On LTE Sequence

Masum Billal
University Of Dhaka
Department of Computer Science and Engineering
Dhaka
Bangladesh
billalmasum93@gmail.com

September 11, 2015

Abstract

In this paper,we have characterized sequences which maintain the same property described in *Lifting the Exponent Lemma*. *Lifting the Exponent Lemma* is a very powerful tool in olympiad number theory and recently it has become very popular. We generalize it to all sequences that maintain a property like it i.e. if $p^\alpha||a_k$ and $p^\beta||n$, then $p^{\alpha+\beta}||a_{nk}$.

Keywords: LTE, Divisibility Sequence
MSC 2010 **Classification:** $11A25, 11A39$ and $11B83$.

---

1 Introduction

We will use just (a) for a sequence $(a_i)_{i\geq 1}$ throughout the whole article. In such a sequence, there may be some positive integers $x_1, x_2, ..., x_m$ associated which will not change. For example, (a) associated with two positive integers x, y with $a_i = x^i - y^i$ gives us the usual LTE.

Definition 1. $\nu_p(a) = \alpha$ is the largest positive integer α so that $p^\alpha | a$ but $p^{\alpha+1} \nmid a$. We say that p^α mostly divides a, sometimes it's denoted alternatively by $p^\alpha || a$.

Theorem 1.1 (Lifting The Exponent Lemma)**.** *If x and y are co-prime integers so that an odd prime p divides $x - y$, then*

$$\nu_p(x^n - y^n) = \nu_p(x - y) + \nu_p(n)$$

Alternatively, if $p^\alpha || x - y$ and $p^\beta || n$, then $p^{\alpha+\beta} || x^n - y^n$.

Definition 2 (Property $\mathcal{L}$ and $\mathcal{L}$ Sequence)**.** A sequence $(a_i)_{i\geq 1}$ has *property* $\mathcal{L}$ if for any odd prime p which divides a_k,

$$\nu_p(a_{kn}) = \nu_p(a_k) + \nu_p(n)$$

Alternatively, if $p^\alpha || a_k$ so that $\alpha \geq 1$ and $p^\beta || n$, then $p^{\alpha+\beta} || a_{kn}$. Call such a sequence an $\mathcal{L}$ *sequence.*

Note 1. $\mathcal{L}$ property is a much more generalization of Lifting the Exponent Lemma. In LTE, we only consider $k = 1$ for $x^n - y^n$.

Definition 3 (Divisible Sequence)**.** If (a) is a sequence so that a_k divides a_{nk} for all positive integers k, n, then (a) is a *divisible sequence.*

Definition 4 (Rank of a prime)**.** For a prime p and a sequence of positive integers $(a_i)_{i\geq 1}$, the smallest index k for which p divides a_k is the rank for prime p in (a). Let's denote it by $\rho(p)$. That is, $p | a_{\rho(p)}$ and $p \nmid a_k$ for $k < \rho(p)$.

Definition 5 (Primitive Divisor)**.** If a prime p divides a_n but p doesn't divide a_i for $i < n$, then p is a primitive divisor of a_n.

2 Characterizing $\mathcal{L}$ Sequence

Theorem 2.1. *If (a) is an $\mathcal{L}$ sequence, it is also a divisibility sequence.*

Proof. If $p^\alpha || a_k$ and $p^\beta || n$, then we have $p^{\alpha+\beta} || a_{kn}$ or $p^\alpha | a_{kn}$. Let $a_k = \prod_{i=1}^{r} p_i^{e_i}$, then $p_i^{e_i} | a_{kn}$ and so $\prod_{i=1}^{r} p_i^{e_i} | a_{nk}$ or $a_k | a_{nk}$.

□

Theorem 2.2. *There is a sequence* (b) *so that*

$$a_n = \prod_{d|n} b_d$$

and $(b_m, b_n) = 1$ *whenever* $m \not| n$ *or* $n \not| m$*. Moreover, we can recursively define* (b) *as* $b_1 = a_1$ *and*

$$b_n = \frac{[a_1, a_2, ..., a_n]}{[a_1, ..., a_{n-1}]}$$

where $[a, b]$ *is the least common multiple of* a *and* b*. In particular,* $b_n | a_n$*.*

Proof. We can prove it by induction. Base case $n = 1$ is easy since $b_1 = a_1$. For $n > 1$, Note that, we are done if we can prove that for a prime p, b_{p^i} and b_{pq} exists for $q \neq p$, a prime and $i \in \mathbb{N}$. First we prove that b_p exists for a prime p.

$$b_p = \frac{a_p}{a_1}$$

which obviously exists.

Now, for b_{p^i} we apply induction. Note that,

$$\begin{aligned} a_{p^{k+1}} &= \prod_{d|p^{k+1}} b_d \\ &= \prod_{i=0}^{k+1} b_{p^i} \\ &= b_{p^{k+1}} \cdot \prod_{i=0}^{k} b_{p^i} \\ &= a_{p^k} b_{p^{k+1}} \\ b_{p^{k+1}} &= \frac{a_{p^{k+1}}}{a_{p^k}} \end{aligned}$$

For b_{pq}, note that, $(a_p, a_q) = (a_p, a_q) = a_1$ and since $a_p = b_1 b_p, a_q = b_1 b_q$, we have $[a_p, a_q] = a_1 b_p b_q = b_1 b_p b_q$.

$$\begin{aligned} a_{pq} &= b_1 b_p b_q b_{pq} \\ b_{pq} &= \frac{a_{pq}}{b_1 b_p b_q} \\ &= \frac{a_{pq}}{[a_p, a_q]} \end{aligned}$$

Since $a_p|a_{pq}$ and $a_q|a_{pq}$, we have $[a_p, a_q]|a_{pq}$. Hence, b_{pq} exists as well.

∎

Theorem 2.3. $(a_m, a_n) = a_{(m,n)}$.

Proof. From the definition of (b),

$$\begin{aligned}(a_m, a_n) &= \left(\prod_{d|m} b_d, \prod_{d|n} b_d\right) \\ &= \left(\prod_{d|(m,n)} b_d\right) \\ &= a_{(m,n)}\end{aligned}$$

∎

Definition 6. Let's call the sequence (b) defined above in theorem (2.2) *b-sequence* of (a). So, in order to characterize $\mathcal{L}$ sequences, we need to actually analyze properties of (b) under $\mathcal{L}$ property.

From now on, let's assume (a) is an $\mathcal{L}$ sequence and (b) is its b-sequence. Also, we fix an odd prime p. For brevity, ρ will denote $\rho(p)$, the rank of p in (a). The theorems that follow can characterize an $\mathcal{L}$ sequence quite well.

Theorem 2.4. *(a) and (b) consists of the same set of prime factors and for a prime p, the rank in (a) is the same as the rank in (b).*

Theorem 2.5. *(a) is a divisible sequence if and only if for any positive integer s,*

$$\nu_p(a_{\rho s}) = \nu_p(a_\rho) + \nu_p(s)$$

The two theorems above are quite straight forward.

Theorem 2.6. *$p|a_k$ if and only if $\rho|k$.*

Proof. Since $p|a_\rho$ and $p|a_k$, according to theorem (2.3), we have $p|(a_\rho, a_k) = a_{(\rho,k)}$. If $g = (\rho, k)$ then $g \leq \rho$. Therefore if $g \neq \rho$ then $p|a_g$ implies g is smaller than ρ and $p|a_g$, contradicting the minimality of ρ. So, $g = \rho$ and hence, $\rho|k$. The only if part is straight forward.

∎

Theorem 2.7. *If $p^r || a_\rho$ and $p^s || a_k$, then $k = p^{s-r}\rho l$ for some integer l not divisible by p.*

Proof. Firstly $s \geq r$ because if $s < r$ that would mean $p | a_k$ with $k < \rho$, so $p^r | a_k$ too. From theorem (2.6), $\rho | k$. Assume that $k = \rho t$. Using the definition,

$$
\begin{aligned}
\nu_p(a_{\rho t}) &= \nu_p(a_\rho) + \nu_p(t) \\
s &= r + \nu_p(t) \\
\nu_p(t) &= s - r \\
t &= p^{s-r} l \text{ with } p \not| l
\end{aligned}
$$

Thus, $k = \rho p^{s-r} l$.

□

Theorem 2.8. *If $p \not| \rho$, then there exists a unique $d | \rho$ such that $p | b_{pd}$. Let's denote such d by δ. Moreover, $p \not| b_{pd}$ for $d \neq \delta$ and $p || b_{p\delta}$.*

Proof. $\nu_p(a_{\rho p}) = \nu_p(a_\rho) + 1$. We get,

$$
\begin{aligned}
p \quad || \quad & \frac{a_{\rho p}}{a_\rho} \\
= \quad & \frac{\prod_{d|\rho p} b_d}{\prod_{d|\rho} b_d} \\
= \quad & \prod_{\substack{d \not| \rho \\ d | \rho p}} b_d \\
= \quad & \prod_{d|\rho} b_{pd}
\end{aligned}
$$

This implies that only one δ among all divisors of ρ has the property that $p || b_{p\delta}$ and $p \not| b_{pd}$ for $d \neq \delta$.

□

Theorem 2.9. *If $(p\rho, k) = 1$, then for any divisor d of ρ and e a divisor of k, $p \not| b_{de}$.*

Proof. If $p \not| k$, then

$$\nu_p(a_{k\rho}) = \nu_p(a_\rho)$$

But $a_\rho | a_{\rho k}$. Therefore, $p \nmid \frac{a_{\rho k}}{a_\rho}$.

$$\begin{aligned}
\frac{a_{k\rho}}{a_\rho} &= \frac{\prod_{d|\rho k} b_d}{\prod_{d|\rho} b_d} \\
&= \prod_{\substack{d \nmid \rho \\ d|\rho k}} b_d \\
&= \prod_{e|k} \prod_{\substack{d \nmid \rho \\ d|\rho e}} b_d \\
&= \prod_{e|k} \prod_{d|\rho} b_{de}
\end{aligned}$$

Since p is a prime, p can't divide any of those b_{de}.

□

3 Conjectures

Conjecture 1. *If $(p, \rho(p)) \neq 1$, then $p = \rho(p)$. Otherwise, $(p, \rho(p)) = 1$.*

Conjecture 2. *If $(b_m, b_n) > 1$, then $\frac{m}{n} = p^\alpha$ for some α.*

We all know about the open problem: Decide if F_p if square-free. Here is a stronger version of that. It is because, F_n is a divisibility sequence and $\mathcal{L}$ sequence.

Conjecture 3. *b_n is square-free if n is square-free.*

The following conjecture(if true) is a much more generalization of *Zsigmondy's theorem*, see (2).

Conjecture 4. *a_n has a primitive prime divisor except for some finite n. Moreover, there is a positive integer M so that, whenever a_n doesn't have a primitive divisor, $n|M$.*

References

[1] Amir Hossein Parvardi, *Lifting The Exponent Lemma(LTE)*, www.taharut.org/imo/LTE.pdf

[2] Bart Michels, *Zsigmondys Theorem*, users.ugent.be/~bmichels/files/zsigmondy_en.pdf