Analysis of the Number of Distinct Prime Factors of $t(\alpha^n - \beta^n)$

Zhengzhou Foreign Language School
Jianqiao Xia, Yuxiang Jin, Mengzhe Zhang
Advisor: Siqing Cao

Abstract

This paper is inspired by an IMO problem which demonstrates that $2^{\prod_{i=1}^{k} p_i} + 1$ has at least 4^k positive divisors, where p_i is odd prime greater than 3[1]. In this paper, we generalized the conclusion. In this process, we proved a theorem which happens to be a corollary of Zsigmondy Theorem[2]. Using this theorem we proved that $a^n + 1$ has at least $\mathrm{d}(f(n))$ distinct prime factors when $3 \nmid n$, and $\mathrm{d}(f(n)) - 1$ when $3 \mid n$, where $f(n)$ stands for the greatest odd divisor of n, $\mathrm{d}(n)$ stands for the number of positive divisors of n. We generalized the result again by including the irrational numbers. We proved that there exists a constant M such that $t(\alpha^n - \beta^n)$ has at least $\frac{d(n)}{\Omega(n)+1} - M$ distinct prime factors.

[Keywords]: Zsigmondy Theorem, Möbius Inversion, prime, divisor, linear recursion sequence

CONTENTS

Section Zero: Notations

In this paper, we used the following notations. We have listed their definitions in the following chart will use them directly in our paper.

$f(n)$	The greatest odd divisor of n.
$\mathrm{d}(n)$	The number of distinct positive factors of n.
p_i	Prime number.
(a,b)	The greatest common divisor of a and b.
$a \nmid b$	b can not be divided by a.
$a \mid b$	b can be divided by a.
$a^n \parallel b$	$a^n \mid b$ while $a^{n+1} \nmid b$.
$[a,b]$	The least common multiple of a and b.
$\binom{a}{b}$	$\frac{a!}{b!(a-b)!}$.
$a \equiv b \ (mod\ p)$	a and b have the same residue modulo p.
$\prod_{a=1}^{k} p_a$	The product of p_1, p_2, p_3, … p_k.
$\sum_{a=1}^{k} p_a$	The sum of p_1, p_2, p_3, … p_k.
$\exists$	Exist.
$\forall$	For all.
$\varphi(n)$	Euler's function. It stands for the number of positive integers co-prime to and smaller than n.
N_+	The set of all positive integers.
$\mu(n)$	Möbius function. $\mu(n) = 1$ if n is a square-free positive integer with an even number of prime factors. $\mu(n) = -1$ if n is a square-free positive integer with an odd number of prime factors. $\mu(n) = 0$ if n has a squared prime factor.
$\Omega(n)$	The number of prime factors of n (the number of repetition counts).

Section One: Lemmas

In order to prove our conclusion, we first need two pertinent lemmas. Following are our proofs. The first lemma is a conclusion often found in mathematical competitions[3] while the second is our corollary.

Lemma One

Let $a \geq 2$, p be an odd prime, $a, \alpha, \beta, n \in N_+$, n is an odd integer, assume $p^\alpha \parallel a+1$, $p^\beta \parallel n$, then

$$p^{\alpha+\beta} \parallel a^n + 1. \tag{1.1.1}$$

Proof:

Since $p^\alpha \parallel a+1$, let $a = kp^\alpha - 1$, $(k,p) = 1$, then

$$a^n + 1 = (kp^\alpha - 1)^n + 1 = \sum_{i=1}^{n} (-1)^{n-i} \binom{n}{i} k^i p^{\propto i}. \tag{1.1.2}$$

Our main idea is to prove that among the sum of n items above, the index of p in the first item is smaller than that in any other item. Since then, the index of first item decides the index of the whole.

For $i = 1$, $p^{\alpha+\beta} \parallel (-1)^{n-1} nkp^{\propto}$.

For $i \geq 2$, we are familiar that

$$\binom{n}{i} = \frac{n}{i}\binom{n-1}{i-1}. \tag{1.1.3}$$

Let $p^\gamma \parallel i$, then

$$p^{\beta-\gamma} \mid \frac{n}{i}\binom{n-1}{i-1} = \binom{n}{i}. \tag{1.1.4}$$

Notice that here $\beta - \gamma$ is not necessary to be positive, but this won't interfere with our proof.

Therefore the index of p in $(-1)^{n-i}\binom{n}{i}k^i p^{\propto i}$ is at least $\alpha i + \beta - \gamma$. We shall prove that it is greater than $\alpha + \beta$, which is the index of first item.

Since $p^\gamma \parallel i$, we know that i is very large, specifically we have

$$i \geq p^\gamma \geq 3^\gamma = (1+2)^\gamma \geq 1 + 2\gamma. \tag{1.1.5}$$

If $\gamma \neq 0$, then

$$\alpha i + \beta - \gamma = \alpha + \beta + (\alpha(i-1) - \gamma) \geq \alpha + \beta + \gamma(2\alpha - 1) \geq \alpha + \beta + 1. \tag{1.1.6}$$

If $\gamma = 0$, then

$$\alpha i + \beta - \gamma \geq 2\alpha + \beta \geq \alpha + \beta + 1. \tag{1.1.7}$$

Based on what have been argued above, we have

$$p^{\alpha+\beta} \parallel \sum_{i=1}^{n} (-1)^{n-i}\binom{n}{i} k^i p^{\propto i} = a^n + 1. \tag{1.1.8}$$

Lemma Two

Let $a \geq 2,\ p$ is an odd prime, $a \in N_+$, then $a^p + 1$ must have a prime divisor that does not divide $a+1$, unless $a = 2,\ p = 3$.

Proof:

First we can prove that $a^p + 1 \geq p(a+1)$, and $a^p + 1 = p(a+1)$ if and only if $a = 2,\ p = 3$.
This fact looks trivial at first, but it is important to deal with details clearly.
In fact, since p is an odd prime, $p \geq 3$.
Then

$$\begin{aligned} a^p + 1 &\geq \left(1 + (a-1)\right)^p + 1 \\ &\geq 2 + \binom{p}{1}(a-1) + \binom{p}{2}(a-1)^2 + (a-1)^p. \end{aligned} \tag{1.2.1}$$

Because $a \geq 2$, we have $a - 1 \geq 1,\ (a-1)^2 \geq 1,\ (a-1)^p \geq 1$.
Therefore

$$a^p + 1 \geq 3 + p(a-1) + \frac{p(p-1)}{2} = p(a+1) + \frac{(p-2)(p-3)}{2}. \tag{1.2.2}$$

When $p = 3$, $\frac{(p-2)(p-3)}{2} = 0$. We also have $a^p + 1 = p(a+1)$, if and only if $a = 2$.

When $p > 3$, $\frac{(p-2)(p-3)}{2} > 0$.

Therefore, we proved our earlier conclusion.
Suppose lemma 2 is incorrect, then $\forall q$ is prime, $q \mid a^p + 1$, we have $q \mid a + 1$.
Let $q^\alpha \parallel a + 1,\ \alpha \in N_+$.
According to lemma 1,
If $q \neq p,\ q^\alpha \parallel a^p + 1$.
If $q = p,\ q^{\alpha+1} \parallel a^p + 1$.
Therefore, the index of prime $q \neq p$ in $a^p + 1$ is no more than that in $a + 1$, the index of p is no more than that in $a + 1$.
$\therefore a^p + 1 \leq p(a+1)$. This contradicts our earlier conclusion.
Therefore, the supposition is fallacious and lemma 2 is correct.

Section Two: The First Conclusion

Using the two preceding lemmas, we study the problem and guess that a^n+1 always has a "unique" prime factor. Hence, when n is odd, we could acquire many different prime factors considering a^n+1 has many ways to be factorized. However, only by considering $2^3+1=3^2$, we know that the guess is fallacious. Luckily, this is the only exception. Following is our proof.

Theorem One

$\forall a \geq 2, n \geq 4$ or $a \geq 3, n \geq 2$, n is odd, there exists a prime p, such that

$$p \mid a^n+1, \text{and } \forall m < n, m \in N_+, p \nmid a^m+1. \qquad (2.1.1)$$

Proof:

Suppose that the conclusion is fallacious. Then for every prime divisor p of a^n+1, there exists $m \in N_+$, $m < n$, such that $p \mid a^m+1$.

We take the smallest m satisfying the above condition. We shall prove $m \mid n$ first. It is a conclusion similar to that of the order, the proof is also similar. Just use the division algorithm and some idea from infinite descent.

If $m \nmid n$, let $n = sm + r$, $r, s \in N_+$, $0 < r < m$. Then

$$0 \equiv a^n+1 \equiv a^{sm+r}+1 \equiv (a^m)^s a^r + 1 \equiv (-1)^s a^r + 1 \ (mod\ p). \qquad (2.1.2)$$

When $2 \nmid s$, $a^r \equiv 1\ (mod\, p)$, then

$$0 \equiv a^m+1 \equiv a^{m-r}a^r + 1 \equiv a^{m-r}+1\ (mod\, p), \qquad (2.1.3)$$

which means $p \mid a^{m-r}+1$.

Since m is the smallest, we have $m - r \geq m$, $r \leq 0$.

This contradicts with $0 < r < m$.

If $2 \mid s$, then $0 \equiv a^r + 1\ (mod\ p)$.

Since m is the smallest, $r \geq m$.

This contradicts $0 < r < m$.

Based on what have been argued above,, $m \mid n$.

If n is prime, then for every prime factor p of a^n+1, have there existed $m < n$, $p \mid a^m+1$ should we have $m \mid n$.

Hence $m = 1$. From lemma 2 we know that theorem 1 is correct.

If n is composite, let the standard factorization of n be

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}. \qquad (2.1.4)$$

Here k represents the number of distinct prime factors of n.

Let $n_i = \frac{n}{p_i}$, $(i = 1,2,3,\dots,k)$.

From our earlier arguments, we know that for any prime $p \mid a^n+1$,

$\exists m \in N_+$, $m < n$, $m \mid n$, $p \mid a^m+1$.

Hence, there exists integer i, such that $m \mid n_i$. For every prime factor q of $a^{n_i}+1$

Let $q^\alpha \parallel a^{n_i}+1$, $\alpha \in N$. According to lemma 1,

When $q = p_i$, $q^{\alpha+1} \parallel a^n + 1$.
When $q \neq p_i$, $q^{\alpha+1} \parallel a^n + 1$.
Hence we have

$$a^n + 1 | [\, a^{n_1} + 1, a^{n_2} + 1, \dots, a^{n_k} + 1] \prod_{i=1}^{k} p_i. \tag{2.1.5}$$

By observing the above divisibility, we find that (2.1.5) is not likely to be true. In fact, the right side is $a^{\varphi(n)}$ approximately, whereas the left side is greater. Following are detailed analysis on the scale of each side, especially the right.
We want to prove

$$a^n + 1 > [\, a^{n_1} + 1, a^{n_2} + 1, \dots, a^{n_k} + 1] \prod_{i=1}^{k} p_i, \tag{2.1.6}$$

which, in another word means

$$a^n \geq [\, a^{n_1} + 1, a^{n_2} + 1, \dots, a^{n_k} + 1] \prod_{i=1}^{k} p_i. \tag{2.1.7}$$

However, the least common multiple is not easy to estimate, so we shall use a conclusion to simplify the right side. That is when u, v are odd, we have

$$(a^u + 1, a^v + 1) = a^{(u,v)} + 1. \tag{2.1.8}$$

We see that when u, v are odd, we have

$$(a^u + 1, a^v + 1) \mid (a^{2u} - 1, a^{2v} - 1) = a^{2(v,u)} - 1. \tag{2.1.9}$$

While

$$\left(a^{(u,v)} - 1, a^u + 1\right) = \left(a^{(u,v)} - 1, a^u - 1 + 2\right) = \left(a^{(u,v)} - 1, 2\right). \tag{2.1.10}$$

Since we have

$$a^{(u,v)} + 1 \mid a^u + 1,\ \ a^{(u,v)} + 1 \mid a^u + 1. \tag{2.1.11}$$

We could acquire

$$a^{(u,v)} + 1 \mid (a^u + 1, a^v + 1). \tag{2.1.12}$$

If a is even, then $\left(a^{(u,v)} - 1, 2\right) = 1$, $(a^u + 1, a^v + 1) = a^{(u,v)} + 1$.
If a is odd, then $\left(a^{(u,v)} - 1, 2\right) = 2$, we can consider the index of 2 in $a^u + 1$ and $a^{(u,v)} + 1$.
Let $(u, v) = d$, $u = ld$, such that d is odd, therefore we have

$$a^u + 1 = (a^d + 1) \sum_{s=0}^{l-1} a^{sd} (-1)^s. \tag{2.1.13}$$

We notice that this addition consists of an odd number (l) of odd numbers. Hence, the result is odd.
Therefore, the indexes of 2 in $a^u + 1$ and $a^{(u,v)} + 1$ are equal, and we still have

$$(a^u + 1, a^v + 1) = a^{(u,v)} + 1. \tag{2.1.14}$$

Then

$$(a^{n_{i_1}}+1, a^{n_{i_2}}+1, \ldots, a^{n_{i_s}}+1) = a^{(n_{i_1}, n_{i_2}, \ldots, n_{i_s})}+1.$$

Now we will use cross classification to represent the least common multiple:

$$\begin{aligned}[& a^{n_1}+1, a^{n_2}+1, \ldots, a^{n_k}+1] \\ & = \prod_{\substack{1\le i_1<i_2,\ldots,<i_t\le k \\ 1\le t\le k}} (a^{n_{i_1}}+1, a^{n_{i_2}}+1, \ldots, a^{n_{i_t}} \\ & + 1)^{(-1)^{t+1}} \\ & = \prod_{\substack{1\le i_1<i_2,\ldots,<i_t\le k \\ 1\le t\le k}} (a^{(n_{i_1}, n_{i_2}, \ldots, n_{i_s})}+1)^{(-1)^{t+1}}.\end{aligned} \tag{2.1.15}$$

Notice that for every positive integer m, we have

$$a^m < a^m+1 < a^m\left(1+\frac{1}{a}\right). \tag{2.1.16}$$

Hence

$$\begin{aligned}& \prod_{\substack{1\le i_1<i_2,\ldots,<i_t\le k \\ 1\le t\le k}} (a^{(n_{i_1}, n_{i_2}, \ldots, n_{i_s})}+1)^{(-1)^{t+1}} \\ \le & \prod_{\substack{1\le i_1<i_2,\ldots,<i_t\le k \\ 1\le t\le k}} a^{(n_{i_1}, n_{i_2}, \ldots, n_{i_s})^{(-1)^{t+1}}} \prod_{\substack{1\le i_1<i_2,\ldots,<i_t\le k \\ 1\le t\le k \\ t \text{ is odd}}} \left(1+\frac{1}{a}\right).\end{aligned} \tag{2.1.17}$$

We shall now simplify our right side of this inequality.

The first product is a product some power of a. The power is

$$\sum_{\substack{1\le i_1<i_2,\ldots,<i_t\le k \\ 1\le t\le k}} (n_{i_1}, n_{i_2}, \ldots, n_{i_s})^{(-1)^{t+1}}. \tag{2.1.18}$$

Notice that

$$(n_{i_1}, n_{i_2}, \ldots, n_{i_s}) = \left(\frac{n}{p_{i_1}}, \frac{n}{p_{i_2}}, \ldots, \frac{n}{p_{i_s}}\right) = \frac{n}{p_{i_1}p_{i_{2,\ldots,}}p_{i_s}}. \tag{2.1.19}$$

So the power of a is

$$\begin{aligned}\sum_{\substack{1\le i_1<i_2,\ldots,<i_t\le k \\ 1\le t\le k}} \left(\frac{n}{p_{i_1}p_{i_{2,\ldots,}}p_{i_s}}\right)^{(-1)^{t+1}} & = n(1-\prod_{i=1}^{k}(1-\frac{1}{p_i})) \\ & = n-\varphi(n).\end{aligned} \tag{2.1.20}$$

The second product of the right side is

$$\prod_{\substack{1\le i_1<i_2,\ldots,<i_t\le k \\ 1\le t\le k \\ t \text{ is odd}}} \left(1+\frac{1}{a}\right) = \left(1+\frac{1}{a}\right)^{\sum_{t \text{ is odd}}\binom{k}{t}}. \tag{2.1.21}$$

Since

$$\sum_{t \text{ is odd}} \binom{k}{t} = \frac{\left(1+(-1)\right)^k + (1+1)^k}{2} = 2^{k-1}. \tag{2.1.22}$$

The right side of (2.1.17) can be written as

$$a^{n-\varphi(n)}\left(1+\frac{1}{a}\right)^{2^{k-1}}\prod_{i=1}^{k} p_i. \tag{2.1.23}$$

Now (2.1.7) is equivalent to

$$a^{\varphi(n)} \geq \left(1+\frac{1}{a}\right)^{2^{k-1}}\prod_{i=1}^{k} p_i. \tag{2.1.24}$$

From a direct sense, the above inequality is trivial, since in the left side, the power of a is already $\varphi(n)$, which is approximately $\prod_{i=1}^{k} p_i$. Following is detailed proof. Basically, we are trying to show how small $\left(1+\frac{1}{a}\right)^{2^{k-1}}$ is.

First, we have

$$\varphi(n) = n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) = \prod_{i=1}^{k} p_i^{\alpha_i}\left(1-\frac{1}{p_i}\right) \geq \prod_{i=1}^{k} (p_i - 1) \geq 2^k. \tag{2.1.25}$$

Therefore

$$\frac{a^{\varphi(n)}}{\left(1+\frac{1}{a}\right)^{2^{k-1}}} \geq \left(\frac{a}{\sqrt{1+\frac{1}{a}}}\right)^{\varphi(n)} \geq \left(\frac{2\sqrt{6}}{3}\right)^{\varphi(n)} \geq \left(\frac{3}{2}\right)^{\varphi(n)}. \tag{2.1.26}$$

In the above inequality, we used that a is not less than 2 and $\frac{a}{\sqrt{1+\frac{1}{a}}}$ increase monotonously.

Also, we have

$$\left(\frac{3}{2}\right)^{\varphi(n)} \geq 1 + \frac{1}{2}\varphi(n) + \frac{1}{4}\varphi(n)^2 > \frac{1}{4}\varphi(n)^2. \tag{2.1.27}$$

Now we only need to prove

$$\frac{1}{4}\varphi(n)^2 \geq \prod_{i=1}^{k} p_i. \tag{2.1.28}$$

Since n is composite, we have $k \geq 2 \ or \ \alpha_1 \geq 2$, $k = 1$.

First case: $k \geq 2$.

At this time, we acquire

$$\varphi(n)^2 \geq \prod_{i=1}^{k} (p_i - 1)^2. \tag{2.1.29}$$

So

$$\frac{\varphi(n)^2}{\prod_{i=1}^{k} p_i} \geq \prod_{i=1}^{k} \frac{(p_i-1)^2}{p_i} \geq \frac{(p_1-1)^2}{p_1}\frac{(p_2-1)^2}{p_2} \geq \frac{(3-1)^2}{3}\frac{(5-1)^2}{5} = \frac{64}{15}. \tag{2.1.30}$$

Hence

$$\frac{1}{4}\varphi(n)^2 \geq \frac{16}{15}\prod_{i=1}^{k} p_i > \prod_{i=1}^{k} p_i. \tag{2.1.31}$$

Therefore

$$a^{\varphi(n)} \geq \left(1+\frac{1}{a}\right)^{2^{k-1}} \prod_{i=1}^{k} p_i. \tag{2.1.32}$$

Second case: $\alpha_1 \geq 2$， $k = 1$.
At this time, we acquire

$$\frac{1}{4}\varphi(n)^2 \geq \frac{1}{4}{p_1}^2(p_1-1)^2 > p_1. \tag{2.1.33}$$

So

$$a^{\varphi(n)} \geq \left(1+\frac{1}{a}\right)^{2^{k-1}} \prod_{i=1}^{k} p_i. \tag{2.1.34}$$

Above all, the inequality (2.1.7) holds, so (2.1.5) cannot be true. Contradiction!
Hence our Theorem 1 is correct.

Section Three: The Second Conclusion and a Special Case of the Dirichlet's Theorem

With the preceding theorem, we could easily acquire one of the conclusions of our thesis and give an estimation of the number of prime factors of $a^n + 1$. Meanwhile, we notice that theorem one can help us provide the proof of a special case of the Dirichlet's Theorem, the case when the first term is 1.

When n is even, let $n = 2^k n_1$, where n_1 is the greatest odd factor of n. Then we have $a^n + 1 = (a^{2^k})^{n_1} + 1$. Therefore, we can convert this case to the case when n is odd. Therefore, in theorem 2 we only discuss the case when n is odd.

Theorem Two

Let $a \geq 2$, n be an odd positive number. Then when $3 \mid n$ or $3 \nmid n$, $a^n + 1$ has at least $\mathrm{d}(n) - 1$ or $\mathrm{d}(n)$ prime factors, respectively.

Proof:

For any divisor m of $n\,(m \neq 3)$, from theorem 1 we know that there exists a prime p such that

$$p \mid a^m + 1, \text{and } \forall k \in N_+, k < m, p \nmid a^k + 1. \tag{3.1.1}$$

Let $p = p(m)$. Since n is an odd positive number, we have

$$a^m + 1 \mid a^n + 1. \tag{3.1.2}$$

Hence, all $p(m)$ divide $a^n + 1$.

Next we prove $p(i) \neq p(j)$ ($i \neq j$).

In fact, had there existed $i \neq j$, while i, j are both positive divisors of n, such that $p(i) = p(j)$, we could assume $i < j$.

From the definition of $p(j)$, we have

$$\forall k \in N_+, k < j, p \nmid a^k + 1. \tag{3.1.3}$$

However, $p(i) = p(j)$, from the definition of $p(i)$, we have

$$p(i) \mid a^i + 1. \tag{3.1.4}$$

This is a contradiction.

Hence, when $3 \mid n$, we acquire $\mathrm{d}(n) - 1$ different prime factors.

When $3 \nmid n$, we acquire $\mathrm{d}(n)$ different prime factors.

Theorem Three

Let $n \in N_+$, then the sequence $\{tn+1\}_{t=1}^{\infty}$ includes an infinite number of prime terms.

Proof:
Let $n = 2^k n_1$, such that n_1 is odd. Now we take $\{a_k\}_{k=1}^{\infty}$ in that

$$a_1 = 3^{2^k}, a_{m+1} = \left(\prod_{k=1}^{m}(a_k^{n_1}+1)\right)^{2^k}. \tag{3.2.1}$$

We know then that $a_1^{n_1}+1,\ a_2^{n_1}+1,\ a_3^{n_1}+1, \dots$ are all respectively co-prime.
From Theorem 1, we know that
For any positive integer i, there exists a prime $p_i \mid a_i^{n_1}+1$, such that

$$\forall m < n, m \in N_+, p_i \nmid a_i^{m} + 1. \tag{3.2.2}$$

From the definition of $\{tn+1\}_{t=1}^{\infty}$, we know that these exists $b_i \in N_+$, such that a_i=$b_i^{2^k}$.

Hence, we have $p_i \mid a_i^{2n_1} - 1 = b_i^{2^{k+1}n_1} - 1$.

Let the order of b_i modulo p_i be t: t is the smallest integer that satisfy

$$p_i \mid b_i^t - 1. \tag{3.2.3}$$

From the properties of order, we have

$$t \mid 2^{k+1}n_1. \tag{3.2.4}$$

Since we obviously also have $p_i \nmid b_i^{2^k n_1} - 1$, we have

$$t \nmid 2^k n_1. \tag{3.2.5}$$

Therefore

$$2^{k+1} \parallel t. \tag{3.2.6}$$

As a result, let $t = 2^{k+1}n_2$, such that

$$n_2 \mid n_1. \tag{3.2.7}$$

We also have $b_i^t - 1 = \left(b_i^{\frac{t}{2}} - 1\right)\left(b_i^{\frac{t}{2}} + 1\right)$,

But since $\frac{t}{2} < t$, we have $p_i \nmid b_i^{\frac{t}{2}} - 1$.

Hence, $p_i \mid b_i^{\frac{t}{2}} + 1 = b_i^{2^k n_2} + 1 = a_i^{n_2} + 1$.

According to (3.2.2), $n_2 \geq n_1$, but from (3.2.7), $n_1 \geq n_2$.
Therefore, $n_1 = n_2$, $t = 2^{k+1}n_1 = 2n$.
According to the Fermat's Little Theorem, we know

$$p_i \mid b_i^{p_i-1} - 1. \tag{3.2.8}$$

As a result, $2n \mid p_i - 1$, $p_i \in \{tn+1\}_{t=1}^{\infty}$.
Since $a_1^{n_1}+1$, $a_2^{n_1}+1$, $a_3^{n_1}+1$, … are all respectively co-prime, we know that p_i $(i = 1, 2, 3 \dots)$ are all different.
Hence, we have found an infinite number of prime terms in $\{tn+1\}_{t=1}^{\infty}$., and the proof is

complete.

Section Four: A Second Thought of Theorem One

Considering the preceding proof, we can see that we almost only used the property of sequence $\{a^n+1\}_{n=1}^{\infty}$ that every two items of this sequence have their greatest common divisor in this sequence. In another word, $(a^u+1, a^v+1) = a^{(u,v)}+1$.
Using the equation from Möbius inversion, we can prove a generalized conclusion.

Theorem Four

If a sequence of positive integers $\{x_n\}_{n=1}^{\infty}$ satisfies the following property:

$$\forall\, m,n \in N_+, (x_m, x_n) = x_{(m,n)}, \tag{4.1.1}$$

then there exists a sequence of positive integers $\{y_n\}_{n=1}^{\infty}$, such that

$$x_n = \prod_{d|n} y_d. \tag{4.1.2}$$

Proof:
First, let's analyze what should $\{y_n\}_{n=1}^{\infty}$ satisfy. According to Möbius inversion, (4.1.2) can be transformed to

$$y_n = \prod_{d|n} {x_d}^{\mu(\frac{n}{d})}, \tag{4.1.3}$$

where $\mu(n)$ denotes Möbius Function.
Hence, we only need to prove that the right side of (4.1.3) is a positive integer.

It is clear that d needs to be concerned only when $\mu(\frac{n}{d}) \neq 0$. In another word, we only consider such d that $\frac{n}{d}$ is square-free.

We use the same notation in theorem 1 and recollect the following two definitions:

$$n_i = \frac{n}{p_i}. \tag{4.1.4}$$

k stands for the number of distinct prime factors of n.

Since we know that

$$\frac{n}{p_{i_1}p_{i_{2,\ldots,}}p_{i_s}} = \left(\frac{n}{p_{i_1}}, \frac{n}{p_{i_2}}, \ldots, \frac{n}{p_{i_s}}\right) = \left(n_{i_1}, n_{i_2}, \ldots, n_{i_s}\right), \tag{4.1.5}$$

we can represent y_n as

$$y_n = x_n \times \prod_{\substack{1\le i_1<i_2,\ldots,<i_t\le k \\ 1\le t\le k}} x_{(n_{i_1}, n_{i_2}, \ldots, n_{i_t})}{}^{(-1)^t}. \tag{4.1.6}$$

We notice that

$$x_{(n_{i_1}, n_{i_2}, \ldots, n_{i_s})} = \left(x_{n_{i_1}}, x_{n_{i_2}}, \ldots, x_{n_{i_t}}\right). \tag{4.1.7}$$

Considering the formula of cross classification or exclusion and inclusion theorem, we can find that the above equation can be simplified to be

$$y_n = \frac{x_n}{[x_{n_1}, x_{n_2}, \dots, x_{n_k}]}. \tag{4.1.8}$$

Since $(x_{n_1}, x_n) = x_{(n_1,n)} = x_{n_1}$, we get $x_{n_1} | x_n$. In other word, x_n is a multiple of every x_{n_i}, so it has to be the multiple of their least common multiple, $[x_{n_1}, x_{n_2}, \dots, x_{n_k}]$. Therefore, we have y_n is an integer.

We notice that since every x_{n_i} is positive, y_n is also positive.

Hence, y_n is a positive integer and the proof of theorem 4 is complete.

From the representation of x_n, we have enough confidence to find many prime divisors of x_n. At least we have already proven that it contains many divisors. A direct thought is to prove that y_n is greater than 1 and co-prime to each other. However, this guess is not totally true; following is a correct and close statement.

Theorem Five

In the sequence $\{y_n\}_{n=1}^{\infty}$ from theorem four, we have the following property: if $m \nmid n$ and $n \nmid m$, then

$$(y_m, y_n) = 1. \tag{4.2.1}$$

Proof:
We mentioned that the sequence $\{x_n\}_{n=1}^{\infty}$ has a property that $(x_m, x_n) = x_{(m,n)}$.
Hence, we have

$$\left(\frac{x_m}{x_{(m,n)}}, \frac{x_n}{x_{(m,n)}}\right) = 1. \tag{4.2.2}$$

From the representation of x_m, x_n, and $x_{(m,n)}$, we have

$$\frac{x_m}{x_{(m,n)}} = \prod_{\substack{d|m \\ d\nmid(m,n)}} y_d; \tag{4.2.3}$$

$$\frac{x_n}{x_{(m,n)}} = \prod_{\substack{d|n \\ d\nmid(m,n)}} y_d. \tag{4.2.4}$$

Since $m \nmid n$ and $n \nmid m$, we know that $(m, n) < m, n$.
So, we could acquire

$$y_m | \prod_{\substack{d|m \\ d\nmid(m,n)}} y_d = \frac{x_m}{x_{(m,n)}}; \tag{4.2.5}$$

$$y_n | \prod_{\substack{d|m \\ d\nmid(m,n)}} y_d = \frac{x_m}{x_{(m,n)}}. \tag{4.2.6}$$

Therefore, we know that

$$(y_m, y_n) = 1, \tag{4.2.7}$$

and the proof is complete.

Section Five: Preparation for the Final Conclusion

Next we will choose a specific sequence $\{x_n\}_{n=1}^{\infty}$ and consider the number of prime factors of each term. In order to meet the requirement that $(x_m,x_n)=x_{(m,n)}$, we consider a familiar sequence $\{t(\alpha^n-\beta^n)\}_{n=o}^{\infty}$, where α, β, and t are real numbers.

Theorem Six

Let $x_n=t(\alpha^n-\beta^n)$ $(n\in N)$, where $\alpha>\beta$, α and β are the roots of the equation $x^2-ux+v=0$, in which u and v are co-prime positive integers, $u^2>4v$, and $u>v$. Here $t=\frac{k}{\alpha-\beta}$ in which $k\in N_+$, $(k,v)=1$.

Then we have

$$\forall\, m,n\in N_+,(x_m,x_n)=x_{(m,n)}. \tag{5.1.1}$$

Proof:

First, we can prove that

$$x_n\ (n\neq 0)\in N_+. \tag{5.1.2}$$

We see that $x_0=0,\ x_1=k.$

From the definition of the sequence, we know that

$$x_{n+1}=ux_n-vx_{n-1}. \tag{5.1.3}$$

Therefore, using mathematical induction, we can easily prove (5.1.2).

Next, we use Euclidean Algorithm to calculate (x_m,x_n).

Since $m,n\in N_+$, we can assume $m<n$, then

$$\begin{aligned} x_n-x_m(\alpha^{n-m}+\beta^{n-m}) &= -t(\alpha\beta)^m(\alpha^{n-2m}-\beta^{n-2m}) \\ &= t(\alpha\beta)^{n-m}(\alpha^{2m-n}-\beta^{2m-n}). \end{aligned} \tag{5.1.4}$$

We notice that $\alpha^{n-m}+\beta^{n-m}$ is symmetrical about α and β, hence it can be written as a polynomial of $\alpha+\beta$ and $\alpha\beta$. Therefore, $\alpha^{n-m}+\beta^{n-m}$ is an integer.

Hence

$$\begin{aligned} (x_m,x_n) &= \left(x_m,-t(\alpha\beta)^m(\alpha^{n-2m}-\beta^{n-2m})\right) \\ &= \left(x_m,t(\alpha\beta)^{n-m}(\alpha^{2m-n}-\beta^{2m-n})\right). \end{aligned} \tag{5.1.5}$$

Because we have (5.1.3), we can acquire

$$x_m\equiv ux_{m-1}(mod v). \tag{5.1.6}$$

We know that u,v are co-prime positive integers, and $x_1=k$, which is also co-prime to v, so

$$\forall\, m\in N_+,(x_m,v)=1. \tag{5.1.7}$$

In other word,

$$\forall\, m\in N_+,(x_m,\alpha\beta)=1. \tag{5.1.8}$$

Then from (5.1.5), we have:

When $-2m\geq 0$, $(x_m,x_n)=(x_m,x_{n-2m})$;

When $-2m\leq 0$, $(x_m,x_n)=(x_m,x_{2m-n})$.

In either case, the superscripts have the same greatest common divisor. In other word, we know

$$(m,n) = (m, n-2m) = (m, 2m-n). \quad (5.1.9)$$

Since the smaller one of the superscript always decrease, this calculation must end in finite steps. At this time, we can suppose we have

$$(x_m, x_n) = (x_i, x_j), \quad (5.1.10)$$

In which either $i = 0$ or $j = 0$. In either case, $i\ or\ j = (i,j) = (m,n)$.
Also, we know $(x_i, x_j) = x_i$ or x_j (because $x_0 = 0$).
So we have

$$(x_m, x_n) = (x_i, x_j) = x_i \text{ or } x_j = x_{(i,j)} = x_{(m,n)}, \quad (5.1.11)$$

and the proof is complete.

Although we already proved that the sequence $\{t(\alpha^n - \beta^n)\}_{n=0}^{\infty}$ satisfies our conditions in theorem four, we still need to prove that the corresponding sequence $\{y_n\}_{n=1}^{\infty}$ satisfies the condition that $y_n > 1$, otherwise we will not find many prime factors even though we have represented $t(\alpha^n - \beta^n)$ as the product of many positive integers.

Theorem Seven

Let $\{x_n\}$ be the same sequence mentioned in the theorem six and let y_n be its corresponding sequence as described in theorem four. Then there exists a positive integer M, such that once $n > M$, we have

$$y_n > 1 \tag{5.2.1}$$

Proof:

First, we observe that there exists two constants c_1, c_2 such that

$$c_1\alpha^n < x_n = t(\alpha^n - \beta^n) < c_2\alpha^n, \tag{5.2.2}$$

because $|(\frac{\beta}{\alpha})^n|$ is sufficiently small when n is sufficiently big.

Now we recall the representation of y_n from theorem four:

$$y_n = x_n \times \prod_{\substack{1\le i_1<i_2,\ldots,<i_s\le k\\ 1\le s\le k}} x_{(n_{i_1},n_{i_2},\ldots,n_{i_s})}{}^{(-1)^s}. \tag{5.2.3}$$

When s is odd, we use the right side of (5.2.2) to estimate.
When s is even, we use the left side of (5.2.2) to estimate.
Then we have

$$y_n > \frac{{c_1}^{2^{k-1}}}{{c_2}^{2^{k-1}}} \times x_n \times \prod_{\substack{1\le i_1<i_2,\ldots,<i_s\le k\\ 1\le s\le k}} \alpha^{(n_{i_1},n_{i_2},\ldots,n_{i_s})^{(-1)^s}}. \tag{5.2.4}$$

In other word, there exists a constant c such that

$$y_n > c \times x_n \times \prod_{\substack{1\le i_1<i_2,\ldots,<i_s\le k\\ 1\le s\le k}} \alpha^{(n_{i_1},n_{i_2},\ldots,n_{i_s})^{(-1)^{s+1}}} = c\alpha^{\varphi(n)} \tag{5.2.5}$$

Since $\alpha > \beta$, and $\alpha\beta = v \in \mathrm{N}$, we have $\alpha > 1$.
Hence when n is sufficiently big, $\varphi(n)$ is sufficiently big. Then we have

$$y_n > c\alpha^{\varphi(n)} > 1, \tag{5.2.6}$$

and the proof is complete.

Section Six: The Final Theorem

Now, it is time to estimate the number of distinct prime factors of x_n and get the result.

Theorem Eight

Using all the same notations and definitions as mentioned in section four and five, we consider the sequence $\{x_n\}_{n=1}^{\infty} = \{t(\alpha^n - \beta^n)\}_{n=0}^{\infty}$. There exists a constant M such that x_n has at least $\frac{d(n)}{\Omega(n)+1} - M$ distinct prime factors.

Proof:
Our main idea is to find many divisors of n, such that anyone of them do not divide any other one. Consider the representation of x_n,

$$x_n = \prod_{d|n} y_d. \tag{6.1.1}$$

In fact, once we find $\frac{d(n)}{\Omega(n)+1}$ different items from the right side of (6.1.1), with every two of them co-prime, we can find $\frac{d(n)}{\Omega(n)+1} - M$ items greater than 1 and co-prime to each other. Hence we can find at least $\frac{d(n)}{\Omega(n)+1} - M$ prime factors.

We use the following method to find these divisors.
We choose all the divisors of n such that $\Omega(n) = e$, where e is an temporarily undetermined constant.
This method of choosing can guarantee that anyone of them do not divide any other one. In fact if $f|g$, then $\Omega(f) \leq \Omega(g)$, the equality is true only when $f = g$.
Now we will prove that there exists a value of e such that we can choose at least $\frac{d(n)}{\Omega(n)+1}$ divisors.
Let the standard factorization of n be

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}. \tag{6.1.2}$$

Then consider the polynomial

$$L(x) = \prod_{i=1}^{k} \sum_{j=0}^{\alpha_i} x^j. \tag{6.1.3}$$

The degree of this polynomial is $\Omega(n)$, and the sum of all the coefficients is $L(1) = d(n)$.
We can choose the term with the greatest coefficient. Suppose this term is x^r, then its coefficient is greater than the average value $\frac{d(n)}{\Omega(n)+1}$.

Consider the meaning of the exponent of each term, we know that its coefficient represents how many divisors we can choose using our method.
We now choose $e = r$, and the proof is complete.

Section Seven: Conclusion

In this paper, we mainly discussed the number of distinct prime factors of one specific kind of sequence $\{t(\alpha^n-\beta^n)\}_{n=0}^{\infty}$. For a more concrete example, we gave an estimation of distinct prime factors of sequence $\{a^n+1\}_{n=1}^{\infty}$. As a by-product, we proved a special case of the Dirichlet's Theorem. Following are our main results:

1. $\forall a \geq 2, n \geq 4$ or $a \geq 3, n \geq 2$, n is odd, there exists a prime p, such that
$$p \mid a^n+1, \text{and } \forall m < n, m \in N_+, p \nmid a^m+1.$$
2. Let $a \geq 2$, n be an odd positive number. Then when $3 \mid n$ or $3 \nmid n$, a^n+1 has at least $\mathrm{d}(n)-1$ or $\mathrm{d}(n)$ prime factors, respectively.
3. Let $n \in N_+$, then the sequence $\{tn+1\}_{t=1}^{\infty}$ includes an infinite number of prime terms.
4. Consider the sequence $\{x_n\}_{n=1}^{\infty}=\{t(\alpha^n-\beta^n)\}_{n=0}^{\infty}$. There exists a constant M such that x_n has at least $\frac{d(n)}{\Omega(n)+1}-M$ distinct prime factors.

References and Acknowledgements

[1]Zhigang Feng, *Elementary Number Theory*, Shanghai, Shanghai Scientific and Technical Publishers, 2009, P26-28
[2]Lola Thompson, *Zsigmondy Theorem*, Mathematical Excalibur, feb 2012
[3] Amir Hossein Parvardi , *Lifting the Exponent Lemma*, http://www.artofproblemsolving.com/Forum/viewtopic.php?t=393335 , 2014,7