Some Divisibility Traits on Valuated Binary Trees

Xingbo Wang[1,2,3*], Hongqiang Guo[1]

[1] Department of Mechatronic Engineering, Foshan University, Foshan City, 528000, China.
[2] Guangdong Engineering Center of Information Security for Intelligent Manufacturing System, Foshan, China.
[3] State Key Laboratory of Mathematical Engineering and Advanced Computing, Wuxi, China.

* Corresponding author. Tel.: +86075782988845; email: xbwang@fosu.edu.cn;dr.xbwang@qq.com

Manuscript submitted May 8, 2018; accepted October 1, 2018.
doi: 10.17706/ijapm.2019.9.1.1-11

Abstract: The paper investigates some divisibility traits on valuated binary trees, including some divisibility rules on T_3 tree and some laws of multiples' distribution on a T_p tree. It proves that the root of a valuated binary tree can always have a common divisor with certain nodes that appear periodically on the left most path or the left side-path of the tree and calculation of divisors of a node is highly related with the two's power plus one and the two's power minus one. Theorems and corollaries are proved with detail mathematical deductions and they provide a foundation for people to design algorithm for factoring odd integers.

Key words: Number theory, integer factorization, congruence equation, binary tree.

1. Introduction

Putting the odd integers bigger than 1 on a full binary tree from top to bottom and from left to right, you will obtain a valuated binary tree, as introduced in [1]. With the help of the valuated binary, many new properties of odd integers are discovered. For example, the properties of symmetric nodes and symmetric common divisors, the properties of subtrees duplication and subtrees transition, the properties of sum by level, root division and uniform sum, as introduced in [2] and [3], and the genetic properties that are disclosed in [4]. All these new properties enable people to know the integers in a different point of view, as stated and investigated in paper [5]. Divisibility, as a central content in number theory [6], is of course an important issue on the valuated binary tree. Accordingly, this paper makes an investigation on the divisibility rules on the valuated binary tree and obtains some new results related with factorization of odd integers.

2. Preliminaries

2.1. Definitions and Notations

A valuated binary tree T is such a binary tree that each of its nodes is assign a value. An odd number 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. The left son is said to have a left attributive and the right son is to have a right attributive. Each son is connected with its father with a path, but there is no path between the two sons. T_3 tree is the case N=3, as introduced in [5]. The root of the T_3 tree is assigned a right attributive. For convenience, symbol $N_{(k,j)}$ is by default the node at the jth position on the kth level of T_3, where $k \geq 0$ and $0 \leq j \leq 2^k - 1$.

Symbol $N_{(i,0)}^{N}$ is the leftmost node on level i ; use symbol $N_{(i,-1)}^{N}$ to denote the odd number left to $N_{(i,0)}^{N}$, namely, $N_{(i,-1)}^{N} = N_{(i,0)}^{N} - 2$. Use symbol P_0^N to indicate the leftmost path defined by $P_0^N = \{N_{(0,0)}^{N}, N_{(1,0)}^{N}, \ldots, N_{(i,0)}^{N}, \ldots\}$, and symbol P_L^N to indicate the path defined by $P_L^N = \{N_{(1,-1),}, \ldots, N_{(i,-1),} \ldots\}$, which is also called a left side-path, as depicted in Fig. 1.

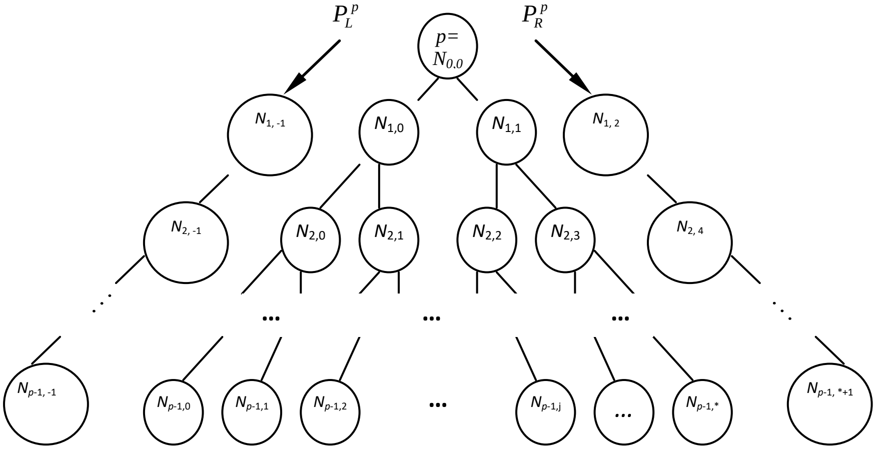

Fig. 1. Tp tree and its side-paths.

An odd interval [*a, b*] is a set of consecutive odd numbers that take *a* as lower bound and *b* as upper bound, for example, [3, 11] = {3, 5, 7, 9, 11}. Intervals in this whole article are by default the odd ones unless particularly mentioned. 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 $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.

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 $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$. Symbol *a*|*b* means *b* can be divided by *a*; symbol (a,b) is to express the greatest common divisor (GCD) of integers *a* and *b*. For an integer *n*, symbols *φ(n)* and *d(n)* denote respectively the Euler's totient function and the number of divisors function of *n*. Symbol $Ord_n a$ means order of *a* modulo *n*.

2.2. Lemmas

Lemma 1 (Node Calculation, see in [1], [5]). Node $N_{(k,j)}$ of T_3 is calculated by

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

Node $N_{(k,j)}$ of T_N is computed by

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

Lemma 2 (Genetic Law 1, see in [4]). If node N can divide $N_{(i,\omega)}^{N}$ of T_N, then it can also divide $N_{(i,2^i-1-\omega)}^{N}$ of

T_N.

And it can also divide nodes $N_{(i,\omega)}^{N_{(i,\omega)}^N}$, $N_{(i,2^i-1-\omega)}^{N_{(i,\omega)}^N}$ $N_{(i,\omega)}^{N_{(i,2^i-1-\omega)}^N}$, and $N_{(i,2^i-1-\omega)}^{N_{(i,2^i-1-\omega)}^N}$ whose roots are $N_{(i,\omega)}^N$ and $N_{(i,2^i-1-\omega)}^N$ respectively. Namely, N transmits its genes to its descendents by making itself a divisor of its certain descendents.

Lemma 3 (Genetic Law 2, see in [4]) Let odd number N be a multiplication of two odd numbers, say $N_{(k,j)}$ and $N_{(l,s)}$, namely, $N=N_{(k,j)}\times N_{(l,s)}$; then subtree T_N inherits all genetic traits from both $N_{(k,j)}$ and $N_{(l,s)}$. In another word, if $d_{(i,\omega)}$ is a common divisor of $N_{(k,j)}$ and $N_{(i,\omega)}^{N_{(k,j)}}$, which lies at the ω^{th} position on the i^{th} level in $T_{N_{(k,j)}}$, then $d_{(i,\omega)}$ is also a common divisor of N and $N_{(i,\omega)}^N$.

3. Main Results and Proofs

3.1. General Mathematical Foundations

Theorem 1. Let *a* be a positive integer and *p* be a prime with (*p*, *a*)=1; if there exist positive integers *α* and β such that $a^{\alpha}-1\equiv 0(\mathrm{mod}\,p)$ and $a^{\beta}+1\equiv 0(\mathrm{mod}\,p)$, then for arbitrary positive integer ω, arbitrary odd integer o and arbitrary even integer *e*, it holds

$$a^{\alpha+\omega\alpha}-1\equiv 0(\mathrm{mod}\,p) \tag{1}$$

$$a^{\beta+\omega\alpha}+1\equiv 0(\mathrm{mod}\,p) \tag{2}$$

$$a^{\alpha+o\beta}+1\equiv 0(\mathrm{mod}\,p) \tag{3}$$

$$a^{\beta+o\beta}-1\equiv 0(\mathrm{mod}\,p) \tag{4}$$

$$a^{\alpha+\omega(p-1)}-1\equiv 0(\mathrm{mod}\,p) \tag{5}$$

$$a^{\beta+\omega(p-1)}+1\equiv 0(\mathrm{mod}\,p) \tag{6}$$

$$a^{\alpha\omega}-1\equiv 0(\mathrm{mod}\,p) \tag{7}$$

$$a^{\beta o}+1\equiv 0(\mathrm{mod}\,p) \tag{8}$$

$$a^{\beta e}-1\equiv 0(\mathrm{mod}\,p) \tag{9}$$

Proof. Direct calculation shows

$$a^{\alpha+\omega\alpha}-1=(a^{\alpha})^{1+\omega}-1=(a^{\alpha}-1)(a^{\alpha\omega}+a^{\alpha(\omega-1)}+\cdots+a^{\alpha}+1).$$

$$a^{\beta+\omega\alpha}+1=a^{\beta}a^{\omega\alpha}-a^{\beta}+a^{\beta}+1=a^{\beta}(a^{\omega\alpha}-1)+(a^{\beta}+1)$$

$$a^{\alpha+\varpi\beta}+1=a^{\alpha+\varpi\beta}-a^{\varpi\beta}+a^{\varpi\beta}+1=a^{\varpi\beta}(a^{\alpha}-1)+(a^{\varpi\beta}+1)$$

$$a^{\beta+\varpi\beta}-1=a^{\beta}a^{\varpi\beta}+a^{\varpi\beta}-a^{\varpi\beta}-1=a^{\varpi\beta}(a^{\beta}+1)-(a^{\varpi\beta}+1)$$

Thus (1), (2), (3) and (4) hold. Note that

$$a^{\alpha+\omega(p-1)}-1=a^{\alpha}a^{\omega(p-1)}-a^{\alpha}+a^{\alpha}-1=a^{\alpha}(a^{\omega(p-1)}-1)+a^{\alpha}-1$$

$$a^{\beta+\omega(p-1)}+1=a^{\beta}a^{\omega(p-1)}-a^{\beta}+a^{\beta}+1=a^{\beta}(a^{\omega(p-1)}-1)+(a^{\beta}+1)$$

By Fermat's little theorem, it holds $a^{\beta(p-1)}-1\equiv 0(\operatorname{mod} p)$. Hence (5) and (6) hold.

The last three ones hold since

$$a^{\alpha\omega}-1=(a^{\alpha}-1)(a^{(\omega-1)\alpha}+a^{(\omega-2)\alpha}+\ldots+a^{\alpha}+1)$$

$$a^{\beta o}+1=(a^{\beta}+1)(a^{\beta(o-1)}-a^{\beta(o-2)}+\ldots+(-1)^{k+1}a^{\beta(o-k)}+\ldots+a^{2\beta}-a^{\beta}+1)$$

$$a^{\beta e}-1=(a^{\beta}+1)(a^{\beta(e-1)}-a^{\beta(e-2)}+\ldots+(-1)^{k-1}a^{\beta(e-k)}+\ldots+a^{2\beta}-a^{\beta}+1)$$

Theorem 2. Let p and q be odd prime numbers with $1<p<q$. Given 4 distinct congruence equations, (10), (11), (12) and (13), each of which is of variable x ,

$$2^{x}-1\equiv 0(\operatorname{mod} p) \tag{10}$$

$$2^{x}+1\equiv 0(\operatorname{mod} p) \tag{11}$$

$$2^{x}-1\equiv 0(\operatorname{mod} q) \tag{12}$$

$$2^{x}+1\equiv 0(\operatorname{mod} q) \tag{13}$$

Then three of the 4 congruence equations must have their solutions, and if $p<q\leq 2p-1$, the solutions lie in interval $[(\frac{1}{2}+\alpha)(p-1),(\alpha+1)(p-1)]$ for arbitrary positive integer α , whereas if $q>2p-1$, the solutions lie in interval $[(\frac{1}{2}+\alpha)(p-1),(\frac{1}{2}+\alpha)(q-1)]$.

Proof. By Fermat's little theorem, it holds

$$2^{p-1}-1\equiv 0(\operatorname{mod} p) \tag{14}$$

Hence $p-1$ is a solution of (10).

Furthermore, Since (14) indicates that either (15) or (16) holds.

$$2^{\frac{p-1}{2}}-1\equiv 0(\operatorname{mod} p) \tag{15}$$

$$2^{\frac{p-1}{2}}+1\equiv 0(\operatorname{mod} p) \tag{16}$$

it knows that, $\frac{p-1}{2}$ is a solution of (10) or (11).

Similarly, it can show that $q-1$ is a solution of (9) and $\frac{q-1}{2}$ is a solution of (12) or (13). Consequently, of the 4 equations there are always 3 ones that have their solutions respectively by $x=p-1$, $x=\frac{p-1}{2}$ and $x=\frac{q-1}{2}$, which lie in interval $[\frac{p-1}{2},p-1]$ if $p<q\le 2p-1$ or lie in $[\frac{p-1}{2},\frac{q-1}{2}]$ if $q>2p-1$. Then referring to Theorem 1.

□

3.2. Some Divisibility Rules on *T*3

Theorem 3. Among three nodes, $N_{(k,\alpha)}$ and its two sons, namely $N_{(k,\alpha)}$, $N_{(k+1,2\alpha)}$ and $N_{(k+1,2\alpha+1)}$, there is exact one multiple of integer 3.

Proof. We prove an alternative conclusion: if $N_{(k,\alpha)}\equiv r(\bmod 3),(r=0,1,2)$ then $N_{(k+1,2\alpha)}\equiv 2(r+1)(\bmod 3)$ and $N_{(k+1,2\alpha+1)}\equiv 2(r-1)(\bmod 3)$. In fact, the following deductions validate the conclusion.

$$N_{(k,\alpha)}\equiv r(\bmod 3)\Rightarrow 2N_{(k,\alpha)}\equiv 2r(\bmod 3)\Rightarrow 2N_{(k,\alpha)}-1\equiv 2r-1(\bmod 3)\Rightarrow N_{(k+1,2\alpha)}\equiv 2(r+1)(\bmod 3)$$

$$N_{(k,\alpha)}\equiv r(\bmod 3)\Rightarrow 2N_{(k,\alpha)}\equiv 2r(\bmod 3)\Rightarrow 2N_{(k,\alpha)}+1\equiv 2r+1(\bmod 3)\Rightarrow N_{(k+1,2\alpha+1)}\equiv 2(r-1)(\bmod 3)$$

Taking $r=0,1,2$ respectively yields the following results

$$N_{(k,\alpha)}\equiv 0(\bmod 3)\Rightarrow N_{(k+1,2\alpha)}\equiv 2(\bmod 3), N_{(k+1,2\alpha+1)}\equiv 1(\bmod 3)$$

$$N_{(k,\alpha)}\equiv 1(\bmod 3)\Rightarrow N_{(k+1,2\alpha)}\equiv 1(\bmod 3), N_{(k+1,2\alpha+1)}\equiv 0(\bmod 3)$$

$$N_{(k,\alpha)}\equiv 2(\bmod 3)\Rightarrow N_{(k+1,2\alpha)}\equiv 0(\bmod 3), N_{(k+1,2\alpha+1)}\equiv 2(\bmod 3)$$

which validate the theorem.

Fig. 2 can intuitionally illustrates Theorem 3.

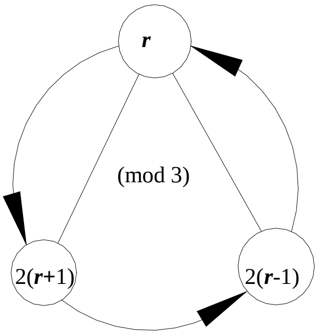

Fig. 2. A node and its two sons modulo 3.

Theorem 4. Let $N_{(n,\beta)}$ be a node of T_3; then $\gcd(2^{n+1}+1,\beta)\,|\,N_{(n,\beta)}$. If there exist positive integers *a* and *b* that satisfy $2^{n+1}-1=ab$; then

$$\gcd(a,\beta+1)\,|\,N_{(n,\beta)}, \gcd(b,\beta+1)\,|\,N_{(n,\beta)}, \gcd(ab,\beta+1)\,|\,N_{(n,\beta)}$$

Proof. $N_{(n,\beta)}=2^{n+1}+1+2\beta=2^{n+1}-1+2(\beta+1)$. it is sure the theorem holds.

Theorem 5. Let $N_{(n,\beta)}$ be a node of T_3. If there exist a positive integer *a* and an odd number $m>1$ such that $n=a\varphi(m)-1$ and $m\,|\,(\beta+1)$, then $m\,|\,N_{(n,\beta)}$.

Proof. The condition $n=a\varphi(m)-1$ yields $N_{(n,\beta)}=2^{n+1}+1+2\beta=2^{a\varphi(m)}-1+2(\beta+1)$. The Euler's totient formula says that an arbitrary odd number m yields $m\,|\,(2^{\varphi(m)}-1)$ and consequently $m\,|\,(2^{a\varphi(m)}-1)$; by $m\,|\,(\beta+1)$, it holds $m\,|\,N_{(n,\beta)}$.

Example 1. For nodes $N_{(5,2)}=69$, positive integers $m=3$ and $a=3$ satisfy $5=3\varphi(3)-1$ and $(m=3)\,|\,(2+1)$. Hence it must yields $(m=3)\,|\,69$.

Example 2. For node $N_{(5,5)}=75$, positive integers $m=3$ and $a=3$ satisfy $5=3\varphi(3)-1$ and $(m=3)\,|\,(5+1)$. Hence it must yields $(m=3)\,|\,75$.

Theorem 6. Integers m and α such that $m\equiv 2(\bmod 3)$ and $\alpha+1\equiv 0(\bmod 7)$ yield $7\,|\,N_{(m,\alpha)}$.

Proof. $m\equiv 2(\bmod 3)\Rightarrow m+1=3s\Rightarrow 2^{m+1}-1=8^s-1=7t,(s,t>0)$. Hence

$$N_{(m,\alpha)}=2^{m+1}+1+2\alpha=2^{m+1}-1+2(\alpha+1) \tag{17}$$

Consequently $\alpha+1\equiv 0(\bmod 7)$ yields $7\,|\,N_{(m,\alpha)}$.

Example 3. Taking $m=5$ will see $N_{(5,6)},N_{(5,13)},N_{(5,20)},N_{(5,27)}$ are all multiples of *7*.

Theorem 7. If positive integer $m>1$ and $m+1=p$ is a prime number; then the following conclusions hold.

(1). $(p,2\alpha+3)\,|\,N_{(m,\alpha)}$;

(2). $(2\alpha+3,\dfrac{2^{p-1}-1}{p})\,|\,N_{(m,\alpha)}$.

Proof. $m+1=p\Rightarrow 2^{m+1}-1=2^p-1=2^{p-1}+2^{p-1}-1\Rightarrow N_{(m,\alpha)}=2(2^{p-1}-1)+2\alpha+3$. Then it is easy to drive out the conclusions the theorem declaims.

Example 4. When $m=4$, $m+1=5$ is a prime. Node $2^{5-1}-1=15$ is a multiple of 5, and it is easy to verify the following fact.

(1) $\alpha=1\Rightarrow 2\alpha+3=5\Rightarrow 5\,|\,N_{(4,1)}(=2^5+1+2=35)$.

(2) $\alpha=6\Rightarrow(2\alpha+3=15)\,|\,(2^4-1)\Rightarrow 15\,|\,N_{(4,6)}(=2^5+1+12=45)$.

(3) $\alpha=\{1,6,11\}\Rightarrow 5\,|\,(2\alpha+3)\Rightarrow 5\,|\,\{N_{(4,1)},N_{(4,6)},N_{(4,11)}(=2^5+1+2\times 11=55)\}$.

(4) $\alpha=\{0,3,6,9,12,15\}\Rightarrow(\dfrac{15}{5}=3)\,|\,(2\alpha+3)\Rightarrow 3\,|\,\{N_{(4,0)},N_{(4,3)},\ldots,N_{(4,15)}\}$.

Theorem 8. If $m+1$ is a composite number and $m+1=ab$ with *a* and *b* being two primes, then the following conclusions hold.

(1) $2^a-1\equiv 0(\bmod(\alpha+1))\Rightarrow(\alpha+1)\,|\,N_{(m,\alpha)}$;

(2) $2^b-1\equiv 0(\bmod(\alpha+1))\Rightarrow(\alpha+1)\,|\,N_{(m,\alpha)}$;

(3) $\alpha+1\equiv 0(\bmod(2^a-1))\Rightarrow(2^a-1)\,|\,N_{(m,\alpha)}$;

(4) $\alpha+1\equiv 0(\mathrm{mod}(2^b-1))\Rightarrow(2^b-1)\mid N_{(m,\alpha)}$;

(5) $(\alpha+1,2^a-1)\mid N_{(m,\alpha)},(\alpha+1,2^b-1)\mid N_{(m,\alpha)}$.

Proof. Formula $N_{(m,\alpha)}=2^{m+1}+1+2\alpha=2^{m+1}-1+2(\alpha+1)$ shows every thing.

Example 5. When $m=5$, $m+1=6=2\times 3$. It can see each $\alpha=\{2,5,6,8,11,13,14,17,20,23,26,27,29\}$ fits its corresponding case in Theorem 8.

Corollary 2. If $n+1=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$, where p_i is prime and α_i is a nonnegative integer, then the following conclusions hold.

(1) $2^{p_i}-1\equiv 0(\mathrm{mod}(\beta+1))\Rightarrow(\beta+1)\mid N_{(n,\beta)}$, $2^{p_i^2}-1\equiv 0(\mathrm{mod}(\beta+1))\Rightarrow(\beta+1)\mid N_{(n,\beta)}$,……,
$2^{p_i^{\alpha_i}}-1\equiv 0(\mathrm{mod}(\beta+1))\Rightarrow(\beta+1)\mid N_{(n,\beta)}$;

(2) $\beta+1\equiv 0(\mathrm{mod}(2^{p_i}-1))\Rightarrow(2^{p_i}-1)\mid N_{(n,\beta)}$, $\beta+1\equiv 0(\mathrm{mod}(2^{p_i^2}-1))\Rightarrow(2^{p_i^2}-1)\mid N_{(n,\beta)}$,……,
$\beta+1\equiv 0(\mathrm{mod}(2^{p_i^{\alpha_i}}-1))\Rightarrow(2^{p_i^{\alpha_i}}-1)\mid N_{(n,\beta)}$;

(3) $\beta+1\equiv 0(\mathrm{mod}(\frac{2^{n+1}-1}{2^{p_i}-1}))\Rightarrow(\frac{2^{n+1}-1}{2^{p_i}-1})\mid N_{(n,\beta)}$, $\beta+1\equiv 0(\mathrm{mod}(\frac{2^{n+1}-1}{2^{p_i^2}-1}))\Rightarrow(\frac{2^{n+1}-1}{2^{p_i^2}-1})\mid N_{(n,\beta)}$,……,
$\beta+1\equiv 0(\mathrm{mod}(\frac{2^{n+1}-1}{2^{p_i^{\alpha_i}}-1}))\Rightarrow(\frac{2^{n+1}-1}{2^{p_i^{\alpha_i}}-1})\mid N_{(n,\beta)}$.

Proof. (Omitted)

Example 6. Let $m=8$, then $m+1=9=3^2$.

(1) $\beta=6$ fits $2^3-1\equiv 0(\mathrm{mod}(\beta+1))$ and $(\beta+1)\mid N_{(n,\beta)}\Leftrightarrow 6\mid N_{(8,6)}(=2^9+1+2\times 6=7\times 75)$.

(2) $\beta=\{6,72\}$ yields $2^9-1\equiv 0(\mathrm{mod}(\beta+1))$, namely, $7\times 73\equiv 0(\mathrm{mod}(\beta+1))$, and $(\beta+1)\mid N_{(n,\beta)}\Leftrightarrow 6\mid N_{(8,72)}(=2^9+1+2\times 72=9\times 73)$.

(3) $\beta+1\equiv 0(\mathrm{mod}(2^3-1))$ yields

$$\beta=\{6s+7\mid s=0,6s+7<2^{10}-1\}\Rightarrow\{6,13,20,27,34,41,48,55,62,69,\dots\}$$

In fact, $N_{(8,13)}=2^9+1+2\times 13=7\times 77$, $N_{(8,20)}=2^9+1+2\times 20=7\times 79$,

$\beta+1\equiv 0(\mathrm{mod}(\frac{2^9-1}{2^3-1}))$, namely, $\beta+1\equiv 0(\mathrm{mod}(73))$, yields

$$\beta=\{72s+73\mid s=0,\dots,72s+73<2^{10}-1\}\Rightarrow\{72,145,\dots\}$$

Actually, $N_{(8,13)}=2^9+1+2\times 72=73\times 9$, $N_{(8,145)}=2^9+1+2\times 145=73\times 11$.

Theorem 9 Suppose $N_{(m,\alpha)}$ and $N_{(n,\beta)}$ be two nodes of T_3; let $d=(m+1,n+1)$ and $g=2^d-1$; then $g\mid(\beta+1,\alpha+1)$ yields $g\mid(N_{(n,\beta)},N_{(m,a)})$.

Proof. By $g=2^d-1=(2^{n+1}-1,2^{m+1}-1)$, it yields $2^{m+1}-1=gs,2^{n+1}-1=gt,(s,t)=1$; hence

$$N_{(m,\alpha)}=2^{m+1}-1+2(\alpha+1)=gs+2(\alpha+1)$$

$$N_{(n,\beta)}=2^{n+1}-1+2(\beta+1)=gt+2(\beta+1)$$

Obviously, $g\,|\,(\beta+1,\alpha+1)$ must lead to $g\,|\,(N_{(n,\beta)},N_{(m,a)})$.

Example 7. Take $m=5$ and $n=8$; then $(5+1,8+1)=3$, $2^3-1=7$. So if take $\alpha=\beta=6$, $N_{(5,6)}$ and $N_{(8,6)}$ have *7* to be their common divisor 7. In fact, a simple calculation shows $N_{(5,6)}=2^{5+1}+12+1$ $=77=7\times11$, $N_{(8,6)}=2^{8+1}+1+12=525=7\times75$,which says $(N_{(5,6)},N_{(8,6)})=7$.

3.3. Some Divisibility Rules on T_p

Theorem 10. Let *p* be an odd prime; then counting from the root and along the leftmost path of T_p, there are at least two multiples of *p* on P_0^N every *p* levels.

Proof. The nodes on the leftmost path are calculated by

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

Note that, by Fermat's little theorem, it always holds when $k=\alpha(p-1)$

$$2^{\alpha(p-1)}-1\equiv 0(\bmod p);\alpha=0,1,2,\ldots;$$

Obviously, $\alpha=0$ and $\alpha=1$ yield two *p's* multiples, $N_{(0,0)}^{p}=p\equiv 0(\bmod p)$ and $N_{(p-1,0)}^{p}=2^{p-1}p-(2^{p-1}-1)\equiv 0(\bmod p)$, and arbitrary α and $\alpha+1$ yield two *p's* multiples. Since there are *p* levels between level $\alpha(p-1)$ and $(\alpha+1)(p-1)$, hence the theorem holds.

Corollary 3. Let *p* be an odd prime; then counting from the root and along the leftmost path of T_p, there are $\frac{p-1}{\beta}+1$ multiples of *p* on P_0^N every *p* levels, where $\beta=\mathrm{Ord}_p 2$ is the order of 2 modulo *p*.

Proof. By Fermat's little theorem, it holds

$$2^{p-1}-1\equiv 0(\bmod p)$$

Since $\beta=\mathrm{Ord}_p 2$, it holds $2^{\beta}-1\equiv 0(\bmod p)$, $\beta\,|\,(p-1)$ and $2^{\alpha\beta}-1\equiv 0(\bmod p)$ with $\alpha=1,2,\ldots,\frac{p-1}{\beta}$. That is to say, there are $\frac{p-1}{\beta}$ multiples of *p* from level *1* to level *p*-1 along the leftmost path of T_p. Considering the root *p*, there are $\frac{p-1}{\beta}+1$ multiples of *p* from level *0* to level *p*-1 along the leftmost path of T_p. By genetic property, the corollary holds.

□

Example 8. Let $p=7$; then $p-1=2\times3$ and $\mathrm{Ord}_7 2=3$. Hence it holds $2^3-1\equiv 0(\bmod 7)$ and $2^6-1\equiv 0(\bmod 7)$, and thus $N_{(0,0)}^{7}=2^0\times7-(2^0-1)=7$, $N_{(3,0)}^{7}=2^3\times7-(2^3-1)=49$ and $N_{(6,0)}^{7}=2^6\times7-(2^6-1)=385$ are *3* multiples of 7 from level *0* to level *6* along the leftmost path of T_7.

Theorem 11. Let *p* be an odd integer and T_p be the p-rooted valuated binary tree and *d* be a positive integer with $1\le d\le p-1$; if there exits a positive integer *e* such that $1\le e\le 2^{d-1}-1$ and

$2^d - \underbrace{(2e-1)}_{odd} \equiv 0(\bmod p)$, then $p \mid N^p_{(d,e-1)}$; if there exits a positive integer f $0 \le p-f \le 2^{d-1}-2$ and $2^d + \underbrace{(2f-1)}_{odd} \equiv 0(\bmod p)$, then $p \mid N^p_{(d,p-f)}$. Particularly, $N^p_{(d,0)} \equiv 0(\bmod p)$ if $2^d - 1 \equiv 0(\bmod p)$, and $N^p_{(d,p-1)} \equiv N^p_{(d,-1)} \equiv 0(\bmod p)$ if $2^d + 1 \equiv 0(\bmod p)$.

Proof. The leftmost node on level d of T_p is given by

$$N^p_{(d,0)} = 2^d p - 2^d + 1$$

Direct calculation yields

$$2^d p - 2^d + 1 = 2^d p - (2^d - (2e-1)) - 2(e-1)$$

Hence the condition $2^d - \underbrace{(2e-1)}_{odd} \equiv 0(\bmod p)$ yields

$$N^p_{(d,0)} + 2(e-1) = N^p_{(d,e-1)} \equiv 0(\bmod p)$$

Since $1 \le e \le 2^{d-1} - 1$, it yields $0 \le e - 1 \le 2^{d-1} - 2$, which shows $N^p_{(d,e-1)}$ is a valid node that lies on the left branch of T_p. Consequently, it holds

$$2^d - \underbrace{(2e-1)}_{odd} \equiv 0(\bmod p) \Rightarrow N^p_{(d,e-1)} \equiv 0(\bmod p) \tag{18}$$

For the case $2^d + \underbrace{(2f-1)}_{odd} \equiv 0(\bmod p)$ with $1 \le p - f \le 2^{d-1} - 2$, it yields

$$N^p_{(d,0)} = 2^d p - 2^d + 1 = 2^d p - (2^d + (2f-1)) + 2f \equiv 2f(\bmod p)$$

that is

$$N^p_{(d,0)} - 2f \equiv 0(\bmod p) \tag{19}$$

Since $N^p_{(d,0)} - 2f \equiv N^p_{(d,p-f)} \equiv 0(\bmod p)$ and the condition $0 \le p - f \le 2^{d-1} - 2$ ensures the validation of $N^p_{(d,p-f)}$, it knows

$$2^d + \underbrace{(2f-1)}_{odd} \equiv 0(\bmod p) \Rightarrow N^p_{(d,p-f)} \equiv 0(\bmod p) \tag{20}$$

Taking $e = 1$ and $f = 1$ respectively in (1) and (3) immediately yields

$$2^d - 1 \equiv 0(\bmod p) \Rightarrow N^p_{(d,0)} \equiv 0(\bmod p)$$

and

$$2^d+1\equiv 0(\bmod p)\Rightarrow N^{p}_{(d,p-1)}\equiv N^{p}_{(d,-1)}\equiv 0(\bmod p)$$

Example 9. $p=5$ and $d=3$ yield $2^3-3\equiv 0(\bmod 5)$ and $e=2$; hence on level 3,

$$N^{5}_{(3,1)}=2^3(5-1)+1+2\times 1=35\equiv 0(\bmod 5)$$

Example 10. $p=17$ and $d=5$ yield $2^5+19\equiv 0(\bmod 17)$ and $e=10$; hence on level 5,

$$N^{17}_{(5,17-10)}=2^5\times(17-1)+1+2\times 7=527\equiv 0(\bmod 5).$$

Example 11. $p=11$ and $d=5$ yield $2^5+1\equiv 0(\bmod 11)$; hence on level 5,

$$N^{11}_{(5,10)}=2^5(11-1)+1+2\times 10=341\equiv 0(\bmod 11) \text{ and } N^{11}_{(5,-1)}=2^5(11-1)+1-2=319\equiv 0(\bmod 11)$$

Example 12. $p=13$ and $d=6$ yield $2^6+1\equiv 0(\bmod 13)$; hence on level 6,

$$N^{13}_{(6,12)}=2^6(13-1)+1+2\times 12=973\equiv 0(\bmod 13) \text{ and } N^{13}_{(6,-1)}=2^6(13-1)+1-2=767\equiv 0(\bmod 13)$$

Corollary 4. Let $N=pq$ with *p* and *q* being odd prime number; then on P^N_0 and P^N_L from level $\frac{p-1}{2}$ to level $p-1$, there are at least 3 nodes each of which has a common divisor *p* or *q* with *N* if $p<q\leq 2p-1$, whereas on P^N_0 and P^N_L from level $\frac{p-1}{2}$ to level $\frac{q-1}{2}$, there are at least 3 nodes each of which has a common divisor *p* or *q* with *N* if $q>2p-1$.

Proof. Note that, by definition, nodes on P^N_L are given by

$$N^{N}_{(i,-1)}=N^{N}_{(i,0)}-2=2^iN-(2^i+1) \tag{21}$$

Then referring to Theorem 11 and Theorem 12, Corollary 4 is surely true.

Theorem 12. Let $N=pq$ with $1<p<q$ being odd integers; then on P^N_0 and P^N_L, there periodically appear *p's* multiple-nodes and *q's* multiple-nodes.

Proof. By Corollary 4, there must be *p's* multiple-nodes and *q's* multiple-nodes on P^N_0 and P^N_L. Lemma 3 and Lemma 4 show that, once a *p's* multiple-node occurs on P^N_0 or P^N_L, there are always *p's* multiple-nodes on the path. By theorem 1, all the *p's* multiple-nodes periodically distribute on the path. By Theorem 2 and Theorem 11, there are always *p's* multiple-nodes on both P^N_0 and P^N_L.

4. Conclusion and Future Work

Looking through the theorems and corollaries proved in previous sections, one can easily know that, for an odd composite integer *N*, with the help of the valuated binary tree T_N, odd integers that have a common divisor with *N* can always be found along the path P_0^N and P_L^N. This obviously provides a foundation for people to design algorithm for factoring *N* by searching along the path P_0^N and P_L^N the nodes that have common divisors with *N*. By formulas $N^N_{(k,-1)}2^kN-(2^k+1)$ and $N^N_{(k,0)}=2^kN-(2^k-1)$, it knows that the algorithm can be highly related with 2^k+1 and 2^k-1 modulus to *N's* divisors. In fact, the famous Pollard *p*-1 method is the one to find the greatest common divisor between 2^k-1 mod *N* and *N.* So this paper proved the validity of the Pollard *p*-1 method in a different way. In addition, this paper also points out new direction beyond the Pollard *p*-1 method. In the future, work will be done on finding more marvelous properties of the valuated binary tree and designing efficient algorithms to factorize big integers.

Acknowledgment

The research work is supported by the State Key Laboratory of Mathematical Engineering and Advanced Computing under Open Project Program No.2017A01, Department of Guangdong Science and Technology under project 2015A010104011, Foshan Bureau of Science and Technology under projects 2016AG100311, Project gg040981 from Foshan University. The authors sincerely present thanks to them all.

References

[1] Wang, X. (2016). Valuated binary tree: A new approach in study of integers. *International Journal of Scientific and Innovative Mathematical Research*, *4(3)*, 63-67.

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

[3] Wang, X. (2017). Two more symmetric properties of odd numbers. *IOSR Journal of Mathematics*, *13(3 Ver.II)*, 37-40.

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

[5] Wang, X. (2018). T3 Tree and its traits in understanding integers. *Advances in Pure Mathematics*, *8(5)*, 494-507.

[6] Rosen, K. H. (2011). *Elementary Number Theory and Its Applications* (6th edition). Addison-Wesley.

Xingbo Wang was born in Hubei, China. He got his master and doctor's degree at National University of Defense Technology of China and had been a staff in charge of researching and developing CAD/CAM/NC technologies in the university. Since 2010, he has been a professor in Foshan University with research interests in computer application and information security. He is now the chief of Guangdong engineering center of information security for intelligent manufacturing system. Prof. WANG was in charge of more than 40 projects including projects from the National Science Foundation Committee, published 8 books and over 90 papers related with mathematics, computer science and mechatronic engineering, and invented 30 more patents in the related fields.

Guo Hongqiang was born in Hebei. He received a bachelor's degree at Hefei University of Technology and became a graduate student of Foshan University in 2017. He is now a member of Guangdong engineering center of information security for intelligent manufacturing system.