J. Appl. Math. & Informatics Vol. **26***(2008), No. 5 - 6, pp. 1215 - 1219*
Website: http://www.kcam.biz

PRIME FACTORS OF $A^n + 1$

YONG SU SHIN

ABSTRACT. We find a necessary and sufficient condition that the prime factors of $A^m + 1$ and $A^n + 1$ coincide for odd positive integers $n > m \geq 1$. Moreover, we also find a necessary and sufficient condition that the set of all prime factors of $A^m + 1$ is a subset of those of $A^n + 1$ for $n > m \geq 1$.

AMS Mathematics Subject Classification : 13D40, 14M10
Key words and Phrases : Prime factors, greatest common divisors, and binomial coefficient.

1. Introduction

Let $\mathbb{Z}$ be the set of all integers and $\mathbb{Z}^+$ be the set of all positive integers. In [1], they showed some calculations of factorizations of positive integers of the form $A^n \pm 1$ when A is a positive integer with $A > 1$ and $n \in \mathbb{Z}^+$. In [3], they gave a necessary and sufficient condition that the prime factors of $A^m - 1$ and $A^n - 1$ coincide when $A \in \mathbb{Z}^+$ and $A > 1$. They also found a necessary and sufficient condition that the set of prime factors of $A^m - 1$ is a subset of those of $A^n - 1$ when $n > m \geq 1$.

In this paper, we find a necessary and sufficient condition that the prime factors of $A^m + 1$ are the same as those of $A^n + 1$ when $n > m \geq 1$ (see Theorem 3). Furthermore, we find a necessary and sufficient condition that the set of prime factors of $A^m + 1$ is a subset of those of $A^n + 1$ when $n > m \geq 1$ (see Corollary 4).

2. Prime Factors

First of all, we introduce some notations and recall some elementary facts in number theory (see [2] and [4] for more elementary details).

Received January 16, 2008. Revised June 7, 2008. Accepted June 10, 2008.
This paper was supported by a grant from Sungshin Women's University in 2008.

Remark 1. (a) We denote the *greatest common divisor* of two integers a and b by (a, b) where a and b are not both 0.

(b) Let a and b be in $\mathbb{Z}$ and $a = bq + c$ for some q and c in $\mathbb{Z}$. Then $(a, b) = (b, c)$.

(c) Let $a \in \mathbb{Z}$ with $|a| > 1$ and $n \in \mathbb{Z}^+$. Then

$$\frac{a^n - 1}{a - 1} = \left[\sum_{i=0}^{n-2} \binom{n}{i} (a-1)^{n-i-1}\right] + n$$

where $\binom{n}{i} = \frac{n!}{(n-i)!i!}$, a binomial coefficient (see [3]).

(d) Note that $3^x - 2^y = 1$ has no integer solution with $x > 2$.

Lemma 2. *Let m and n be odd positive integers with $(m, n) = 1$ and $a \in \mathbb{Z}^+$ with $a > 1$. Then*

$$(a^m + 1, a^n + 1) = a + 1.$$

Proof. Let

$$\begin{array}{rcll} n & = & mq_1 + r_1, & 0 < r_1 < m, \\ m & = & r_1 q_2 + r_2, & 0 < r_2 < r_1, \\ r_1 & = & r_2 q_3 + r_3, & 0 < r_3 < r_2, \\ & \vdots & & \\ r_k & = & r_{k+1} q_{k+1}, & r_{k+1} = 1. \end{array} \tag{1}$$

Using equation (1),

$$\begin{array}{ll} (a^m + 1, a^n + 1) & \\ = (-a^m - 1, -a^n - 1) & \\ = ((-a)^m - 1, (-a)^n - 1) & (\because m \text{ and } n \text{ are odd}) \\ = ((-a)^{r_1} - 1, (-a)^m - 1) & (\because \text{Remark } 1(b)) \\ \quad \vdots & \\ = ((-a)^{r_{k+1}} - 1, (-a)^{r_k} - 1), & (\because \text{Remark } 1(b)) \\ = ((-a) - 1, (-a)^{r_k} - 1), & (\because \text{Remark } 1(b)) \\ = (a + 1, (-a)^{r_k} - 1), & \end{array}$$

which divides $a + 1$. Note that $(a + 1) \mid (a^m + 1)$ and $(a + 1) \mid (a^n + 1)$ since m and n are odd. In other words,

$$(a + 1) \mid (a^m + 1, a^n + 1) \mid (a + 1) \quad \Rightarrow \quad (a^m + 1, a^n + 1) = a + 1$$

as we desired. □

Theorem 3. *Let $A \in \mathbb{Z}^+$ with $A > 1$ and let n and m be odd positive integers with $n > m \geq 1$. Then the prime factors of $A^m + 1$ and $A^n + 1$ coincide if and only if $A = 2$, $m = 1$, and $n = 3$.*

Proof. First of all, by Remark 1 (c),

$$\begin{aligned}\frac{A^n+1}{A+1} &= \frac{-A^n-1}{-A-1} \\ &= \frac{(-A)^n-1}{(-A)-1} \quad (\because n \text{ is odd}) \\ &= \left[\sum_{i=0}^{n-2}\binom{n}{i}(-A-1)^{n-i-1}\right]+n \\ &= \left[\sum_{i=0}^{n-2}\binom{n}{i}(-A-1)^{n-i-2}\right](-A-1)+n \end{aligned} \tag{2}$$

Moreover, note that

$$\frac{A^n+1}{A+1} = A^{n-1} - A^{n-2} + \cdots - A + 1. \tag{3}$$

It follows from Remark 1 (b), and equations (2) and (3) that

$$(A^{n-1} - A^{n-2} + \cdots - A + 1, A+1) = (n, A+1).$$

We first assume that $n = p$ is an odd prime number and $m = 1$. Then

$$\begin{aligned} & (A^{n-1} - A^{n-2} + \cdots - A + 1, A+1) \\ = & (A^{p-1} - A^{p-2} + \cdots - A + 1, A+1) \\ = & (p, A+1) \end{aligned} \tag{4}$$

is either 1 or p. If a prime number q divides $(A^{p-1} - A^{p-2} + \cdots - A + 1, A+1)$, then it divides $(p, A+1)$. In other words, $q \mid p$, that is, $q = p$. This means from equation (4) that $A^{p-1} - A^{p-2} + \cdots - A + 1$ and $A + 1$ have the same prime factors, and so $A^{p-1} - A^{p-2} + \cdots - A + 1 = p^\ell$ for some $\ell \in \mathbb{Z}^+ \cup \{0\}$.

Notice that

$$\begin{aligned} & A^{p-1} - A^{p-2} + \cdots - A + 1 \\ = & A^{p-2}(A-1) + A^{p-4}(A-1) + \cdots + A(A-1) + 1 \\ \geq & A^{p-2} + A^{p-4} + \cdots + A + 1 \quad (\because A > 1) \\ \geq & 2^{p-2} + 2^{p-4} + \cdots + 2 + 1 \\ \geq & \underbrace{2 + \cdots + 2}_{\frac{p-1}{2}\text{-times}} + 1 \\ = & p, \end{aligned} \tag{5}$$

and thus $\ell \geq 1$. Since $A^{p-1} - A^{p-2} + \cdots - A + 1$ and $A + 1$ have the same prime factors, $A + 1$ is also of the form p^α for some $\alpha \in \mathbb{Z}^+$, that is, $A = p^\alpha - 1$.

Now assume $p = 3$. Then

$$\begin{aligned} & A^{p-1} - A^{p-2} + \cdots - A + 1 \\ = & A^2 - A + 1 \\ = & 3^\beta \end{aligned}$$

for some $\beta \in \mathbb{Z}^+$. Since $A = 3^\alpha - 1$, we also have that

$$\begin{aligned} 3^\beta &= A^2 - A + 1 \\ &= (3^\alpha - 1)^2 - (3^\alpha - 1) + 1 \\ &= 3^{2\alpha} - 3^{\alpha+1} + 3 \\ &= 3(3^{2\alpha-1} - 3^\alpha + 1), \end{aligned}$$

which follows that $\alpha = \beta = 1$, and thus $A = 3 - 1 = 2$.

Suppose $p > 3$. If we consider equation (5) for this case, then we obtain

$$A^{p-1} - A^{p-2} + \cdots - A + 1 > p.$$

In other words,

$$A^{p-1} - A^{p-2} + \cdots - A + 1 = p^\ell$$

for some $\ell \in \mathbb{Z}^+$ with $\ell \geq 2$. Furthermore, notice that p^2 divides

$$\left[\sum_{i=0}^{p-2} \binom{p}{i} (-A-1)^{p-i-1}\right],$$

and so,

$$A^{p-1} - A^{p-2} + \cdots - A + 1 \equiv 0 \pmod{p^2}, \qquad \text{and}$$

$$\left[\sum_{i=0}^{p-2} \binom{p}{i} (-A-1)^{p-i-1}\right] \equiv 0 \pmod{p^2},$$

and hence

$$(A^{p-1} - A^{p-2} + \cdots - A + 1) - \left[\sum_{i=0}^{p-2} \binom{p}{i} (-A-1)^{p-i-1}\right] = p \equiv 0 \pmod{p^2},$$

which is a contradiction.

Now suppose that $m = 1$ and n is a composite number. Let p and q be two distinct prime factors of n. Note that p and q are odd primes since n is odd and

$$(A+1) \mid (A^p + 1) \mid (A^n + 1) \quad \text{and} \quad (A+1) \mid (A^q + 1) \mid (A^n + 1).$$

Since $A + 1$ and $A^n + 1$ have the same prime factors, so do those of $A^p + 1$ and $A^q + 1$. By the same idea as the above case $n = p$ is a prime number, $p = q = 3$ and $A = 2$. Hence $n = 3^\gamma$ for some $\gamma \in \mathbb{Z}^+$ and $A^n + 1$ is of the form 3^δ for some $\delta \in \mathbb{Z}^+$, and thus we have

$$A^n + 1 = 2^n + 1 = 2^{3^\gamma} + 1 = 3^\delta \quad \Leftrightarrow \quad 3^\delta - 2^{3^\gamma} = 1.$$

Since $\gamma \geq 1$, by Remark 1 (d), we have only integer solution $\delta = 2$ and $\gamma = 1$. Hence $n = 3^\gamma = 3$, which is a contradiction since n is a composite number.

Now assume $n > m > 1$ and let $g = (m, n)$. Then $m = Mg$ and $n = Ng$ for some odd positive integers M and N, and $(N, M) = 1$. Let $B = A^g$.

Then, by Lemma 2

$$(B^M + 1, B^N + 1) = B + 1.$$

Moreover, since $B^M + 1$ and $B^N + 1$ have the same prime factors and $(B^M + 1, B^N + 1) = B + 1$, the prime factors of $B + 1$ and $B^M + 1$ coincide. By what we proved earlier, this implies $B = 2$ and $M = 3$. Furthermore, since the prime factors of $B + 1$ and $B^N + 1$ coincide, we also have that $N = 3$, which is a contradiction since $(M, N) = 3 \neq 1$.

Conversely, if $A = 2$, $m = 1$, and $n = 3$, then $A + 1$ and $A^n + 1$ have the same prime factors, as we wished. □

Corollary 4. *Let m and n be odd positive integers and $A \in \mathbb{Z}^+$ with $A > 1$ and $n > m \geq 1$. Then the prime factors of $A^m + 1$ are a subset of those of $A^n + 1$ if and only if $A = 2$, either $m = 1$ or $m = 3$, and n is any odd positive integer n.*

Proof. Let $(m, n) = g$. Then there exist odd positive integers M and N such that $m = Mg$ and $n = Ng$. Note that $(M, N) = 1$. Let $B = A^g$. Then, by Lemma 2

$$(B^M + 1, B^N + 1) = B + 1.$$

Hence the set of the prime factors of $B^M + 1$ is a subset of that of $B^N + 1$ if and only if the prime factors of $B + 1$ and $B^M + 1$ coincide. Thus by Theorem 3 $B = 2$ and either $M = 1$ or $M = 3$. Note that $g = 1$ since $A = B = 2$, i.e., either $m = 1$ or $m = 3$. Hence $A^m + 1 = 3$ or 3^2. Moreover, since $A^n + 1$ is a multiple of $A + 1 = 3$, the set of the prime factors of $A^n + 1$ always contains 3 for any odd positive integer n with $n > 3$.

Conversely, if $A = 2$, and either $m = 1$ or 3, then the set of prime factors of $A^m + 1$ is a subset $\{3\}$ of those of $A^n + 1$ for any odd positive integer n, as we wished. □

References

1. J. Brillhert, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., *Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 12$ up to High Powers*, Contemp. Math., no. **22**, American Mathematical Society, Providence, (1988).
2. G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers.* 4th Ed. Oxford:Clarendon Press, (1960).
3. T. Ishikawa, N. Ishida, and Y. Yukimoto, *On Prime Factors of $A^n - 1$*, American Mathematical Monthly, **111**(3):243–245, (2004).
4. K.H. Rosen, *Elementary Number Theory and Its Application.* 5th Ed. Addison and Wesley, (2005).

Yong Su Shin received his MS and Ph.D at Seoul National University. On 1997, he became an assistant Professor at Sungshin Women's University, where he is a Professor. His research interest is the Hilbert functions of sets of finite points in $\mathbb{P}^n$, Gorenstein and Level algebras, and number theory.

Department of Mathematics, Sungshin Women's University, Seoul, Korea, 136-742
`email: ysshin@sungshin.ac.kr`