Connections on Valuated Binary Tree and Their Applications in Factoring Odd Integers

Xingbo Wang1, Jinfeng Luo1, Ying Tian1 and Li Ma2

1Department of Mechatronic Engineering, Foshan University, Foshan City, China.
2Department of Electronic and Information Engineering, Foshan University, Foshan City, China.

Authors’ contributions

This work was carried out in collaboration among all authors. Author XW is in charge of theory and proof. Authors JL and YT are in charge of programming test. Author LM is in charge of other work. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/ARJOM/2021/v17i330287

Received 25 March 2021
Accepted 31 May 2021
Published 01 June 2021

Abstract

This paper makes an investigation on geometric relationships among nodes of the valuated binary trees, including parallelism, connection and penetration. By defining central lines and distance from a node to a line, some intrinsic connections are discovered to connect nodes between different subtrees. It is proved that a node out of a subtree can penetrate into the subtree along a parallel connection. If the connection starts downward from a node that is a multiple of the subtree’s root, then all the nodes on the connection are multiples of the root. Accordingly composite odd integers on such connections can be easily factorized. The paper proves the new results with detail mathematical reasoning and demonstrates several numerical experiments made with Maple software to factorize rapidly a kind of big odd integers that are of the length from 59 to 99 decimal digits. It is once again shown that the valuated binary tree might be a key to unlock the lock of the integer factorization problem.

Keywords: Integer factorization; valuated binary tree; parallel lines; connection.
2020 Mathematics Subject Classification: 11A51, 11Y99.

1 Introduction

The idea using binary tree to study odd integers bigger than 1 was first put forward in WANG’s paper [1]. In that paper and its following studies, many new properties were discovered. For example, articles [2] and [3] discovered the properties of symmetric nodes and symmetric common divisors, article [4] disclosed the genetic properties of odd integers, and article [5] demonstrated the periodical divisibility traits along the leftmost path or the left side-path of the tree. All these new properties enable people to know the integers in a different point of view, as stated and investigated in paper [6].

Based on the new properties, fast approaches to factorize odd integers are disclosed. For example, article [7] presented an algorithm of \(O(\log_2 N)\) searching steps (or \(O((\log_2 N)^3)\) bit operations) to factorize an odd integer \(N = pq\) with the divisor \(q\) being of the form \(2^u + 1\) or \(2^v - 1\) and the divisor \(p\) satisfying \(1 < p \leq 2^u + 1\) or \(2^v < p \leq 2^u - 1\). Article [8] exhibited a fast approach to factorized big Fermat numbers, and article [9] introduced a method to estimate the divisors’ bounds for semiprimes or RSA numbers. Thereby, it is reasonable to believe that valuated binary tree might be a key to unlock the lock of the integer factorization problem.

It is undoubted that knowing the distribution of all the multiples of an odd integer \(p\) bigger than 1 is surely helpful to factorize a composite odd integer that has \(p\) as a divisor. Under description of the valuated binary tree, say \(T_p\), the distribution of the multiples of the root \(p\) is critically important, as investigated in articles [4,5,6] and [7]. When a multiple, say \(m = ap\) with odd integer \(a > 1\) and \((a, p) = 1\), lies in the tree \(T_p\), \(m\) is very easy to be factorized by \(p = \gcd(m, p)\) because tracing upwards from \(m\) by \(\log_2 a\) steps reaches \(p\). Since unfortunately \(m\) is out of \(T_p\) in most cases, the research topic is naturally brought out on how to make \(m\) be related with an inner descendant of \(T_p\). This paper does such a research. The paper first defines several metric relations on the valuated binary tree from the point of view of geometry, then finds out the converting relations from an outer node to an inner node of a tree, and in the end the paper proves that there are a special kind of odd integers that can be factorized in \(O(\log_2 N)\) searching steps.

The paper is composed of five parts. The first is this introductory part, the second cites some old related preliminaries, the third gives some new definitions, the fourth presents new theorems together with their proof, and the last part introduces factorization of the special kind of odd integers.

2 Preliminaries

This section cites some definitions, notations and lemmas that have been defined, introduced or proved in the related previous publications that are necessary for later descriptions. Also, some new conclusions with their simple proofs are placed here.

2.1 Definitions and notations

A valuated binary tree \(T\) is a perfect full binary tree that each of its nodes is assigned a value. The terms binary tree and its root, nodes, father, left-son, right-son as well as subtrees can be seen in school-books of data structure, for example, Dinesh’s handbook [10] (Dinesh P. Mehta, Sartaj Sahni, 2005). Let \(N\) be an odd integer bigger than 1; an \(N\)-rooted tree, denoted by \(T_N\) is a recursively constructed valuated binary tree whose root is the odd number \(N\) with \(2N-1\) and \(2N+1\) being the root’s left and right sons, respectively. Each son is connected with its father with a path, but there is no path between the two sons. The father, grandfather and so forth are called direct ancestors; accordingly a path connecting a node with its direct ancestor or descendant is called a direct path, and it either starts or ends at the root. The number of nodes on a path is the length of the path. Nodes on the same level are brothers. \(T_3\) tree is the case \(N=3\). For convenience, symbol \(N_{(i,j)}\) is by default the node at position \(j\) on level \(k\) of \(T_3\), where \(k \geq 0\) and \(0 \leq j \leq 2^k - 1\). An odd integer bigger than 1 is regarded to be a node
of a certain valuated binary tree. Symbol \( N_{(k,j)}^x \) is to denote the node at position \( j \) on level \( k \) of \( T_x \), where \( k = 0,1,\ldots \) and \( j = 0,1,\ldots,2^k - 1 \). When the index \( j \) is out of the range \( 0 \leq j \leq 2^k - 1 \), for example, \( j = -2, -1 \) or \( j = 2^k, 2^k + 1 \), \( N_{(k,j)}^x \) is called an outer-node of \( T_x \). Symbol \( x \in T_x \) means node \( x \) is a node of \( T_x \) while symbol \( x \not\in T_x \) means \( x \) is not a node of \( T_x \). Symbol \( x \in l(T_x) \) means node \( x \) is in the left branch of \( T_x \) while symbol \( x \in r(T_x) \) means node \( x \) is in the right branch of \( T_x \). Symbol \( A_x \) is \( X \)'s direct ancestor that is \( a \) levels over \( X \). A walk of a node \( N_{(k,j)}^x \) means an operation on either the index \( k \) or \( j \), for example, \( N_{(k,a+e,j)}^x, N_{(k,j+\omega)}^x \) and \( N_{(k,a+e,j+\omega)}^x \) are all results from the walk of \( N_{(k,j)}^x \). A tracing step or a searching step is the computation of a father based on a son or vice versa, or a node to its adjacent brother.

Symbol \( A \Rightarrow B \) means result \( B \) is derived from condition \( A \) or \( A \) can derive \( B \) out. In this whole article, symbol \( \lfloor x \rfloor \) denotes the floor function, an integer function of the real number \( x \) such that \( x - 1 < \lfloor x \rfloor \leq x \) or equivalently \( \lfloor x \rfloor \leq x < \lfloor x \rfloor + 1 \). Article [11] collected most necessary properties to refer. An odd interval \([a,b]\) is a set of consecutive odd numbers that take \( a \) as lower bound and \( b \) as upper bound. Intervals in this whole article are by default the odd ones unless particularly mentioned. Symbol \( Z^+ \) is the set of positive integers.

### 2.2 Lemmas

**Lemma 1.** [1,5,12]. The \( T_j \) Tree has the following fundamental properties.

(P1). Every node is an odd integer and every odd integer bigger than 1 must be a node of the tree. Odd integer \( N \) with \( N > 1 \) lies on level \( \lceil \log_2 N \rceil - 1 \). On the same level, there is not a node that is a multiple of another one.

(P2). \( N_{(k,j)}^x \) is calculated by

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

(P3) Nodes \( N_{(k+1,j,2)}^x \) and \( N_{(k+1,2,j+1)}^x \) on the \((k+1)\)th level are respectively left son and right son of node \( N_{(k,j)}^x \) on the \( k \)th level. The descendants of \( N_{(k,j)}^x \) on the \((k+i)\)th level with \( i \geq 0 \) are \( N_{(k+i,2^{i-1}+j,2)}^x \) \((0 \leq \omega \leq 2^i - 1)\), which are

\[
N_{(k+i,2^{i-1}+j,2)}^x, N_{(k+i,2^{i-1}+j+1,2)}^x, \ldots, N_{(k+i,2^{i-1}+j+2^i-1,2)}^x
\]

(P4) For given \( N_{(k,j)}^x \in T_x \), it holds

\[
N_{(k,j)}^x + 2^{k-1}(2^k - 1) + 2\omega = N_{(i,j+\omega)}^x
\]

and

\[
N_{(k,j)}^x + 2^{k-1}(2^k - 1) - 2\theta = N_{(i,j-\theta)}^x
\]

where integers \( \sigma \geq 0 \), \( \omega \) and \( \theta \) satisfy \( 0 \leq \omega \leq 2^{k-\sigma} - 1 - j \) and \( 0 \leq \theta \leq j \).

**Lemma 2.** [1,5,12]. Let \( T \) be \( X \)-rooted binary tree. Then

(P1) On level \( k \) with \( k = 0,1,\ldots \), there are \( 2^k \) nodes. On the same level, there is not a node that is a multiple of another one.
(P2) Node $N^X_{(k,j)}$ is computed by

$$N^X_{(k,j)} = 2^k X - 2^j + 2j + 1; k = 0, 1, 2, \ldots; j = 0, 1, \ldots, 2^k - 1$$

(P3) Let $p$ be an odd integer bigger than 1 and $p = N^X_{(k,j)}$; then $N^p_{(\omega,0)}$ of $T_p$ $(0 \leq \ell; 0 \leq \omega \leq 2^\ell - 1)$ is corresponding to node $N^X_{(k+2^\ell+2, j+\omega)}$ of $T_j$, namely, $N^p_{(\omega,0)} = N^X_{(k+2^\ell+2, j+\omega)}$.

(P4) For $T_j$ and integer $k \geq 0$, it holds

$$N^X_{(k+2^\ell+1, 2^\omega+1)} = N^X_{(k+2^\ell+1, 2^\omega+2)} \pm 2^k X$$

and

$$N^X_{(k+2^\ell+2, 2^\omega+1)} = N^X_{(k+2^\ell+2, 2^\omega+2)} \pm 2^k X$$

where $\omega$ is an integer satisfying $0 \leq \omega \leq 2^{[\log_2 X] - 1}$ and the $\pm$ symbols are mandatory to be the same in the corresponding terms, namely, one term taking $+$ requires the other terms to take $+$, or vice versa.

Lemma 3. Suppose $N > 1$ is an odd integer; then $N = N^X_{(k,j)}$ in $T_j$ with $k = \lfloor \log_2 N \rfloor - 1$ and $j = \frac{N-1}{2} - 2^{\lfloor \log_2 N \rfloor - 1}$. Accordingly, $n = aN$ with $a \geq 1$ being an odd integer lies on $k + \lfloor \log_2 a \rfloor + 1$.

Proof. By Lemma 1(P1), $p$ lies on level $\lfloor \log_2 p \rfloor - 1$. Let $p = 2^{j+1} + 2j + 1$; then $j = \frac{p-1}{2} - 2^k$. Thereby, $n = aN$ lies on level $k = \lfloor \log_2 aN \rfloor - 1$. By properties of the floor function it holds

$$k + \lfloor \log_2 a \rfloor = \lfloor \log_2 a \rfloor + \lfloor \log_2 N \rfloor - 1 \leq k = k + 1 + \lfloor \log_2 a \rfloor$$

3 Geometric Relationships on a Tree

By definition, a valuated binary tree consists of nodes and paths connecting sons with fathers and so forth with the direct ancestors. Geometrically, nodes are considered to place with rows and columns. For example, the first five rows of a valuated binary tree $T$ can be either one of the two layouts illustrated in Fig. 1.

![Fig. 1. Different layouts of a tree](image)
A row is conventionally called a level while a column has no alternative new name. By definition, there is a gap between two nodes. When the gap between arbitrary two adjacent levels is the same as that between arbitrary two adjacent columns, the tree is an equal-distanced tree. The equal-distanced tree is by default supposed in scientific research however it is usually drawn to layout in an isosceles triangle, as seen in Fig. 2. It can be seen that nodes are in parallel distribution from level to level and from column to column. Except for the parallelism, there are other geometric relationships on a valuated binary tree, as introduced next.

### 3.1 Central lines and connections

Suppose \( p > 1 \) is an odd integer and \( T_p \) is the \( p \)-rooted valuated binary tree; let \( C_l = \{N^p_{(0,0)}, N^p_{(1,1)}, N^p_{(2,3)}, \ldots, N^p_{(k,2^k-3)}, \ldots\} \) and \( C_r = \{N^p_{(1,1)}, N^p_{(2,2)}, N^p_{(3,3)}, \ldots, N^p_{(k,2^k-1)}, \ldots\} \); then the path connecting nodes in \( C_l \) is defined to be a left central line and the path connecting nodes in \( C_r \) is defined to be a right central line, as shown in Fig. 2(a). In \( T_p \), the root \( p = N^p_{(0,0)} \) is regarded to be the end of both \( C_l \) and \( C_r \). On a level \( k > 0 \), the number of nodes between node \( N^p_{(k,1)} \) and \( N^p_{(a,2^b-1)} \) is defined to be the distance from \( N^p_{(k,1)} \) to \( C_l \). Statement that \( A \) is \( d \) away from \( B \) means \( d \) is the distance between node \( A \) and \( B \). The number of nodes on an entire level is a span of the tree on the level. A connection is a virtual (imaginary) path (line) to connect two nodes between which there is no direct path. For example, connect two nodes that have the same distance to \( C_l \), as shown in Fig. 2(b). Connections can connect nodes both inside and outside of a tree. A connection on which all the nodes have the same distance to \( C_l \) is a parallel connection of \( C_l \). Distance to \( C_l \) and parallel connections of \( C_l \) can be defined likewise. Fig. 2 illustrates \( C_l, C_r \) and a connection. The number of nodes on a connection is the length of the connection.

![Fig. 2. Left-center line and right-center line](image)

### 3.2 Trace and penetration

Lemma 1 (P1) indicates that, for an arbitrary odd integer \( N \geq 3 \), \( T_N \) is a subtree of \( T_3 \). Obviously, \( T_N \) and \( T_3 \) are two distinct subtrees if two odd integers \( X \) and \( Y \) satisfying \( X > 3 \), \( Y > 3 \) and \( X \neq Y \). Accordingly, for a subtree \( T_N \) with \( X > 3 \), a node \( x \in T_N \) might be \( x \in T_3 \) or \( x \notin T_3 \). When \( x \notin T_3 \), it can walk into \( T_3 \). For this reason, in later statements of the paper, the root of a subtree is by default bigger than 3 unless it is particularly declared. By definition, a walk can go along a path, a connection, or a combination of them. The ordered array of all paths and connections for a walk forms a trace and the number of non-repeat nodes on a trace is the length of the trace. For example, if walking into subtree \( T_{33} \), illustrated in Fig. 3, node \( N_{1,0} \) can have at least four selective decisions:

(1) Along trace \( N_{1,0} \rightarrow N_{0,0} \rightarrow N_{1,1} \) that is combined of path \( N_{1,0} \rightarrow N_{0,0} \) and path \( N_{0,0} \rightarrow N_{1,1} \);
(2) Along trace (connection) \( N_{1,0} \rightarrow N_{1,1} \);
(3) Along trace (connection) \( N_{0,0} \rightarrow N_{0,0} \);
(4) Along trace (connection) \( N_{0,0} \rightarrow N_{0,0} \).
(3) Along trace (connection) $N_{1,0} \rightarrow N_{2,1}$;
(4) Along trace $N_{1,0} \rightarrow N_{2,1} \rightarrow N_{2,1}$ that is combined of path $N_{1,0} \rightarrow N_{2,1}$ and connection $N_{2,1} \rightarrow N_{2,1}$.

![Fig. 3. Traces of a walk](image)

If the trace of a walk is parallel to $C_l$ or $C_r$ of a tree, the walk is a parallel walk. A penetration is a walk whose trace has the shortest length. Obviously the penetration of a node into a tree is worth to investigate because it concerns something with the optimal problems of finding a shortest path.

4 Main Results and Proofs

**Property 1.** In any valued binary tree, $C_l$ and $C_r$ are in perpetuity parallel to each other.

**Proof.** By definition, the distance between $C_l$ and $C_r$ is in perpetuity 2.

**Property 2.** In $T_3$, a connection that starts downwards from $N_{(k,j)} (k > 0, 0 \leq j \leq 2^k - 1)$ and connects the node $N_{(k+1,j(2^{k-1}+1))}$ with $i \geq 0$ is parallel to $C_l$ and $C_r$.

**Proof.** The condition $k > 0$ and $0 \leq j \leq 2^k - 1$ is mandatory because $C_l$ starts downwards from $N_{(1,0)}$. Now consider the case that $N_{(k,j)}$ is on the left of $C_l$. Direct calculation shows that, the distances from $N_{(k,j)}$ to $C_l$ and $C_r$ are respectively

$$d'_l = \frac{N_{(k,2^k+j)} - N_{(k,0)}}{2} + 1 = 2^{k-1} - j$$

and

$$d'_r = \frac{N_{(k,2^k+j)} - N_{(k,0)}}{2} + 1 = 2^{k-1} - j + 1$$

Since the distances from $N_{(k+1,j(2^{k-1}+1))}$ to $C_l$ and $C_r$ are respectively...
\[ d'_{k,i} = \frac{N_{(k+1,2^{i}+1)} - N_{(k+1,2^{i}+2)}}{2} + 1 = 2^{k-1} - j \]

and

\[ d'_{k,i} = \frac{N_{(k+1,2^{i+1})} - N_{(k+1,2^{i+2})}}{2} + 1 = 2^{k-1} - j + 1 \]

the property surely holds.

For the case \( N_{(k,j)} \) is on the right of \( C_r \), it holds

\[ d'_k = \frac{N_{(k,j)} - N_{(k,2^{i}+1)}}{2} + 1 = j - 2^{k-1} + 1 \]

\[ d'_k = \frac{N_{(k,j)} - N_{(k,2^{i+1})}}{2} + 1 = j - 2^{k-1} \]

\[ d'_{k,i} = \frac{N_{(k+1,2^i(2^i+2)^i)} - N_{(k+1,2^i(2^i+2)^i+1)}}{2} + 1 = j - 2^{k-1} + 1 \]

\[ d'_{k,i} = \frac{N_{(k+1,2^i(2^i+2)^i+1)}}{2} + 1 = j - 2^{k-1} \]

Thereby the property holds.

**Property 3.** Let \( p > 3 \) be an odd integer and \( T_p \) be the \( p \)-rooted valuated binary tree with \( C_L \) and \( C_R \) being the left and right central lines respectively; the connection that starts downwards from \( N^p_{(k,j)} (k > 0, 0 \leq j \leq 2^{k-1} - 1) \) and connects the node \( N^p_{(k+1,2^i(2^i+2)^i+1)} \) with \( i \geq 0 \) is parallel to \( C_L \) and \( C_R \), as illustrated in Fig. 4.

![Fig. 4. Connection parallel to C_L and C_R](image-url)
Proof. Referring to the proof of Property 2, there are two cases to be considered. One is the case that $N_{(k,j)}^p$ is on the left of $C_r$ and the other is the case $N_{(k,j)}^p$ is on the right of $C_r$. For the case that $N_{(k,j)}^p$ is on the left of $C_r$, direct calculation shows that, the distances from $(k,j)N$ to $C_l$ and $C_r$ are respectively

$$d_l = \frac{N_{(k,j)}^p - N_{(k,j)}^{p-1}}{2} + 1 = 2^{k-1} - j$$

$$d_r = \frac{N_{(k,j)}^p - N_{(k,j)}^{p-1}}{2} + 1 = 2^{k-1} - j + 1$$

and the distances from $N_{(k+1,2^{k+1}-2)}$ to $C_l$ and $C_r$ are respectively

$$d_{l,i} = \frac{N_{(k,i)}^p - N_{(k,i)}^{p-1}}{2} + 1 = 2^{k-1} - j$$

$$d_{r,i} = \frac{N_{(k,i)}^p - N_{(k,i)}^{p-1}}{2} + 1 = 2^{k-1} - j + 1$$

Likewise, the case $N_{(k,j)}^p$ is on the right of $C_r$ can be shown by following calculations.

$$d_l = \frac{N_{(k,j)}^p - N_{(k,j)}^{p-1}}{2} + 1 = j - 2^{k-1} + 1$$

$$d_r = \frac{N_{(k,j)}^p - N_{(k,j)}^{p-1}}{2} + 1 = j - 2^{k-1}$$

$$d_{l,i} = \frac{N_{(k,i)}^p - N_{(k,i)}^{p-1}}{2} + 1 = j - 2^{k-1} + 1$$

$$d_{r,i} = \frac{N_{(k,i)}^p - N_{(k,i)}^{p-1}}{2} + 1 = j - 2^{k-1}$$

Hence the property holds.

Remark 1. Property 2 and Property 3 are of the same essence because taking $p=3$ in Property 3 immediately yields Property 2.

Property 4. Let $p \geq 3$ be an odd number and $T_p$ be the p-rooted valuated binary tree with $C_l$ and $C_r$ being the left and right central lines respectively; suppose $n = N_{(k,j)}^p \in T_p$ such that $\lfloor \log_2 n \rfloor - \lfloor \log_2 p \rfloor \geq 0$ and is $d_1(n)$ away from $C_r$. Then the connection $L_n$ starting downwards from $n$ and parallel to $C_r$, as is illustrated with Fig. 5, passes through $N_{(l,2^{k+1}+d_1)}^p$ if $n$ is on the left of $C_r$ whereas it passes through $N_{(l,2^{k+1}+d_1(n)-2)}^p$ if $n$ is on the right of $C_r$, where integer $i \geq 1$ and the node $N_{(l,2^{k+1}+d_1(n)})^p$ or $N_{(l,2^{k+1}+d_1(n)-2)}^p$ might be a virtual one.
Fig. 5. Nodes of $T_p$ on connection from $T_3$ to $T_p$

**Proof.** Let $k_n = \lfloor \log_2 n \rfloor - 1$ and $k_p = \lfloor \log_2 p \rfloor - 1$ be respectively the levels of $T_3$ where $n$ and $p$ lie. The condition $\lfloor \log_2 n \rfloor - \lfloor \log_2 p \rfloor \geq 0$ means $n$ lies on the same level as $p$ lies or on a lower level.

Since $L_n$ starts downwards from level $k_n$ of $T_3$, it is sure $i \geq 1$ if node $N_{(i,p)} \in T_p$ is on $L_n$.

Now referring to the proof of Property 3, it is seen that, for the case $n$ is on the left of $C_i$, the node $x \in T_p$ that is on level $i$ and is $d_i(n)$ away from $C_i$ satisfies

$$N_{(i,x^{i+1-1})} - x \over 2 + 1 = d_i(n)$$

That is

$$x = N_{(i,x^{i+1-1})} - 2(d_i(n) - 1) = N_{(i,x^{i+1-1})} - d_i(n)$$

Likewise, for the case $n$ is on the right of $C_i$, the node $y \in T_p$ that is $d_i(n)$ away from $C_i$ satisfies

$$y = N_{(i,x^{i+1-1})} + 2(d_i(n) - 1) = N_{(i,x^{i+1-1})} + d_i(n) - 2$$

Namely

$$y = N_{(i,x^{i+1-1})} + 2(d_i(n) - 1) = N_{(i,x^{i+1-1})} + d_i(n) - 2$$

**Property 5.** Let $p > 3$ be an odd number and $T_p$ be the $p$-rooted valuated binary tree with $C_l$ and $C_r$ being the left and right central lines respectively; Given a node $n$ of $T_3$ satisfying $\lfloor \log_2 n \rfloor - \lfloor \log_2 p \rfloor \geq 0$; suppose $L_n$ is the connection starting downward from $n$ and parallel to $C_l$ and $C_r$, as is illustrated with Fig. 6; then after penetrating at most $\lfloor \log_2 n \rfloor - 1$ levels, $L_n$ goes into $T_p$. 
Proof. Let $k_p$ and $k_n$ be the levels where $p$ and $n$ lies in $T_3$; denote $d_l(n)$ and $d_r(n)$ to be the distances from $n$ to $C_l$ and $C_r$ respectively. Consider the case $n$ is on the right side of $C_r$. The proof is based on the fact that $L_n$ goes into $T_p$ when the span on a level of the right branch of $T_p$ is bigger than $d_r(n)$. Obviously, the Property is surely true if $n \in r(T_p)$. If $n \notin T_p$, let $k_n - k_p = \sigma$. Then $n$ lies on the level matching to level $\sigma$ of $T_p$. Take an arbitrary level $\sigma + i$ of $T_p$ with $i \geq 0$; then there are $2^{\sigma+i}$ nodes from $C_r$ to the rightmost node on the level.

Thereby, if $2^{\sigma+i-1} \leq d_r(n)$, namely, $i \geq \lceil \log_2 d_r(n) \rceil + 1 - \sigma$. $L_n$ goes into $T_p$. Take $i_0 = \lceil \log_2 d_r(n) \rceil + 1 - \sigma$ to be the critical case; then $i_0 < \lceil \log_2 d_r(n) \rceil + 2 - \sigma$. Since $n$ lies on level $k_n$ in $T_3$, it knows $d_l(n) \leq 2^{k_n} - 1$ and $d_r(n) \leq 2^{k_n} - 2$. Thereby,

$$i_0 < \lceil \log_2 d_r(n) \rceil + 2 - \sigma \leq \log_2 d_r(n) + 1 - \sigma < k_n + 2 - \sigma \leq k_n + 1 = \lceil \log_2 n \rceil$$

that is

$$i_0 \leq \lceil \log_2 n \rceil - 1$$

Similarly, the conclusion holds when $n$ is on the left side of $C_r$.

Example 1. Take in $T_3$ a node $p=27$ and $n=61$, as shown in Fig. 7; then $\lceil \log_2 n \rceil = 5$, $\lceil \log_2 p \rceil = 4$, $C_r$ of $T_{27}$ is $C_r = \{55,109,217,433,865,...\}$ and $d_r(n) = 5$ by Property 4. Construct a connection $L_n$ by Property 4; then $L_n$ passes through $N_{(0,4)}^{27} = 61$, $N_{(2,5)}^{27} = 115$, $N_{(3,7)}^{27} = 223$ and $N_{(4,11)}^{27} = 439$, among which $N_{(3,7)}^{27} = 223 \in T_{27}$ and $N_{(4,11)}^{27} = 439 \in T_{27}$. It is sure $L_n$ goes into $T_{23}$ by penetrating at most $\lceil \log_2 n \rceil - 1 = 4$ levels.

Fig. 6. Connection goes from $T_3$ into $T_p$

Fig. 7. Penetration of a node into a tree
**Theorem 1.** Let $m$ and $n$ be two odd integers bigger than 3; then there always a trace that leads $m$ to walk into $T_n$ or $n$ to walk into $T_m$.

**Proof.** Without loss of generality, assume $m < n$. Then by Properties 4 and 5, $n$ is surely able to walk into $T_m$. By Lemma 2, $m$ can first walk along a parallel connection to the level where $n$ lies, then penetrates into $T_n$.

**Property 6.** Let $p > 3$ be an odd number, $T_p$ be the $p$-rooted valuated binary tree with $C_j$ and $C_r$ being the left-center and right-center lines respectively; suppose $n \in T_p$ is a node that is $d_l(n)$ and $d_r(n)$ away from $C_j$ and $C_r$, respectively; assume $s_l$ and $s_r$ are $n$’s left son and right son respectively, as illustrated in Fig. 8; then $s_l + 2(d_l(n) - 1)$ and $s_r + 2(d_r(n) - 1)$ are respectively $d_l(n)$ and $d_r(n)$ away from $C_j$ and $C_r$ if $n$ lies on the left of $C_j$, whereas $s_l - 2(d_l(n) - 1)$ and $s_r - 2(d_r(n) - 1)$ are respectively $d_l(n)$ and $d_r(n)$ away from $C_j$ and $C_r$ if $n$ lies on the right of $C_j$.

**Fig. 8.** $n$ and $s_r + 2(d_r(n) - 1)$ are equal-distanced from $C_l$

**Proof.** Here the proof is for the case $n$ lies on the left of $C_j$. Assume $n = N_{(k,l,j)} - 2(d_l(n) - 1)$, where $N_{(k,l,j)} \in C_j$; then $2N_{(k,l,j)} + 1 = N_{(k+1,l+1,j)} \in C_j$. $s_l$ and $s_r$ are on level $k_n + 1$. Considering

$$s_r = 2n + 1 \Rightarrow s_r + 2(d_l(n) - 1) = 2n + 1 + 2(d_l(n) - 1) = 2(N_{(k,l,j)} - 2(d_l(n) - 1) + 1 + 2(d_l(n) - 1) = 2N_{(k+1,l+1,j)} - 2(d_l(n) - 1) + 1 = N_{(k+1,l+1,j)} - 2(d_l(n) - 1))$$

it knows that $s_r + 2(d_l(n) - 1)$ is $d_l(n)$ away from $C_j$.

Similarly, other cases can be proved.

**Remark 2.** There is a more geometric proof for Property 6 shown here. $n$’s being $d_l(n)$ away from $C_j$ leads to $s_l$ being $2d_l(n)$ away from $C_j$. Accordingly, from $s_l$ to $C_j$, there is one that is $d_l(n)$ away from $C_j$. That one is sure $d_l(n) - 1$ away from $s_l$ and is expressed by $s_r + 2(d_l(n) - 1)$.

**Property 7.** Let $m$ be an odd integer and $\beta = \lceil \log_2 m \rceil$; suppose integer $\alpha$ satisfies $\alpha > \beta$; then $m + 2^{\alpha - \beta}(2^{\alpha + \beta} - 1)m = N_{(2\alpha - \beta + 1,l,j)} \in l(T_m)$, where integer $\chi \geq 0$.
Proof. First, $\alpha > \beta$ is mandatory because $m + 2^\alpha \beta \left(2^{n+1} \chi - 1\right)m = 2^{n+1} m \not\in T_m$ in the case $\alpha = \beta$. Now let $n = m + 2^\alpha \beta \left(2^{n+1} \chi - 1\right)m$ and $J = 2^{2n-\beta+1} - 2^{\alpha-\beta+1}m + \frac{m-1}{2}$; then

$$n = 2^{2n-\beta+1}m - 2^{2n-\beta+1} + 2^{2n-\beta+1} \chi - 2^{\alpha-\beta+1}m + m$$

$$= 2^{2n-\beta+1}(m-1) + 2(2^{2n-\beta+1} - 2^{\alpha-\beta+1}m + \frac{m-1}{2}) + 1$$

$$= 2^{2n-\beta+1}(m-1) + 2J + 1$$

Now it is to show $0 \leq J \leq 2^{n-\beta+1} - 1$ and $n = N_m^{(2n-\beta+1,J)}$. In fact, $\beta = \left\lfloor \log_2 m \right\rfloor$ yields $2^\beta + 1 \leq m \leq 2^\beta - 1$, namely, $-2^\beta + 1 \leq -m \leq -2^\beta - 1$. Multiplying each term of this inequality by $2^{\alpha-\beta+1}$ yields $-2^\alpha + 2^\alpha \chi \leq -2^\beta + 2^\alpha \chi - 1$.

Since $2^\beta - 1 \leq \frac{m-1}{2} \leq 2^\beta - 1$, it is sure $2^{2n-\beta+1} - 2^\alpha + 2^\alpha \chi - 1 \leq J \leq 2^\beta - 1 - 2^\alpha + 2^\alpha \chi - 1$.

Subtracting $2^{2n-\beta+1} - 1$ from the right side term yields $2^\beta - 2^\alpha + 2^\alpha \chi - 1 \leq 0$.

Next is to show $2^{2n-\beta+1} - 2^\alpha + 2^\alpha \chi - 1 \leq 0$ by using proof of contradiction. In fact, assume $2^{2n-\beta+1} - 2^\alpha + 2^\alpha \chi - 1 < 0$; then

$$2^{2n-\beta+1} + 2^\alpha \chi + 2^\alpha - 1 < 2^\alpha$$

$$\Rightarrow 2^{n-\beta+1} + 2^\alpha \chi + 2^\alpha - 1 < 1$$

which is contradictory to $\alpha \geq \beta + 1$ and $\chi \geq 0$.

As a result,

$$0 \leq J \leq 2^{n-\beta+1} - 1$$

which shows

$$m + 2^\alpha \beta \left(2^{n+1} \chi - 1\right)m = N_m^{(2n-\beta+1,J)} \in (T_m)$$

Property 7*. Let $m$ be an odd integer and $\beta = \left\lfloor \log_2 m \right\rfloor$; then $m + 2^\sigma \left(2^{n+1} \chi - 1\right)m \not\in (T_m) \ddot{\smile}$, where $\sigma > 0$ and $\chi \geq 0$ are integers. Particularly, $m + 2(2^\beta - 1)m \in T_m$, $m + 2(2^{\beta+1} - 1)m \in T_m$ and $m + 2(2^{\beta+\delta} - 1)m \in T_m$ with $\delta \geq 0$.

Proof. Taking $\sigma = \alpha - \beta$ in Property 7 immediately turns $m + 2^\sigma \beta \left(2^{n+1} \chi - 1\right)m$ into $m + 2^\alpha \beta \left(2^{n+1} \chi - 1\right)m$. The particular case $m + 2(2^\beta - 1)m \in T_m$ is shown in the following reasoning.
\[m + 2(2^\beta - 1)m = 2^\beta m - m = 2^\beta m - 2^\beta + 1 - m = 2^\beta (m - 1) + 2(2^\beta - m + \frac{1}{2}) + 1\]

Obviously, if \(0 \leq 2^\beta - \frac{m + 1}{2} \leq 2^\beta - 1\) then \(m + 2(2^\beta - 1)m = N_{(\beta + 1, 2^\beta - m + \frac{1}{2})}^n \in T_n\). Note that

\[
\beta = \left\lfloor \log_2 m \right\rfloor \\
\Rightarrow 2^\beta + 1 \leq m \leq 2^\beta - 1 \\
\Rightarrow 2^\beta + 1 \leq \frac{m + 1}{2} \leq 2^\beta \\
\Rightarrow -2^\beta \leq -\frac{m + 1}{2} \leq -2^\beta - 1 \\
\Rightarrow 0 \leq 2^\beta - \frac{m + 1}{2} \leq 2^\beta - 1
\]

Consequently, it follows

\[m + 2(2^\beta - 1)m = N_{(\beta + 1, 2^\beta - m + \frac{1}{2})}^n \in T_n\]

Actually, \(N_{(\beta + 1, 2^\beta - m + \frac{1}{2})}^n\) lies on level \(\beta + 1\) in the left branch of \(T_n\).

The particular case \(m + 2(2^\beta - 1)m \in T_n\) is shown as follows

\[
\beta = \left\lfloor \log_2 m \right\rfloor \\
\Rightarrow -2^\beta \leq -\frac{m + 1}{2} \leq -2^\beta - 1 \\
\Rightarrow 2^\beta - 2^\beta \leq 2^\beta - \frac{m + 1}{2} \leq 2^\beta - 2^\beta - 1 \\
\Rightarrow 2^\beta - \frac{m + 1}{2} \leq 2^\beta - 1 \\
\Rightarrow m + 2(2^\beta - 1)m = 2^\beta m - m + m = 2^\beta m - m^2 - 2^\beta + 1 - m = 2^\beta (m - 1) + 2(2^\beta - m + \frac{1}{2}) + 1 = N_{(\beta + 2^\beta - m + \frac{1}{2})}^n \in T_n
\]

It can be seen that, \(N_{(\beta + 2^\beta - m + \frac{1}{2})}^n\) lies on level \(\beta + 2\) in the right branch of \(T_n\).

The case \(m + 2(2^\beta - 1)m \in T_n\) is shown as follows.
\[2^{\beta -1} + 1 \leq \frac{m+1}{2} \leq 2^\beta\]
\[\Rightarrow -2\beta \leq -\frac{m+1}{2} \leq -2^{\beta -1} -1\]
\[\Rightarrow 2^{\beta +d} -2\beta \leq 2^{\beta +d} - \frac{m+1}{2} \leq 2^{\beta +d} - 2^{\beta -1} -1\]
\[\Rightarrow 2^{\beta} (2^{d} -1) \leq 2^{\beta +d} - \frac{m+1}{2} \leq 2^{\beta +d} - 2^{\beta -1} -1 < 2^{\beta +d} -1\]
\[m + 2(2^{\beta +d} -1)m = 2^{\beta +d} m - m\]
\[= 2^{\beta +d} m - 2^{\beta +d +1} + 2^{\beta +d +1} - m\]
\[= 2^{\beta +d +1} (m -1) + 2(2^{\beta +d} - \frac{m+1}{2}) + 1\]
\[= N^m_{(\beta, \delta + 1, \delta + 1, \frac{m+1}{2})} \in T_n\]

It can be seen that, the bigger \(\beta\) is, the closer \(N^m_{(\beta, \delta + 1, \delta + 1, \frac{m+1}{2})}\) is to the right branch of \(T_n\).

**Property 8.** Let \(p>3\) be an odd integer and \(T_p\) be the \(p\)-rooted valuated binary tree with \(C_i\) and \(C_r\) being the left and right central lines respectively; suppose \(n = ap\) with \(\alpha >1\) being an odd integer is a node of \(T_3, L_n\) is the connection starting downwards from \(n\) and parallel to \(C_i\); then each node on \(L_n\) is a multiple of \(p\).

**Proof.** By Lemma 3, \(p\) lies at position \(J_p = \frac{p-1}{2} - 2^{\beta} \) on level \(k_p = \lfloor \log_2 p \rfloor -1\) of \(T_3\). Assume \(n\) lies at position \(J_n\) on level \(k_n\) of \(T_3\), namely, \(n = N_{(k_n, J_n)}\). Then by \(a >1\) and Lemma 1(P1), \(k_n \geq k_p +1\) and \(J_n = \frac{n-1}{2} - 2^{\beta}\). By Lemma 2(P3), \(C_i\) and \(C_r\) are represented in \(T_3\) by

\[C_i = \{N_{(k_n+1, J+n)}, N_{(k_n+2, J+n)}, \ldots, N_{(k_n+2, J+n)}\}\]
\[C_r = \{N_{(k_n+1, J+n)}, N_{(k_n+2, J+n+2)}, \ldots, N_{(k_n+2, J+n+2)}\}\]

Assume \(k_n + \sigma = k_p\); then the node on \(C_i\) and on level \(k_n\) is \(N_{(k_n, 2^\sigma J_n + 2^{\sigma -1} -1)}\) and its distance to \(n = N_{(k_n, J_n)}\) is given by

\[d = \frac{N_{(k_n, 2^\sigma J_n + 2^{\sigma -1} -1)} - N_{(k_n, J_n)}}{2} +1\]

That is

\[d = \left\{\begin{array}{ll}
2^\sigma J_p + 2^{\sigma -1} -1 - J_n & +1 \\
N_{(k_n+2^\sigma J_n + 2^{\sigma -1} -1)} & > N_{(k_n, J_n)} \\
J_n - 2^\sigma J_p - 2^{\sigma -1} + 2, N_{(k_n+2^\sigma J_n + 2^{\sigma -1} -1)} & < N_{(k_n, J_n)}
\end{array}\right\}

Now take an arbitrary node on \(C_i\), say \(N_{(k_n+i, 2^\sigma J_n + 2^{\sigma -1} -1)}\) with \(i > \sigma\); it can be seen that, when \(N_{(k_n+2^\sigma J_n + 2^{\sigma -1} -1)} > N_{(k_n, J_n)}\), the node \(N_{(k_n+i, 2^\sigma J_n + 2^{\sigma -1} -1)} -2(d-1)\) is the node on \(L_n\) that has distance \(d\) to
$N_{(k,2^i,j,x^2+1)}$, whereas when $N_{(k,2^i,j,x^2+1)} < N_{(k,i,j)}$, the node $N_{(k,2^i,j,x^2+1)} + 2(d(k_a) - 1)$ is the node on $L_a$ that has distance $d$ to $N_{(k,2^i,j,x^2+1)}$.

Note that, for the case $N_{(k,2^i,j,x^2+1)} > N_{(k,i,j)}$, it holds

$N_{(k,2^i,j,x^2+1)} - 2(d - 1)$

$= N_{(k,2^i,j,x^2+1)} - 2(2^i J_p + 2^{x-1} - J_a - 1)$

$= 2^{i+1} + 2(2^i J_p + 2^{x-1} - 1) + 1 - 2^{x+1} J_p - 2^x + 2 J_a + 2$

$= 2^{i+1} + 2^{x+1} J_p + 2^{x-1} J_p - 2^x + 2 J_a + 2$

$= 2^{i+1} + 2^{x+1} J_p + 2^{x-1} J_p - 2^x + 2 J_a + 1$

$= 2^{x+1} + 2 J_p + 1 - 2^{x+1} J_p - 2^x + 2 J_a + 1$

$= 2^{x+1} + 2 J_p + 1 - 2^x (2 J_p + 1) + 2^{x+1} J_p + 2 J_a + 1$

$= 2(2^{x+1} + 2 J_p + 1) - 2^x (2 J_p + 1) + (2^{x+1} + 2 J_a + 1)$

$= (2 - 2^x) p + ap$

while for the case $N_{(k,2^i,j,x^2+1)} < N_{(k,i,j)}$ it holds

$N_{(k,2^i,j,x^2+1)} + 2(d - 1)$

$= N_{(k,2^i,j,x^2+1)} + 2((J_a - 2^x J_p - 2^{x-1} + 2) - 1)$

$= 2^{i+1} + 2(2^i J_p + 2^{x-1} - 1) + 1 + 2 J_a - 2^{x+1} J_p - 2^x + 2$

$= 2^{i+1} + 2^{x+1} J_p + 2^{x-1} J_p - 2^x + 2$

$= 2^{i+1} + 2^{x+1} J_p + 2^{x-1} J_p - 2^x + 2 J_a + 1$

$= 2^{x+1} + 2 J_p + 1 - 2^x (2 J_p + 1) - 2^{x+1} J_p - 2^x + 2 J_a + 1$

$= 2^{x+1} + 2 J_p + 1 - 2^x (2 J_p + 1) + 2^{x+1} J_p + 2 J_a + 1$

$= 2(2^{x+1} + 2 J_p + 1) - 2^x (2 J_p + 1) + (2^{x+1} + 2 J_a + 1)$

$= (2 - 2^x) p + ap$

It is seen that, either $N_{(k,2^i,j,x^2+1)} > N_{(k,i,j)}$ or $N_{(k,2^i,j,x^2+1)} < N_{(k,i,j)}$ leads to that a node on $L_a$ is of the form $(2^x - 2^x) p + ap$, which is a multiple of $p$.

**Property 8*. Let $p > 3$ be an odd integer; then there are always odd integers of the form $(2^x - 2^x) p + ap$ that are descendant nodes of $T_p$, where $a > 1$ is an odd integer and $i > \sigma \geq \lceil \log_2 p \rceil$.

**Proof.** Property 4 ensures $n = ap$ reaches a descendant of $T_p$ after penetrating downwards along a parallel connection by $\lceil \log_2 ap \rceil - 1 = \lceil \log_2 (a + \log_2 p) \rceil - 1 \geq \lceil \log_2 p \rceil$ steps. The reasoning processes in proving property 8 show that the descendant is of the form $(2^x - 2^x + \alpha) p$ and $i > \sigma \geq \lceil \log_2 p \rceil$.
5 Applications in Integer Factorization

Property 7, Property 7*, and Property 8* indicate that an odd integer of the form \((2^n - 2^\beta + \gamma)p\) must be a descendant of the p-rooted tree, where \(\gamma \geq 1\) and \(p > 3\) are positive odd integers, \(\alpha > \beta\). This on the other hand means that an odd integer \(m\) that has a divisor of the form \((2^n - 2^\beta + \gamma)p\) can be factorized very soon. This section proves the related results.

5.1 Corollaries

**Corollary 1.** The divisor \(p\) of odd positive composite integer \(m = pq\) can be found out in at most \(O(1 + \log_2 q)\) searching steps provided that \(q = 2^n - 1\) with integers \(\alpha \geq \left\lfloor \frac{\log_2 m}{2} \right\rfloor + 1\).

**Proof.** Referring to the particular cases in Property 7* knows that, an arbitrary positive odd integer \(1 > n\) results in
\[
1 \geq 2(2^{\beta + 1} - 1)n \in T_\beta, \quad \text{where} \quad \beta = \left\lfloor \log_2 n \right\rfloor \quad \text{and} \quad \delta \geq 0.
\]
This is equivalent to \((2^n - 1)n \in T_\alpha\) with integer \(\chi \geq \left\lfloor \log_2 n \right\rfloor + 1\). By \(m = pq\), \(q = 2^n - 1\) and \(\alpha \geq \left\lfloor \frac{\log_2 m}{2} \right\rfloor + 1\), it follows
\[
q \geq 2^{\left\lfloor \frac{\log_2 m}{2} \right\rfloor} - 1 > 2^{\left\lfloor \frac{\log_2 m}{2} \right\rfloor} - 1 = \sqrt{m} - 1 \Rightarrow q \geq \left\lfloor \sqrt{m} \right\rfloor \geq p \Rightarrow \left\lfloor \frac{\log_2 m}{2} \right\rfloor \geq \left\lfloor \log_2 p \right\rfloor
\]

Let \(\left\lfloor \frac{\log_2 m}{2} \right\rfloor = \left\lfloor \log_2 p \right\rfloor + \delta\) with \(\delta \geq 0\); then it is known
\[
\begin{align*}
m &= pq \\
q &= 2^n - 1 \\
\alpha &\geq \left\lfloor \log_2 p \right\rfloor + \delta + 1 \Rightarrow m \in T_\alpha \\
\delta &\geq 0
\end{align*}
\]

Since \(m\) and \(p\) lie respectively on level \(\left\lfloor \log_2 m \right\rfloor - 1\) and level \(\left\lfloor \log_2 p \right\rfloor - 1\) of \(T_\delta\), the difference is
\[
\left\lfloor \log_2 q \right\rfloor \leq \left\lfloor \log_2 m \right\rfloor - 1 \leq \left\lfloor \log_2 p \right\rfloor \leq \left\lfloor \log_2 q \right\rfloor + 1
\]

Namely, it takes at most \(\left\lfloor \log_2 q \right\rfloor + 1\) searching steps for \(m\) to trace up to \(q\).

**Remark 3.** The conclusion \(q \geq \left\lfloor \sqrt{m} \right\rfloor \geq p\) in the reasoning process is the key. Accordingly, Corollary 1 still holds if the condition \(\alpha \geq \left\lfloor \frac{\log_2 m}{2} \right\rfloor + 1\) is substituted with \(\alpha \geq \left\lfloor \log_2 p \right\rfloor + 1\) because
\[
\alpha \geq \left\lfloor \log_2 p \right\rfloor + 1 \Rightarrow q = 2^n - 1 \geq 2^{\left\lfloor \log_2 p \right\rfloor + 1} - 1 > 2^{\log_2 p} - 1 = p - 1 \Rightarrow q \geq p
\]

**Corollary 2.** The divisor \(p\) of odd positive composite integer \(m = pq \geq 9\) can be found out in at most \(O(1 + \left\lfloor \log_2 q \right\rfloor)\) searching steps provided that \(q = 2^{2\alpha + \beta - 2^n + 1}\) with integers \(\alpha \geq 1, \beta \geq \left\lfloor \frac{\log_2 m}{2} \right\rfloor\).

**Proof.** The given conditions yield
\[ q = 2^{2a+\beta} - 2^a + 1 \]
\[ \geq 2^{\left\lfloor \log_2 m \right\rfloor + 2a} - 2^a + 1 = 2^a \left( 2^{\left\lfloor \log_2 m \right\rfloor + a} - 1 \right) + 1 \]
\[ \geq 2^a \left( 2^{\left\lfloor \log_2 m \right\rfloor} - 1 \right) + 1 > 2^a \left( 2^{\log_2 m} - 1 \right) + 1 = 2^a \left( \sqrt{m} - 1 \right) + 1 \]
\[ \Rightarrow \sqrt{m} > 2^a \left( 1 - \frac{1}{\sqrt{m}} \right) + \frac{1}{\sqrt{m}} \geq 2^a \left( 1 - \frac{1}{3} \right) + \frac{1}{3} > 1 \]

which means

\[ p < q \Rightarrow p \leq \sqrt{m} \Rightarrow \log_2 p \leq \frac{\log_2 m}{2} \Rightarrow \left\lfloor \log_2 p \right\rfloor \leq \left\lfloor \frac{\log_2 m}{2} \right\rfloor \]

Let \( \beta = \left\lfloor \frac{\log_2 m}{2} \right\rfloor + \delta = \left\lfloor \log_2 p \right\rfloor + \omega; \) then integers \( \omega \geq 0, \delta \geq 0 \) and \( 2^{2a+\beta} - 2^a + 1 = 2^{\left\lfloor \log_2 m \right\rfloor + a} + 2^a - 2^a + 1 \). By Property 7 it follows

\[ m = pq = (2^{\left\lfloor \log_2 m \right\rfloor + a + 2a} - 2^a + 1) \in (T_p) \]

Since \( m \) and \( p \) lie respectively on level \( \left\lfloor \log_2 m \right\rfloor - 1 \) and \( \left\lfloor \log_2 p \right\rfloor - 1 \), it takes \( \left\lfloor \log_2 m \right\rfloor - \left\lfloor \log_2 p \right\rfloor \leq \left\lfloor \log_2 q \right\rfloor + 1 \) steps for \( m \) to trace up to \( q \).

**Remark 4.** By substituting the condition \( \beta \geq \left\lfloor \frac{\log_2 m}{2} \right\rfloor \) with \( \beta \geq \left\lfloor \log_2 p \right\rfloor \), Corollary 2 still holds because

\[ q = 2^{2a+\beta} - 2^a + 1 \]
\[ \geq 2^{\left\lfloor \log_2 m \right\rfloor + a + 2a} - 2^a + 1 = 2^a \left( 2^{\left\lfloor \log_2 m \right\rfloor + a} - 1 \right) + 1 \]
\[ \geq 2^a \left( 2^{\log_2 m} - 1 \right) + 1 > 2^a \left( 2^{\log_2 m} - 1 \right) + 1 = 2^a (p - 1) + 1 \geq 2p - 1 \]

**Corollary 3.** The divisor \( p \) of odd positive composite integer \( m = pq \) can be found out in at least \( O(\log_2 q) \) and at most \( O(\left\lfloor \log_2 m \right\rfloor) \) searching steps provided that \( q = 2^a - 2^\beta + 2 \gamma \) with integers \( \alpha > \beta > \left\lfloor \log_2 p \right\rfloor \) and odd integer \( \gamma \geq 1 \).

**Proof.** By Property 8*, an arbitrary odd integer of the form \( m = (2^a - 2^\beta + 2 \gamma p) \) must be a descendant node of \( T_p \). By \( \alpha > \beta > \left\lfloor \log_2 p \right\rfloor \), it follows \( q \geq 2^{\beta + 1} - 2^\beta + 2 \gamma > p \). Since obviously \( q < \frac{m}{3} \), it yields

\[ \left\lfloor \log_2 q \right\rfloor \leq \left\lfloor \log_2 \frac{m}{3} \right\rfloor = \left\lfloor \log_2 m - \log_2 3 \right\rfloor \leq \left\lfloor \log_2 m \right\rfloor - 1 \]

Note that, \( p \) and \( m \) lie respectively on level \( \left\lfloor \log_2 p \right\rfloor - 1 \) and level \( \left\lfloor \log_2 m \right\rfloor - 1 \) of \( T_3 \), the difference between the two levels satisfies

\[ \left\lfloor \log_2 p \right\rfloor \leq \left\lfloor \log_2 q \right\rfloor \leq \left\lfloor \log_2 m \right\rfloor - \left\lfloor \log_2 p \right\rfloor \leq \left\lfloor \log_2 q \right\rfloor + 1 \leq \left\lfloor \log_2 m \right\rfloor \]

and the corollary is validated.
5.2 Numerical experiments

Numerical experiments are made with Maple software. Table 1 lists the experimental results. In the table, the column ‘Big Number N’ is the big odd composite number to be factorized, the column ‘nDigits’ is the number of decimal digits, the column ‘sDivisor’ is the found divisor of N, the column ‘Tsteps’ is the number of searching steps calculated theoretically from the previous corollaries and the column ‘Rsteps’ is the real searching steps recorded by the computer. It can be seen that the real searching steps are exactly match to the theoretical steps. For readers to know the algorithms more deeply, the Maple programs are list in the appendix section. Readers can test them with the programs.

Table 1.

<table>
<thead>
<tr>
<th>Big Number N</th>
<th>nDigits</th>
<th>sDivisor</th>
<th>Tsteps</th>
<th>Rsteps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1361129467683753874933991060479210657</td>
<td>59</td>
<td>80000000000000001239</td>
<td>126</td>
<td>126</td>
</tr>
<tr>
<td>100433627760186892213726306090627668</td>
<td>59</td>
<td>61897001964269013744</td>
<td>106</td>
<td>106</td>
</tr>
<tr>
<td>369708606467922467573448011163181901</td>
<td>68</td>
<td>2172951891767154277</td>
<td>126</td>
<td>126</td>
</tr>
<tr>
<td>6393505518278570670458580224861</td>
<td>68</td>
<td>91638919976965192288</td>
<td>126</td>
<td>126</td>
</tr>
<tr>
<td>1559155429592009364435823204937723814</td>
<td>68</td>
<td>12676506002282294014</td>
<td>126</td>
<td>126</td>
</tr>
<tr>
<td>205298186366538114062107392351</td>
<td>69</td>
<td>96702681091</td>
<td>126</td>
<td>126</td>
</tr>
<tr>
<td>216397573372051183573360314936866748</td>
<td>69</td>
<td>12676506002282294014</td>
<td>126</td>
<td>126</td>
</tr>
<tr>
<td>15718346332418321746200380770157</td>
<td>71</td>
<td>16225927682921336339</td>
<td>126</td>
<td>126</td>
</tr>
<tr>
<td>2760698538716225514973902344910793166</td>
<td>71</td>
<td>1578010288127</td>
<td>126</td>
<td>126</td>
</tr>
<tr>
<td>84587161426206116995480300803329</td>
<td>71</td>
<td>59565421307610088978</td>
<td>126</td>
<td>126</td>
</tr>
<tr>
<td>1013453127459823122874618528109162771</td>
<td>71</td>
<td>16225927682921336339</td>
<td>126</td>
<td>126</td>
</tr>
<tr>
<td>39255363536893359315153211936321</td>
<td>71</td>
<td>1578010288127</td>
<td>126</td>
<td>126</td>
</tr>
<tr>
<td>2607406049708142190423610481163987976</td>
<td>93</td>
<td>16225927682921336339</td>
<td>200</td>
<td>199</td>
</tr>
<tr>
<td>7654369593753705042663627621537194650</td>
<td>93</td>
<td>1578010288127</td>
<td>200</td>
<td>199</td>
</tr>
<tr>
<td>5523582829895109067</td>
<td>99</td>
<td>17014118346046923173</td>
<td>200</td>
<td>199</td>
</tr>
<tr>
<td>2734063405978764905465627783897026706</td>
<td>99</td>
<td>1687303715884105727</td>
<td>200</td>
<td>199</td>
</tr>
<tr>
<td>6753924081589598660106153660338579389</td>
<td>99</td>
<td>164560743076778192897</td>
<td>196</td>
<td>195</td>
</tr>
</tbody>
</table>

6 Conclusions and Future Work

By means of defining connection and penetration in a valuated binary tree, nodes out of a tree can be related with those in a tree and some outer properties are brought into the tree so that more properties of nodes are discovered. This broadens the studies on a tree. Research in this paper validates such means. It is seen from previous research and the research in this paper that, there is always a proper approach to factorize rapidly a certain kind of special odd integers. The theoretical analysis and numerical experiments in this paper once again demonstrate this point of view. However something is still very rough and there is still work to make it refinery. For example, the traits of $\alpha$, $\beta$ in the three corollaries still need further investigating to make their limits more accurate. This remains future studies to make them clear. Meanwhile, this paper merely draws a rough outline in studying the connections and penetrations, more subtle contents need further studying. Hope more young to join the work.

Acknowledgement

The research work is supported Natural Science Foundation of Guangdong Province under Grant No. 2018A030310082.
Competing Interests

Authors have declared that no competing interests exist.

References

DOI: http://dx.doi.org/10.20431/2347-3142.0403008


DOI: https://dx.doi.org/10.9790/5728-1303023740


DOI: https://doi.org/10.4236/apm.2018.85028

DOI: https://doi.org/10.17706/ijapm.2019.9.4.173-181

DOI: https://doi.org/10.3844/jmssp.2020.24.34

DOI: 10.17706/jsw.15.3.86-97


DOI: http://doi.org/10.17706/ijapm.2020.10.4.135-142

DOI: https://doi.org/10.5539/jmr.v13n3p1
Appendix

Maple Source Codes

SubRoutine Father (Calculate the father of a node Son)

```maple
Father:= proc(Son)
local X, r;
r:=modp(Son,4);
if r=1 then X:=(Son+1)/2;
else X:=(Son-1)/2;
fi
End proc
```

MainRoutine FactIt (Calculate the small divisor of N)

```maple
FactIt:= proc(N)
local X, AA, g, p, q, Tsteps, Rsteps:=0, len;
AA:=Father(N);
g:=gcd(AA,N);
while g=1 do
Rsteps:=Rsteps+1;
X:=AA;
AA:=Father(X);
g:=gcd(AA,N);
end;
p:=g;
q:=N/p;
Tsteps:=floor(evalf(log2(q)));
lprint("Find p=", p , " Tsteps=" , Tsteps, "Rsteps=", Rsteps);
End proc
```

© 2021 Wang et al.; This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
http://www.sdiarticle4.com/review-history/69077