI_2^{1.5} > eI_2^2 \\ eI_4^{1.5} > eI_4^2 \end{cases}$ holds. So the next proof is merely for $\begin{cases} eI_2^{\sqrt{2}} > eI_2^{1.5} \\ eI_4^{\sqrt{2}} > eI_4^{1.5} \end{cases}$. Direct calculations yield

$$\begin{aligned}
eI_2^{\sqrt{2}} - eI_2^{1.5} &= \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \sqrt{2} \right\rfloor + 1 - 2^{\lfloor \frac{k+1}{2} \rfloor} + 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3} - 1 \\
&= \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \sqrt{2} \right\rfloor - 2^{\lfloor \frac{k+1}{2} \rfloor} + 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3} \\
&> 2^{\lfloor \frac{k+1}{2} \rfloor - 1} \sqrt{2} - 1 - 2^{\lfloor \frac{k+1}{2} \rfloor} + 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 3} \\
&= 2^{\lfloor \frac{k+1}{2} \rfloor} (\tfrac{\sqrt{2}}{2} - 1 + \tfrac{3}{8}) - 1 \\
&= 2^{\lfloor \frac{k+1}{2} \rfloor - 3} (4\sqrt{2} - 5) - 1
\end{aligned}$$

Since $\sqrt{2} > 1 + \frac{1}{2} - \frac{1}{4} + \frac{1}{8}$, it holds

$$eI_2^{\sqrt{2}} - eI_2^{1.5} > 2^{\lfloor \frac{k+1}{2} \rfloor - 3}(4\sqrt{2} - 5) - 1 > 2^{\lfloor \frac{k+1}{2} \rfloor - 3}(4 \times (1 + \frac{1}{2} - \frac{1}{4} + \frac{1}{8}) - 5) - 1 = 2^{\lfloor \frac{k+1}{2} \rfloor - 4} - 1$$

Similarly, when $k > 6$ it yields

$$\begin{aligned}
&eI_4^{\sqrt{2}} - eI_4^{1.5} = \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor}\sqrt{2} \right\rfloor + 1 - 2^{\lfloor \frac{k+1}{2} \rfloor + 1} + 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} - 1 \\
&= \left\lfloor 2^{\lfloor \frac{k+1}{2} \rfloor}\sqrt{2} \right\rfloor - 2^{\lfloor \frac{k+1}{2} \rfloor + 1} + 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} \\
&> 2^{\lfloor \frac{k+1}{2} \rfloor}\sqrt{2} - 1 - 2^{\lfloor \frac{k+1}{2} \rfloor + 1} + 3 \times 2^{\lfloor \frac{k+1}{2} \rfloor - 2} \\
&= 2^{\lfloor \frac{k+1}{2} \rfloor + 1}(\tfrac{\sqrt{2}}{2} - 1 + \tfrac{3}{8}) - 1 \\
&= 2^{\lfloor \frac{k+1}{2} \rfloor - 2}(4\sqrt{2} - 5) - 1 > 1
\end{aligned}$$

□

The relationships described in Proposition 8 can be intuitionally illustrated with figure 1. In the figure, $I_2^{\sqrt{2}}$,$I_2^{1.5}$ and I_2^2 are lengths of the second subintervals subdivided with (16), (17) and (18), respectively.

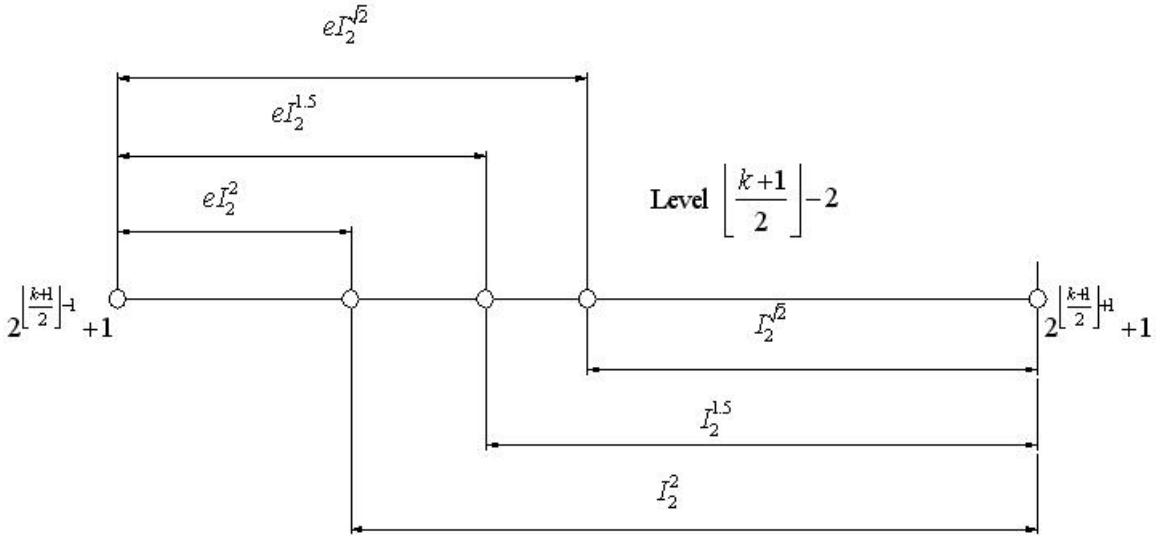

Figure 1. $eI_2^{\sqrt{2}} > eI_2^{1.5} > eI_2^2$ vs. $I_2^{\sqrt{2}} < I_2^{1.5} < I_2^2$ on level $\left\lfloor \frac{k+1}{2} \right\rfloor - 2$

Theorem 1. *Let* $(N = pq) > 128$ *be an odd integer and* $k = \lfloor \log_2 N \rfloor - 1$*, where divisors* p *and* q *satisfy* $1 < p < q$ *and* $1 < \frac{q}{p} = \alpha < 2$*; then there always exists a subdivision of the interval* $[2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 1]$ *into 6 subintervals* I_1, I_2, I_3, I_4, I_5 *and* I_6 *that satisfy*

$$[2^{\lfloor \frac{k+1}{2} \rfloor - 1} + 1, 2^{\lfloor \frac{k+1}{2} \rfloor + 2} - 1] = I_1 \cup I_2 \cup I_3 \cup I_4 \cup I_5 \cup I_6 \tag{22}$$

by means of which holds one of the three cases, $p \stackrel{\wedge}{=} I_2 \otimes (q \stackrel{\wedge}{=} I_3 \oplus q \stackrel{\wedge}{=} I_4)$, $(p < q) \stackrel{\Delta}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1$ *and* $p \stackrel{\wedge}{=} I_4 \otimes (q \stackrel{\wedge}{=} I_5 \oplus q \stackrel{\wedge}{=} I_6)$.

Proof. The subdivision (16) is applicable if $1 < \alpha < \sqrt{2}$, the subdivision (17) is applicable if $\sqrt{2} < \alpha < \frac{3}{2}$, and the subdivision (18) or (19) is applicable if $\frac{3}{2} < \alpha < 2$. □

The three cases mentioned in Theorem 1 can be intuitionally depicted with figure **??**. In the figure, (a) is for the case $p \stackrel{\wedge}{=} I_2 \otimes (q \stackrel{\wedge}{=} I_3 \oplus q \stackrel{\wedge}{=} I_4)$, (b) is for the case $(p \leq \sqrt{N} \leq q) \stackrel{\Delta}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1$ and (c) is for the case $p \stackrel{\wedge}{=} I_4 \otimes (q \stackrel{\wedge}{=} I_5 \oplus q \stackrel{\wedge}{=} I_6)$.

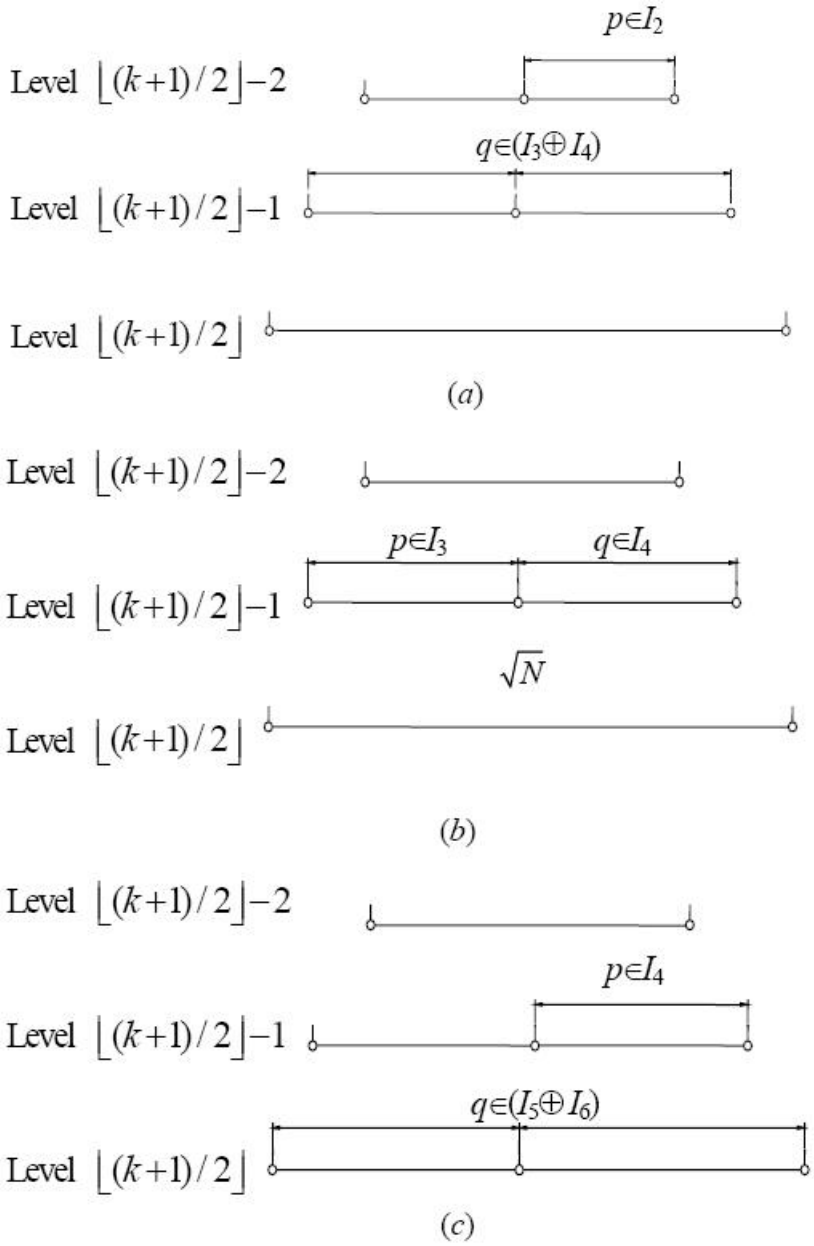

Figure 2. (*a*) $p \stackrel{\wedge}{=} I_2 \otimes (q \stackrel{\wedge}{=} I_3 \oplus q \stackrel{\wedge}{=} I_4)$; (*b*) $(p \leq \sqrt{N} \leq q) \stackrel{\Delta}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1$; (*c*) $(p \leq \sqrt{N} \leq q) \stackrel{\Delta}{=} \left\lfloor \frac{k+1}{2} \right\rfloor - 1$

4. Conclusion

Factorization of the RSA numbers has been a challenge for researchers working in the field of cryptography as well as the field of number theory. Investigation shows, the two divisors of a RSA number may lie on at most two adjacent levels, and the smaller their divisor-ratio is the closer they are. This trait indicates a direction for researcher to design algorithm to factorize the RSA numbers. The Theorem 1 shows that, for a divisor-ratio $1 < q/p < 2$ of odd interger $N = pq$, there is always a subdivision around level $\left\lfloor \frac{k+1}{2} \right\rfloor - 1$ with which p and q are located. Readers can see that, the subdivisions presented in this paper are not so refinery, hence a refinery subdivision is still worthy of seeking in the future work. Hope it is obtained soon.

Acknowledgements

The research work is supported by the State Key Laboratory of Mathematical Engineering and Advanced Computing under Open Project Program No.2017A01, the Youth Innovative Talents Project (Natural Science) of Education Department of

Guangdong Province under grant 2016KQNCX192, 2017KQNCX230. The authors sincerely present thanks to them all.

References

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

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

WANG, X. B. (2016). Valuated binary tree: a new approach in study of integers, *International Journal of Scientific and Innovative Mathematical Research*, *4*(3), 63-67.

WANG, X. B. (2016). Amusing properties of odd numbers derived from valuated binary tree, *IOSR Journal of Mathematics*, *12*(6), 53-57.

WANG, X. B. (2017). Genetic traits of odd numbers with applications in factorization of integers, *Global Journal of Pure and Applied Mathematics*, *13*(2), 493-517.

WANG, X. B. (2017). Two more symmetric properties of odd numbers, *IOSR Journal of Mathematics*, *13*, 3-ver.II, 37-40.

WANG, X. B. (2018). T_3 tree and its traits in understanding integers, *Advances in Pure Mathematics*, *8*(5), 494-507.

WANG, X. B. (2018). Some inequalities on T_3 tree,*Advances in Pure Mathematics*, *8*(8), 711-719.

WANG, X. B. (2018). More on square and square root of a node on T_3 tree,*International Journal of Mathematics and Statistics Study*, *6*(3), 1-7.

CHEN, G. H., & LI, J. H. (2018). Brief investigation on square root of a node of T_3 tree, *Advances in Pure Mathematics*, *8*(7), 666-671.

FU, D. B. (2017). A parallel algorithm for factorization of big odd numbers, *IOSR Journal of Computer Engineering*, *19*, 2-Ver.V, 51-54.

LI, J. H. (2018). A parallel probabilistic approach to factorize a semiprime, *American Journal of Computational Mathematics*, *8*(2), 153-162.

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

WANG, X. B. (2018). Some new inequalities with proofs and comments on applications,*Journal of Mathematics Research*, *11*(3), 15-19.

Copyrights