

A criterion to estimate the least common multiple of sequences
and asymptotic formulas for $\zeta(3)$ arising from recurrence relation
of an elliptic function *

Shigeki Akiyama

§0. Introduction

In [2], the author studied the asymptotic behavior of the least common multiple of a sequences $\{a_n\}_{n=1}^{\infty}$ provided that it satisfies certain axioms (A1) and (A2) (see page 4). Sequences defined by binary linear recurrence, for example, were handled there. A typical result was

$$\frac{\log |a_1 a_2 \cdots a_n|}{\log [a_1, a_2, \dots, a_n]} = \zeta(2) + O\left(\frac{\log n}{n}\right), \quad (1)$$

where $[a_1, a_2, \dots, a_n]$ is the least common multiple of the terms a_1, a_2, \dots, a_n and $\zeta(\cdot)$ is the Riemann zeta function. On the origin of these problems and related works, see [7] [5] [1] [2] [10]. To prove (1) in [2], the fundamental tool employed was to rewrite the least common multiple by "an inclusion exclusion principle". This was done in [2] with the essential use of the axioms (A1) and (A2). In this article, we employ a more sophisticated axiom

$$(S) \quad (a_n, a_m) = |a_{(n,m)}|.$$

We say that the non zero sequence $\{a_n\}_{n=1}^{\infty}$ satisfying (S) to be a strongly divisible sequence. This "strong divisibility" was studied by several authors in [4] [3] [9]. And we prove that the assertion of [2] still holds (See Theorem 1). It is easily seen that (S) is weaker than (A1) and (A2). Furthermore, it is shown in Theorem 1 that the relation (2), which is the "inclusion exclusion principle of the least common multiple", is *equivalent* to the axiom (S).

Our next problem is to find the good example of a strongly divisible sequence which has appropriate asymptotic behavior. Let $\sigma(u)$ be the Weierstrass sigma function associated with some lattice. Put $\psi_n(u) = \sigma(nu)/(\sigma(u)^{n^2})$. Then $\psi_n(u)$ is an elliptic function with respect to u and satisfies the recurrence relation:

*Only for the private copy. See Japanese Journal of Math., Vol.22, no.1 (1996), 129 – 146, for the exact published version.

$$\psi_{m+n}(u)\psi_{m-n}(u) = \psi_{m+1}(u)\psi_{m-1}(u)\psi_n(u)^2 - \psi_{n+1}(u)\psi_{n-1}(u)\psi_m(u)^2,$$

and $\psi_0(u) = 0$, $\psi_1(u) = 1$. This relation was classically known and used to calculate the algebraic relation between $p(nu)$ and $p(u)$, where $p(u)$ is the Weierstrass p -function. The sequence $\{\psi_n(u)\}_{n=1}^{\infty}$ is determined completely by the initial values $\psi_2(u)$, $\psi_3(u)$ and $\psi_4(u)$ when $\psi_2(u)\psi_3(u) \neq 0$. Now let $\psi_i(u)$ ($i = 2, 3, 4$) be integers. The sequences of this type are systematically studied by Ward. He showed in [12] and [13] that, when

$$\psi_2(u)|\psi_4(u) \quad \text{and} \quad (\psi_3(u), \psi_4(u)) = 1,$$

each $\psi_n(u)$ is an integer and the sequence $\{\psi_n(u)\}$ satisfies (S). In section 3, we prove the average asymptotic formula for $\log |\psi_n(u)|$. So, under certain conditions, we can derive the asymptotic formula:

$$\frac{\log |\psi_1(u)\psi_2(u)\cdots\psi_n(u)|}{\log[\psi_1(u), \psi_2(u), \dots, \psi_n(u)]} = \zeta(3) + O\left(\frac{1}{n}\right),$$

(Theorem 4), by using the method developed in [2]. As a by-product, in some special cases, we can calculate $\log |\sigma(u)|$, where u is a division point of some period of the elliptic function (see section 4).

§1. The Fundamental Theorem.

Let $\{a_n\}_{n=1}^{\infty}$ be a non zero integer sequence. We say that $\{a_n\}$ is divisible when it has the property:

$$(D) \quad n|m \quad \text{implies} \quad a_n|a_m.$$

It is easily seen that the axiom (S) implies (D).

Theorem 1. Let $\{a_n\}_{n=1}^{\infty}$ be a strongly divisible sequence. Then we have

$$[a_1, a_2, \dots, a_n] = \prod_{i=1}^n |M(i)| \tag{2}$$

where $M(i) = \prod_{d|i} (a_{i/d})^{\mu(d)}$ and $\mu(\cdot)$ is the Möbius function. Conversely, if a sequence of non zero integers $\{a_n\}_{n=1}^{\infty}$ satisfies (2) then $\{a_n\}_{n=1}^{\infty}$ is strongly divisible.

Proof. We first prove the sufficiency. The case $n = 1$ is obvious. Assume the equality (2) for $n - 1$. First we see that

$$\begin{aligned}
[a_1, a_2, \dots, a_n]/[a_1, a_2, \dots, a_{n-1}] &= \text{G.C.D.}_{i=1,2,\dots,n-1} \left(\frac{a_n}{(a_n, a_i)} \right) \\
&= |a_n| / \left(\text{L.C.M.}_{i=1,2,\dots,n-1} a_{(n,i)} \right) = |a_n| / \left(\text{L.C.M.}_{d|n} a_{n/d} \right).
\end{aligned}$$

Since $\{a_n\}$ is divisible, we may restrict to the prime divisor p of n :

$$[a_1, a_2, \dots, a_n]/[a_1, a_2, \dots, a_{n-1}] = |a_n| / \left(\text{L.C.M.}_{p|n} a_{n/p} \right).$$

Using the inclusion exclusion principle, we have

$$\begin{aligned}
&= |a_n| \frac{\prod_{p_1, p_2} (a_{n/p_1}, a_{n/p_2}) \prod_{p_1, p_2, p_3, p_4} (a_{n/p_1}, a_{n/p_2}, a_{n/p_3}, a_{n/p_4}) \cdots}{\prod_{p_1} |a_{n/p_1}| \prod_{p_1, p_2, p_3} (a_{n/p_1}, a_{n/p_2}, a_{n/p_3}) \cdots} \quad (3) \\
&= |a_n| \frac{\prod_{p_1, p_2} |a_{n/p_1 p_2}| \prod_{p_1, p_2, p_3, p_4} |a_{n/p_1 p_2 p_3 p_4}| \cdots}{\prod_{p_1} |a_{n/p_1}| \prod_{p_1, p_2, p_3} |a_{n/p_1 p_2 p_3}| \cdots} \\
&= |M(n)|.
\end{aligned}$$

Thus the relation (2) is proved by induction.

Now we prove the necessity. So we assume the relation (2). Then every $M(n)$ is an integer because

$$|M(n)| = [a_1, a_2, \dots, a_n]/[a_1, a_2, \dots, a_{n-1}]. \quad (4)$$

The axiom (S) is equivalent to the following statement:

$$\text{if } d_1 \not\mid d_2 \text{ and } d_2 \not\mid d_1 \text{ then } (M(d_1), M(d_2)) = 1.$$

This can easily be shown by the inverse relation $a(n) = \prod_{d|n} M(d)$. In fact, let us assume that there exists a pair d_1 and d_2 which satisfies

$$d_1 < d_2, d_1 \not\mid d_2, d_2 \not\mid d_1, p \mid M(d_1) \text{ and } p \mid M(d_2),$$

where p is a prime. We also assume that d_1 is chosen to be minimum under these conditions. Denote by $\text{ord}_p(x)$ the multiplicities of p in the prime factorization of an integer x . Then if $d \mid d_1$, we have $d \mid d_2$ or $p \nmid M(d)$ by the minimality of d_1 . Thus

$$\text{ord}_p a_{d_1} = \sum_{d \mid d_1} \text{ord}_p M(d) = \sum_{d \mid (d_1, d_2)} \text{ord}_p M(d) = \text{ord}_p a_{(d_1, d_2)}.$$

But from (4), this means $\text{ord}_p M(d_1) = 0$. This is a contradiction. \square

The equality (3) can be found in Ward [14] Lemma 9.1. He also noticed in the same paper that the axiom (S) is equivalent to:

(R) There exists a function f from \mathbf{N} to \mathbf{N} such that

$$M|a_n \text{ is equivalent to } f(M)|n.$$

We can easily show this equivalence itself. It seems that the main interest of Ward [14] is to characterize this axiom (R) by using $M(n)$. Now let us recall the axioms (A1) and (A2) in [2]:

(A1) For each prime p , we denote by S_p the set of positive integer n 's so that a_n is divisible by p . If $S_p \neq \emptyset$, there exists an integer $r(p)$ such that S_p coincides with the set of all positive $r(p)$ multiples,

(A2) For each prime p , there exists a weakly increasing function f_p from $\mathbf{N} \cup \{0\}$ to itself satisfying the property $\text{ord}_p(a_n) = f_p(\text{ord}_p(n))$, for $n \in S_p$.

We see that the axioms (A1) + (A2) are stronger than (R). So Theorem 1 of [2] is a consequence of the above Theorem 1. But the author does not have a good, not too artificial, example of strongly divisible sequence which does not satisfy both (A1) and (A2).

Proposition 1. Let $\{a_n\}$ and $\{b_n\}$ be strongly divisible sequences. Then the greatest common divisor sequence $\{(a_n, b_n)\}_{n=1}^{\infty}$ is strongly divisible. Moreover, if we assume that each b_n is positive, then the composition sequence $\{a_{b_n}\}_{n=1}^{\infty}$ is also strongly divisible.

Proof. These are easily verified by the relations,

$$((a_n, b_n), (a_m, b_m)) = ((a_n, a_m), (b_n, b_m)) = (a_{(n,m)}, b_{(n,m)})$$

and

$$(a_{b_n}, a_{b_m}) = |a_{(b_n, b_m)}| = |a_{b_{(n,m)}}|. \quad \square$$

The similar assertion holds for the axioms (A1) and (A2) (see Proposition 1 and 2 in [2]). Once we establish Theorem 1, the next two theorems follow immediately by the same proof as for Proposition 3 of [2].

Theorem 2. Let $\{a_n\}$ be a strongly divisible sequence which has the following asymptotic behavior:

$$\log |a_n| = An^l + O(n^{l-1}\omega(n)),$$

with positive constant A and

$$\omega(n) = \begin{cases} 1 & \text{if } l > 1 \\ \log n & \text{if } l = 1. \end{cases}$$

Then we have

$$\log[a_1, a_2, \dots, a_n] = \frac{n^{l+1}}{(l+1)\zeta(l+1)} + O(n^l \omega(n)) \quad (5)$$

and

$$\frac{\log |a_1 a_2 \cdots a_n|}{\log[a_1, a_2, \dots, a_n]} = \zeta(l+1) + O\left(\frac{\omega(n)}{n}\right). \quad (6)$$

Theorem 3. Let $\{a_n\}$ be a strongly divisible sequence. If we have

$$\log |a_1 a_2 \cdots a_n| = An^{l+1} + O(n^l),$$

with $l \geq 1$. Then we have (5) and (6).

In the case $l > 1$, the assumption of Theorem 3 is weaker than that of Theorem 2. Consider the case $l = 1$. If we know more precise average asymptotic behavior, we can proceed further. Assume that there exist constants ε, A and B such that

$$\frac{1}{n} \log |a_1 a_2 \cdots a_n| = An + B + O(n^{-\varepsilon}), \quad (7)$$

where A and ε are positive. Then we easily see, for the strongly divisible sequence $\{a_n\}$ it holds that

$$\frac{\log |a_1 a_2 \cdots a_n|}{\log[a_1, a_2, \dots, a_n]} = \zeta(2) + O\left(\frac{E(n)}{n^2}\right), \quad (8)$$

where

$$E(n) = \sum_{k=1}^n \varphi(k) - \frac{3}{\pi^2} n^2,$$

and $\varphi(\cdot)$ is Euler's totient function. The error term of (8) is better than those of Theorem 2 and 3 (see [11], [8]) and is best possible. The estimate of type (7) is established in the case of Lucas sequence in [6] by using the estimation of discrepancy of a sequence $\{n\theta\}_{n=1}^{\infty}$ where θ is a certain irrational number. See also [10].

§2. Sequences arising from an Elliptic Function.

In this section, we treat an example of strongly divisible sequences. Let $\mathcal{L} = 2\omega_1\mathbf{Z} + 2\omega_3\mathbf{Z}$ be a lattice in \mathbf{C} . We choose $\omega_i (i = 1, 3)$ so that $\tau = \omega_3/\omega_1$ is in the upper half plane

$\mathbf{H} = \{z \in \mathbf{C} \mid \text{Im}(z) > 0\}$. Denote by $\sigma_i(u) = \sigma_i(u, \mathcal{L})$ the Weierstrass sigma function:

$$\sigma_i(u, \mathcal{L}) = u \prod_{w \in \mathcal{L}'} (1 - u/w) \exp(u/w + (1/2)(u/w)^2),$$

where $\mathcal{L}' = \mathcal{L} - \{0\}$. Put $\psi_n(u) = \sigma(nu)/(\sigma(u)^{n^2})$. Then $\psi_n(u)$ is an elliptic function and satisfies the following recurrence relation for $m \geq n \geq 1$:

$$\psi_{m+n}(u)\psi_{m-n}(u) = \psi_{m+1}(u)\psi_{m-1}(u)\psi_n(u)^2 - \psi_{n+1}(u)\psi_{n-1}(u)\psi_m(u)^2.$$

This relation is crucial in calculating the n -th multiple value of Weierstrass p -function in the classical elliptic function theory. Note that when $u \notin \mathcal{L}$ then $\psi_0(u) = 0$ and $\psi_1(u) = 1$. Let $\{h_n\}$ be the sequence defined by the recurrence

$$h_{m+n}h_{m-n} = h_{m-1}h_{m+1}h_n^2 - h_{n+1}h_{n-1}h_m^2 \quad (9)$$

and $h_0 = 0, h_1 = 1$. The systematical study of this sequence in the rational number field was done by Ward in [12] and [13]. We quote some of his results in this section.

- Let $h_i (i = 2, 3, 4)$ be integers, $h_2h_3 \neq 0$ and $h_2|h_4$. Then $\{h_n\}$ is well defined and every h_n is an integer.

Hereafter, we assume $h_i (i = 2, 3, 4)$ to be integers. We call this type of sequence $\{h_n\}$ as an elliptic sequence.

- If $h_2h_3h_4h_5 \neq 0$ then every $h_n \neq 0$ for $n \geq 1$.
- The sequence $\{h_n\}$ is divisible. Moreover if $(h_3, h_4) = 1$, then $\{h_n\}$ is strongly divisible.

Now let Δ be the discriminant of the elliptic curve corresponding to the lattice \mathcal{L} . Under the assumption $h_2h_3 \neq 0$, we can determine the values $g_2(u, \mathcal{L}), g_3(u, \mathcal{L})$ and $p(u, \mathcal{L})$ formally in terms of h_2, h_3 and h_4 by solving simultaneous equations:

$$\psi_i(u) = \psi_i(u, \mathcal{L}) = h_i,$$

for $i = 2, 3$ and 4 . In fact, $g_2(\mathcal{L}), g_3(\mathcal{L})$ and $p(u, \mathcal{L})$ are written in a form of rather complicated rational function of h_2, h_3 and h_4 in page 50 of [12]. Thus Δ is given by

$$\begin{aligned} \Delta &= g_2(\mathcal{L})^3 - 27g_3(\mathcal{L})^2 \\ &= (-h_2^{15}h_4 + h_2^{12}h_3^3 - 3h_2^{10}h_4^2 + 20h_2^7h_3^3h_4 - 3h_2^5h_4^3 - 16h_2^4h_3^6 - 8h_2^2h_3^3h_4^2 - h_4^4)/(h_2^8h_3^3). \end{aligned}$$

Note that the corresponding formula (19.3) of [12] is not valid. When $\Delta \neq 0$, then the sequence $\{h_n\}$ does correspond to some elliptic curve. In other words, there exist a lattice \mathcal{L} with j -invariant $g_2(\mathcal{L})^3/\Delta$ and the value $g_2(\mathcal{L})$ and $g_3(\mathcal{L})$ fit together with the above calculated ones. Thus, when $h_2h_3 \neq 0$ and $\Delta \neq 0$, we can express $h_n = \psi_n(u)$ for every n .

Let $\{a_n\}, \{b_n\}$ be any complex valued sequences. We say that $\{a_n\}$ is equivalent to $\{b_n\}$ when there exists a non-zero constant C such that

$$a_n = C^{n^2-1}b_n.$$

We have

- Let $\{h_n\}$ be an elliptic sequence, $h_2h_3 \neq 0$ and $\Delta = 0$. Then $\{h_n\}$ is equivalent either to the sequence $0, 1, 2, \dots, n, \dots$ of non negative integers or to a sequence $\{U_n\}$ where $U_n = (\alpha^n - \beta^n)/(\alpha - \beta)$, $\alpha\beta = 1$ and $\alpha + \beta$ is contained in a quadratic extension of \mathbf{Q} .

Notice that $\log[1, 2, \dots, n]$ is the Chebyshev's psi function which is widely studied, and the least common multiple of Lucas type sequence was treated in [2]. As we are interested in the estimation of the least common multiple of a sequence, there will be no problem in the case $\Delta = 0$. Taking into account of Theorem 2, we can state our problem as follows:

Problem. Let $\{h_n\}$ be an elliptic sequence with $h_2h_3 \neq 0$ and $\Delta \neq 0$. Study the asymptotic behavior of $\log |h_n|$.

§3. Asymptotic Behavior of Elliptic Sequences.

Let $z = \exp(\pi\sqrt{-1}v)$, $v = u/(2w_1)$ and $\theta_1(v)$ be the elliptic theta function:

$$\theta_1(v) = \sqrt{-1} \sum_{n \in \mathbf{Z}} (-1)^n q^{(n-1/2)^2} z^{2n-1},$$

where $q = \exp(\pi\sqrt{-1}\tau)$. Denote by $\theta_1^{\prime 0}$ the value of $\theta_1'(v)$ at 0, that is,

$$\theta_1^{\prime 0} = 2\pi \sum_{n \geq 1} (-1)^{n-1} (2n-1) q^{(n-1/2)^2}.$$

Then we have

Lemma 1. The function $\mathcal{F}(v) = \pi(\text{Im}(v))^2/\text{Im}(\tau) - \log |\theta_1(v)|$ is invariant under parallel translations $v \rightarrow v + 1$ and $v \rightarrow v + \tau$. In other words, the value $\mathcal{F}(u/(2w_1))$ is determined by $u \bmod \mathcal{L}$.

Proof. This can be shown by the well known formulas:

$$\theta_1(v+1) = -\theta_1(v)$$

and

$$\theta_1(v+\tau) = -\exp(-\pi\sqrt{-1}(2v+\tau))\theta_1(v). \quad \square$$

Lemma 2. Let

$$A(u) = \mathcal{F}(v) + \log |\theta_1^{\prime 0}| - \log |2w_1|. \quad (10)$$

Then we have

$$\log |\psi_n(u)| = A(u)n^2 - A(nu)$$

Proof. The function $\sigma(u)$ is written in the form:

$$\sigma(u) = 2w_1 \exp(2\eta_1 w_1 v^2) \theta_1(v) / \theta_1^{\prime 0},$$

with a constant η_1 which satisfies

$$\sigma(u+2w_1) = -\sigma(u) \exp(2\eta_1(u+w_1)).$$

Then we have

$$A(u) = \operatorname{Re}(\eta_1 u^2 / (2w_1)) + \pi(\operatorname{Im}(v))^2 / \operatorname{Im}(\tau) - \log |\sigma(u)|. \quad (11)$$

This formula implies

$$n^2 (A(u) + \log |\sigma(u)|) = A(nu) + \log |\sigma(nu)|.$$

This proves the lemma. □

Lemma 3. Let $|z| > 1$ and $q^{2m} z^{2n} \neq 1$ for all $m \in \mathbf{Z}$. Denote by $[x]$ the maximal integer which does not exceed x . Then we have

$$\log \left| \prod_{m \geq 1} (1 - q^{2m} z^{2n}) \right| = \log |1 - q^{2m_0} z^{2n}| - (n \log |z|)^2 / \log |q| + O(n),$$

where $m_0 = [-n \log |z| / \log |q| + 1/2]$.

Proof. We can show that $|q^{2m} z^{2n}| < |q|$ for $m > m_0$ and $|q^{-2m} z^{-2n}| \leq |q|$ for $m < m_0$. Thus we have

$$\begin{aligned}
\log \left| \prod_{m \geq 1} (1 - q^{2m} z^{2n}) \right| &= \log |1 - q^{2m_0} z^{2n}| + \sum_{m < m_0} \log |q^{2m} z^{2n}| \\
&\quad + \sum_{m < m_0} \log |1 - q^{-2m} z^{-2n}| + \sum_{m > m_0} \log |1 - q^{2m} z^{2n}| \\
&= \log |1 - q^{2m_0} z^{2n}| + 2m_0 n \log |z| + m_0^2 \log |q| + O(n) \\
&= \log |1 - q^{2m_0} z^{2n}| - (n \log |z|)^2 / \log |q| + O(n).
\end{aligned}$$

Lemma 4. For all positive integer n , let $nu \notin \mathcal{L}$. Then $A(nu)$ is bounded from below as a function of n and we have

$$A(nu) = - \min_{m \in \mathbf{Z}} \log |1 - \mathbf{e}(m\tau + nv)| + O(n),$$

where $\mathbf{e}(z) = \exp(2\pi\sqrt{-1}z)$.

Proof. By (10) and Lemma 1, $A(u)$ is determined by $u \bmod \mathcal{L}$. Since $\theta_1(v)$ is entire, $\log |\theta_1(v)|$ is bounded from above in the fundamental paralleloptope $\{ v = \xi_1 + \xi_3\tau \in \mathbf{C} \mid \xi_1, \xi_3 \in [0,1] \}$. This shows that $A(nu)$ is bounded from below as a function of n . Changing the sign of v if necessary, we may assume that $|z| > 1$. Then by using Lemma 3 and the infinite product representation of $\theta_1(v)$:

$$\theta_1(v) = -\sqrt{-1}q^{1/4}z \prod_{m \geq 1} (1 - q^n)(1 - q^{2m}z^2)(1 - q^{2m-2}z^{-2}),$$

we have

$$\log |\theta_1(nv)| = \log |1 - q^{2m_0} z^{2n}| - (n \log |z|)^2 / \log |q| + \sum_{m \geq 1} \log |1 - q^{2m-2} z^{-2n}| + O(n).$$

Since $|z| > 1$, the third term of the right hand side is $O(1)$. Thus we have

$$\log |\theta_1(nv)| = \log |1 - q^{2m_0} z^{2n}| + \pi(\operatorname{Im}(nv))^2 / \operatorname{Im}(\tau) + O(n).$$

By (10), we proved the assertion. \square

Lemma 5. Let Θ be a positive number smaller than $1/2$ and z be a complex number with $|1 - z| < \Theta$. Then the inequality

$$k|1 - z|/2 < |1 - z^k| < 2k|1 - z|$$

holds for any positive integer $k \leq (2\Theta)^{-1}$.

Proof. We easily see that $|(1 - z^k)/(1 - z)| \leq k \max\{1, |z^{k-1}|\}$. Let $r = z - 1$ then

$$k \log |1 + r| \leq k \log(1 + |r|) \leq k|r| \leq 1/2.$$

So $|(1 + r)^{k-1}| \leq \sqrt{e} \cdot (1 + |r|)^{-1} \leq \sqrt{e} < 2$. This shows the right inequality. So we have

$$\begin{aligned} |(1 - z^k)/(1 - z) - k| &\leq \sum_{i=1}^{k-1} |z^i - 1| \leq 2|z - 1| \sum_{i=1}^{k-1} i \\ &= k(k-1)|z - 1| < (k-1)/2 < k/2 \end{aligned} \quad (12)$$

This implies that $|(1 - z^k)/(1 - z)| > k - k/2$, which is the left inequality. \square

We are now able to prove $A(nu) = O(n)$ for almost all n .

Lemma 6. Assume that there exists no integer n such that $nu \in \mathcal{L}$. Consider a set $C = \{n \in \mathbf{N} \mid A(nu) > Ln\}$ for sufficiently large fixed L . Assume that C contains infinitely many elements. We put $C = \{n_i\}_{i=1}^{\infty}$ with

$$n_1 < n_2 < n_3 < \cdots \cdots.$$

Then there exists a positive constant $T \geq 2$ and a sequence of positive integers $\{\nu_k\}_{k=1,2,\dots}$ which satisfies three conditions:

- (a) $\nu_{k+1} > \exp(T\nu_k)$,
- (b) if $\nu_k \leq n_i < \nu_{k+1}$, then n_i is a multiple of ν_k ,
- (c) Let $\xi(n_i) = -\min_{m \in \mathbf{Z}} \log |1 - \mathbf{e}(m\tau + n_iv)|$, then ξ is a decreasing function of $n_i \in C$ in each interval $[\nu_k, \nu_{k+1})$.

Proof. By Lemma 4, there exists L_0 such that

$$A(nu) + \min_{m \in \mathbf{Z}} \log |1 - \mathbf{e}(m\tau + nv)| \leq L_0 n$$

for any n . Take a positive constant L greater than L_0 . Then we have

$$\log |1 - \mathbf{e}(m_i\tau + n_iv)| < -(L - L_0)n_i,$$

for a certain integer m_i . This shows that

$$|1 - \mathbf{e}(m_i\tau + n_iv)| < \exp(-Ln_i).$$

for a positive constant $\mathbf{L}(= L - L_0)$. Define a new set

$$C' = \{n \in \mathbf{N} \mid \exists m \in \mathbf{Z}, |1 - \mathbf{e}(m\tau + nv)| < \exp(-\mathbf{L}n)\}.$$

Then the set C is a subset of C' . Thus our aim is to verify the above three conditions for the set C' for a sufficiently large \mathbf{L} . More precisely, we shall show that there exist two sequences of positive integers $\{\nu_k\}_{k=1}^{\infty}$ and $\{r_k\}_{k=1}^{\infty}$ so that C' is the set consisting of elements of the form

$$\nu_1 < 2\nu_1 < \cdots < r_1\nu_1 < \nu_2 < 2\nu_2 < \cdots < r_2\nu_2 < \nu_3 < \cdots.$$

We proceed by induction. Let $\nu_1 = n_1$, $\mu_1 = m_1$ and r_1 be the biggest integer so that

$$|1 - \mathbf{e}(k(\mu_1\tau + \nu_1v))| < \exp(-\mathbf{L}k\nu_1) \quad (13)$$

holds for any integer $k \leq r_1$. This inequality implies that

$$|1 - \mathbf{e}(\mu_1\tau + \nu_1v)| < \exp(-\mathbf{L}r_1\nu_1).$$

In fact, by using Lemma 5 and induction, we can show

$$|1 - \mathbf{e}(\mu_1\tau + \nu_1v)| < \exp(-\mathbf{L}k\nu_1).$$

for $1 \leq k \leq r_1$. The existence of r_1 easily follows from this. By (13), we see that $\nu_1, 2\nu_1, \dots, r_1\nu_1 \in C'$. It is shown that the minimum of $|1 - \mathbf{e}(m\tau + k\nu_1v)|$ is attained by $m = k\mu_1$, if we take sufficiently large \mathbf{L} . We can also show that $\xi(k\nu_1)$ is a decreasing function. To see this, we note that the inequality (12) implies that

$$\left| \frac{1 - \mathbf{e}(k(\mu_1\tau + \nu_1v))}{1 - \mathbf{e}(\mu_1\tau + \nu_1v)} - k \right| < \frac{k}{2}$$

and

$$\frac{1 - \mathbf{e}((k+1)(\mu_1\tau + \nu_1v))}{1 - \mathbf{e}(\mu_1\tau + \nu_1v)} - \frac{1 - \mathbf{e}(k(\mu_1\tau + \nu_1v))}{1 - \mathbf{e}(\mu_1\tau + \nu_1v)} = \mathbf{e}(k(\mu_1\tau + \nu_1v)).$$

The value $\mathbf{e}(k(\mu_1\tau + \nu_1v))$ is close enough to 1, which show that $\xi(k\nu_1) \geq \xi((k+1)\nu_1)$ for $k \leq r_1 - 1$.

Now we assume that

$$\nu_1 < 2\nu_1 < \cdots < r_1\nu_1 < \nu_2 < 2\nu_2 < \cdots < r_2\nu_2 \cdots < \nu_i < 2\nu_i < \cdots < r_i\nu_i$$

are the elements of C' satisfying the following:

(a') There exists a constant $T \geq 2$ such that $\nu_{j+1} > \exp(Tr_j\nu_j)$ for $j = 1, 2, \dots, i-1$,

- (b') $\xi(l\nu_j)$ is a decreasing function of l for $l = 1, 2, \dots, r_j$,
- (c') There exist no other elements of C' smaller than ν_i .
- (d') r_j is defined to be the biggest integer k so that $|1 - e(k(\mu_j\tau + \nu_jv))| < \exp(-\mathbf{L}k\nu_j)$ holds for $j = 1, 2, \dots, i$.

Take the smallest element ν_{i+1} of $C' - \{l\nu_j\}_{j,l}$ where $j = 1, 2, \dots, i$ and $l = 1, 2, \dots, r_j$. Let μ_{i+1} be the corresponding m . We see $\nu_{i+1} > \nu_i$ by (c'). At first, we shall show $\nu_{i+1} > r_i\nu_i$. If $\nu_{i+1} \leq r_i\nu_i$ then we have

$$\begin{aligned} & |1 - \mathbf{e}((\mu_{i+1} - \mu_i)\tau + (\nu_{i+1} - \nu_i)v)| \\ & \leq |1 - \mathbf{e}(\mu_{i+1}\tau + \nu_{i+1}v)| + |1 - \mathbf{e}(\mu_i\tau + \nu_i v)| \\ & \leq \exp(-\mathbf{L}\nu_{i+1}) + \exp(-\mathbf{L}r_i\nu_i) \leq \exp(-\mathbf{L}(\nu_{i+1} - \nu_i)), \end{aligned}$$

which contradicts the definition of ν_{i+1} . Let E and F be integers such that $\nu_{i+1} = Er_i\nu_i + F$ and $|F| \leq r_i\nu_i/2$. Let G be a certain positive integer which will be chosen suitably later. Then we have

$$r_i\nu_i - G \cdot F = (G \cdot E + 1)r_i\nu_i - G \cdot \nu_{i+1}.$$

Thus we have

$$\begin{aligned} & |1 - \mathbf{e}(((G \cdot E + 1)r_i\mu_i - G \cdot \mu_{i+1})\tau + (r_i\nu_i - G \cdot F)v)| \\ & \leq |1 - \mathbf{e}(G \cdot (\mu_{i+1}\tau + \nu_{i+1}v))| + |1 - \mathbf{e}((G \cdot E + 1)r_i(\mu_i\tau + \nu_i v))| \\ & \leq 2G \cdot \exp(-\mathbf{L}\nu_{i+1}) + 2(G \cdot E + 1)r_i \exp(-\mathbf{L}r_i\nu_i). \end{aligned}$$

Here we used Lemma 5. (The conditions of G in Lemma 5 cause no problem in showing the assertion.) Hence if we have the inequality

$$2G \cdot \exp(-\mathbf{L}\nu_{i+1}) + 2(G \cdot E + 1)r_i \exp(-\mathbf{L}r_i\nu_i) < \exp(-\mathbf{L}(\nu_i r_i - G \cdot F))$$

then $\nu_i r_i - G \cdot F \in C'$. Firstly, we consider the case $F > 0$. Then we have

$$2G \cdot \exp(-\mathbf{L}\nu_{i+1}) + 2(G \cdot E + 1)r_i \exp(-\mathbf{L}r_i\nu_i) < 2r_i G \cdot (E + 2) \exp(-\mathbf{L}r_i\nu_i).$$

Thus if $2r_i G \cdot (E + 2) < \exp(\mathbf{L}G \cdot F)$ then $\nu_i r_i - G \cdot F \in C'$. Put $G = 1$ when $r_i\nu_i/4 \leq |F|$. If $r_i\nu_i/4 > |F|$ then take G such that $r_i\nu_i/4 \leq |G \cdot F| \leq 3r_i\nu_i/4$. In this case, we remark that there are at least two ways to choose G . If $E \leq \exp(\mathbf{L}r_i\nu_i/5)$ then we have

$$2r_i G \cdot (E + 2) \leq 3/2 \cdot r_i^2 \nu_i \cdot (E + 2) \leq \exp(\mathbf{L} \cdot r_i \nu_i / 4) \leq \exp(\mathbf{L} G \cdot F)$$

for $\mathbf{L} \geq 60$. This shows $\nu_i | (F \cdot G)$. Moreover, we see $\nu_i | F$. In fact, when $G \neq 1$, we can choose G with $\nu_i | F$ among the several possible candidates. Secondly, consider the case $F < 0$. Note that $|1 - \exp(z)| = |1 - \exp(-z)|$. So, in the same way, we can prove $\nu_i | F$, substituting $\nu_i r_i - G \cdot F$ with $G \cdot F - \nu_i r_i$. Now, we consider the case $\nu_i | F$, which includes the case $F = 0$. Then we have $\nu_{i+1} = H \nu_i$ for a positive integer H . When $\mu_{i+1} = H \mu_i$, by using Lemma 5, if $H \leq \exp(\mathbf{L} r_i \nu_i) / 2$ then

$$\begin{aligned} |1 - \mathbf{e}(\mu_{i+1} \tau + \nu_{i+1} v)| &= |1 - \mathbf{e}(H \cdot (\mu_i \tau + \nu_i v))| \geq H/2 \cdot |1 - \mathbf{e}(\mu_i \tau + \nu_i v)| \\ &\geq \frac{H}{4(r_i + 1)} \exp(-\mathbf{L}(r_i + 1) \nu_i) \end{aligned}$$

The last inequality follows from the definition of r_i and Lemma 5. On the other hand

$$|1 - \mathbf{e}(\mu_{i+1} \tau + \nu_{i+1} v)| \leq \exp(-\mathbf{L} \cdot H \nu_i),$$

and $H \geq r_i + 2$, which gives a contradiction. This shows that $H > \exp(\mathbf{L} r_i \nu_i) / 2$ and $\nu_{i+1} > \exp(\mathbf{L} r_i \nu_i)$. If $\mu_{i+1} \neq H \mu_i$, then there exists a positive constant c which depends only on τ such that $c < |1 - \mathbf{e}((\mu_{i+1} - H \mu_i) \tau)|$. But we have

$$\begin{aligned} |1 - \mathbf{e}((\mu_{i+1} - H \mu_i) \tau)| &\leq |1 - \mathbf{e}(\mu_{i+1} \tau + \nu_{i+1} v)| + |1 - \mathbf{e}(H \cdot (\mu_i \tau + \nu_i v))|. \\ &\leq \exp(-\mathbf{L} \nu_{i+1}) + |1 - \mathbf{e}(H \cdot (\mu_i \tau + \nu_i v))| \end{aligned}$$

Choose \mathbf{L} sufficiently large so that $\exp(-\mathbf{L}) < c/2$. Applying Lemma 5, we obtain $H \gg \exp(\mathbf{L} r_i \nu_i)$ and $\nu_{i+1} > \exp(\mathbf{L} r_i \nu_i)$. Let r_{i+1} be the integer defined by the property (d') for $j = i + 1$. Then, in a similar way as above, we can show that (b') for $j = i + 1$ is valid. This completes the proof. \square

Now we prove the average asymptotic behavior of elliptic sequence.

Lemma 7. Let $\{h_n\}$ be an elliptic sequence satisfying $h_2 | h_4$, $(h_3, h_4) = 1$, $\Delta \neq 0$ and $h_2 h_3 h_4 h_5 \neq 0$. Then we have

$$\frac{1}{n} \log |h_1 h_2 \cdots h_n| = \frac{A(u)}{3} n^2 + O(n),$$

where u is a complex number determined by $h_n = \psi_n(u)$, and $A(\cdot)$ is defined by (10).

Proof. Let C be the set defined in Lemma 6. If C is finite, then by Lemma 4, we see that $A(nu) = O(n)$. Thus we have, by Lemma 2,

$$\begin{aligned}\log |h_1 h_2 \cdots h_n| &= \sum_{i=1}^n \left(A(u) i^2 + O(i) \right) \\ &= \frac{A(u)}{3} n^3 + O(n^2).\end{aligned}$$

This shows the assertion. Now we assume that C is an infinite set.

$$\begin{aligned}\log |h_1 h_2 \cdots h_n| &= \sum_{i=1}^n A(u) i^2 - \sum_{i=1}^n A(iu) \\ &= \frac{A(u)}{3} n^3 + O(n^2) - \sum_{i \notin C(n)} A(iu) - \sum_{i \in C(n)} A(iu),\end{aligned}\tag{14}$$

where $C(n) = \{i \in \mathbf{N} \mid i \leq n, n \in C\}$. By the definition of C and Lemma 4, we have

$$\sum_{i \notin C(n)} A(iu) = O\left(\sum_{i=1}^n i\right) = O(n^2).\tag{15}$$

Without loss of generality, we may assume that n is an integer in the interval $l\nu_k \leq n < (l+1)\nu_k$, $l \leq r_k$, where k, l are positive integers. Then we have

$$\sum_{i \in C(n)} A(iu) = \sum_{i=1}^{k-1} \sum_{j=1}^{r_i} \xi(j\nu_i) + \sum_{j=1}^l \xi(j\nu_k) + O\left(\sum_{i=1}^n i\right).$$

By Lemma 6, we have

$$\sum_{i=1}^{k-1} \sum_{j=1}^{r_i} \xi(j\nu_i) \leq \sum_{i=1}^{k-1} r_i \xi(\nu_i),$$

and

$$\sum_{j=1}^l \xi(j\nu_k) \leq l\xi(\nu_k).$$

Since each $h_n (n \geq 1)$ is a non zero integer, we see $A(nu) \leq A(u)n^2$. So, by Lemma 4, we have $A(nu) = O(n^2)$. This implies that $\xi(x) = O(x^2)$. Thus

$$\sum_{i=1}^{k-1} \sum_{j=1}^{r_i} \xi(j\nu_i) = O\left(\sum_{i=1}^{k-1} r_i \nu_i^2\right) = O\left(kr_{k-1}\nu_{k-1}^2\right),$$

and

$$\sum_{j=1}^l \xi(j\nu_k) = O(l\nu_k^2) = O(n^2).$$

Using the inequality $\exp(Tr_{k-1}\nu_{k-1}) < \nu_k$ appearing in the proof of Lemma 6, we have

$$k - 1 \leq \nu_{k-1} \leq r_{k-1}\nu_{k-1} \leq \log(\nu_k)/T = \log(n)/T.$$

This shows that

$$\sum_{i=1}^{k-1} \sum_{j=1}^{r_i} \xi(j\nu_i) = O(\log^3 n) = O(n^2).$$

Summing up, we have shown

$$\sum_{i \in C(n)} A(iu) = O(n^2).$$

By (14) and (15), we see the assertion. \square

Our last task is to show that $A(u) > 0$ for the elliptic sequence of Lemma 7.

Lemma 8. Let $\{h_n\}$ be an elliptic sequence satisfying $h_2|h_4$, $(h_3, h_4) = 1$. Then, for any prime p , there exists $n \leq 2p + 1$ such that $p|h_n$.

Proof. This is the Theorem 5.1 of Ward [12]. Consider $h_{n-1}h_{n+1}/h_n^2 \pmod{p}$ for $n = 2, 3, \dots, p + 1$ and use Dirichlet's box principle with (9). \square

Lemma 9. Let $\{h_n\}$ be an elliptic sequence satisfying $h_2|h_4$, $\Delta \neq 0$ and $h_2h_3h_4h_5 \neq 0$. Let u be the complex number determined by $h_n = \psi_n(u)$. Then we have $A(u) > 0$.

Proof. By Lemma 2, we have $\log|h_n| = A(u)n^2 - A(nu)$. If $A(u) < 0$, by Lemma 4, $\log|h_n| < 0$ for a certain n , which contradicts the fact $|h_n| \geq 1$. This shows that $A(u) \geq 0$. Assume that $A(u) = 0$. Then $\log|h_n| = -A(nu)$ holds for all n . By Lemma 4, there exists a positive constant K such that $|h_n| \leq K$. Let p be a prime greater than K . Then Lemma 8 implies that $p|h_n$ for a certain n . This shows $h_n = 0$. This is a contradiction. \square

Theorem 4. Let $\{h_n\}$ be an elliptic sequence satisfying $h_2|h_4$, $(h_3, h_4) = 1$, $\Delta \neq 0$ and $h_2h_3h_4h_5 \neq 0$. Then we have

$$\frac{\log|h_1h_2 \cdots h_n|}{\log[h_1, h_2, \dots, h_n]} = \zeta(3) + O\left(\frac{1}{n}\right).$$

Proof. Combine Theorem 3, Lemma 7 and Lemma 9. \square

§4. Concluding Remarks.

In section 1, we proposed axiom (S) in order to treat the least common multiple of

sequences. How can we generalize these situations? The asymptotic behaviour of the least common multiples of sequences admits a rather big error term such as

$$\log[a_1, a_2, \dots, a_n] = (\text{main term}) + O(n^l),$$

to obtain our type of results. It seems that the axiom (S) is too strict. We want a weaker axiom to obtain this asymptotic formula without using (2).

It seems natural to expect $A(nu) = O(n)$. In other words, the estimation $\log |\psi_n(u)| = A(u)n^2 + O(n)$ for every n is expected. (However, it would not cause any improvement of our asymptotic formulas.) In the case of sequences of Lucas type, this individual estimation is established in the light of Baker's estimation of the summation of logarithm of algebraic numbers. The analogue of this for our case is needed. Up to now, the author does not know any result of this type. However if it exists, the above argument has an independent merit. To derive the average asymptotic behavior of this sequence, we do not use the fact that the corresponding elliptic curve is defined over rational number field. Thus our argument, elementary but a little complicated, might be used in other problems.

There exist examples of elliptic sequences with $A(u) = 0$, which stimulated some interest to the author. Let $(h_2, h_3, h_4) = (1, 1, 1)$ or $(1, 1, 0)$. In this case we see $\Delta \neq 0$ and $h_\kappa = 0$ for a certain κ . Take the smallest such $\kappa (\geq 4)$. Choose u such that $h_n = \psi_n(u)$. Then u is a κ -division point of the corresponding elliptic curve. This shows that $h_{n\kappa} = 0$ for every $n \in \mathbf{N}$, $h_n \neq 0$ for $\kappa \nmid n$ and $h_n = h_{n+\kappa}$ for every n . The formula $\log |\psi_n(u)| = A(u)n^2 - A(nu)$ still holds for $\kappa \nmid n$. Using the argument of Lemma 9, we have $A(u) \geq 0$. If $A(u) > 0$ then, by Lemma 6, $\psi_n(u) = h_n$ is not bounded, which contradicts the periodicity of h_n . This shows that $A(u) = 0$, which gives a relation:

$$\log |\sigma(u)| = \operatorname{Re}(\eta_1 u^2 / (2w_1)) + \pi(\operatorname{Im}(u / (2w_1)))^2 / \operatorname{Im}(\tau),$$

by the use of (11).

Some numerical examples are found in the following Table 1.

Acknowledgements.

The author would like to express his gratitude to the referee for careful reading of the manuscript.

Table 1.

$(h_2, h_3, h_4) = (1, 1, -1)$ $p = 1/3$ $g_2 = 4/3$ $g_3 = -35/27$ $\Delta = -43$ $J = -64/1161$ $\tau = -1/2 + 1.002926948197305394966\sqrt{-1}$ $w_1 = 0 + 1.363182418170433596392\sqrt{-1}$ $u = 1.531551051899213180325$ $A(u) = 0.031408253543743824633$
$(h_2, h_3, h_4) = (1, 2, 1)$ $p = 3/4$ $g_2 = 19/4$ $g_3 = -23/8$ $\Delta = -116$ $J = -6859/7424$ $\tau = -1/2 + 1.228990832129246397562\sqrt{-1}$ $w_1 = 0 + 1.111804814975135231767\sqrt{-1}$ $u = 1.301268905063793834665$ $A(u) = 0.084840615679859699533$
$(h_2, h_3, h_4) = (1, 3, 1)$ $p = 28/27$ $g_2 = 2812/243$ $g_3 = -168083/19683$ $\Delta = -11321/27$ $J = -22235451328/6016443561$ $\tau = -1/2 + 1.411429696528812658305\sqrt{-1}$ $w_1 = 0 + 0.907350665488871173676\sqrt{-1}$ $u = 1.252539774071157056878$ $A(u) = 0.136695663405057918491$
$(h_2, h_3, h_4) = (1, -1, 1)$ $p = 0$ $g_2 = 4$ $g_3 = -1$ $\Delta = 37$ $J = 64/37$ $\tau = 0 + 1.221127360764627252496\sqrt{-1}$ $w_1 = 0 + 1.225694690993395030427\sqrt{-1}$ $u = -0.92959271528539567440519$ $\quad + 1.22569469099339503042711\sqrt{-1}$ $A(u) = 0.025555704119984420117$

$(h_2, h_3, h_4) = (2, 1, 4)$ $p = 41/6$ $g_2 = 1573/3$ $g_3 = -62387/27$ $\Delta = -676$ $J = -23030293/108$ $\tau = -1/2 + 3.139317204766964341216\sqrt{-1}$ $w_1 = 0 + 0.352738304847112422947\sqrt{-1}$ $u = 0.660057981718722555872$ $A(u) = 0.126242626431163986909$
$(h_2, h_3, h_4) = (3, 5, 6)$ $p = 821/300$ $g_2 = 425041/7500$ $g_3 = -277119161/3375000$ $\Delta = -2129/125$ $J = -76787844018343921/7185375000000$ $\tau = -1/2 + 2.662903182751486527437\sqrt{-1}$ $w_1 = 0 + 0.615192114179878726930\sqrt{-1}$ $u = 0.759101080162039522511$ $A(u) = 0.162312085677860900909$
$(h_2, h_3, h_4) = (1, 1, 0)$ $p = 5/12$ $g_2 = 1/12$ $g_3 = -161/216$ $\Delta = -15$ $J = -1/25920$ $\tau = -1/2 + 0.877437661348222505688\sqrt{-1}$ $w_1 = 0 + 1.596242222131783510148\sqrt{-1}$ $u = 1.400603042332602023180$ $A(u) = 0.000000000000000000000$
$(h_2, h_3, h_4) = (1, 1, 1)$ $p = 2/3$ $g_2 = 4/3$ $g_3 = -19/27$ $\Delta = -11$ $J = -64/297$ $\tau = -1/2 + 1.087533286862971250700\sqrt{-1}$ $w_1 = 0 + 1.458816616938495229330\sqrt{-1}$ $u = 1.269209304279553421688$ $A(u) = 0.000000000000000000000$

References

- [1] S. Akiyama, Lehmer numbers and an asymptotic formula for π , *J. Number Theory* **36** (1990) 328-331.
- [2] S. Akiyama, A new type of inclusion exclusion principle for sequences and asymptotic formulas for $\zeta(n)$, *J. Number Theory* **45** (1993) 200-214.
- [3] P. Horak and L. Skula, A characterization of the second order strong divisibility sequences, *Fibonacci Quart.* **23** (1985) no. 2, 126–132.
- [4] C. Kimberling, Strong divisibility sequences and some conjectures, *Fibonacci Quart.* **17** (1979) no. 1, 13 - 17.
- [5] P. Kiss and F. Mátyás, An asymptotic formula for π , *J. Number Theory* **31** (1989) 255-259.
- [6] P. Kiss and B. Tropic, Average order of logarithms of terms in binary recurrences, *Discussion Math.* **10** (1990) 29-39.
- [7] Y.V. Matiyasevich and R.K. Guy, A new formula for π , *Amer. Math. Monthly* **93** (1986) 631-635.
- [8] A.I. Saltykov, On Euler's function, *Vestnik M.G.U.*, **15** (1960), 34-50
- [9] A. Schinzel, Second order strong divisibility sequences in an algebraic number field, *Arch. Math. (Brno)* **23** (1987) no. 3, 181–186.
- [10] B. Tropic, Some asymptotic properties of Lucas numbers, *Algebra and number theory, Pedagogical Univ.* (1990) 49-55, ed. A Grytczuk.
- [11] A. Walfisz, *Weylsche Exponentialsummen in der neuen Zahlen Theorie*, *Mathematische Forschungsberichte* **15**, Deutsher Verlag Wissen. , Berlin 1963.
- [12] M. Ward, Memoir on elliptic divisibility sequence, *Amer. J. Math.* **70** (1948) 31-74.
- [13] M. Ward, The law of repetition of primes in an elliptic divisibility sequence, *Duke Math. J.* **15** (1948) 941-946.
- [14] M. Ward, The mapping of the positive integers into themselves which preserve division, *Pacific J. Math.* **5** (1955) 1013-1023.

FACULTY OF SCIENCE, NIIGATA UNIVERSITY
NIIGATA, 950-21, JAPAN