Indian J. Pure Appl. Math., **46**(5): 701-714, October 2015

DOI: 10.1007/s13226-015-0140-9

THE NUMERICAL FACTORS OF $\Delta_n(f,g)$[1]

Qingzhong Ji and Hourong Qin

Department of Mathematics, Nanjing University, Nanjing 210093*, P. R. China,*
e-mails: qingzhji@nju.edu.cn, hrqin@nju.edu.cn

(*Received* 19 *June* 2014; *after final revision* 30 *September* 2014;
accepted 24 *December* 2014)

Let $\alpha_1, \alpha_2, \ldots, \alpha_r$ be the roots of the polynomial $f(x) = x^r + a_1x^{r-1} + \cdots + a_r \in \mathbb{Z}[x]$ and let $g = \{g_n(X)\}_{n\in\mathbb{N}}$, where $g_n(X) = g_n(x_1, x_2, \ldots, x_r) \in \mathbb{Z}[x_1, x_2, \ldots, x_r]$ is a symmetric polynomial. For each n, put $\Delta_n(f,g) = g_n(\alpha_1, \alpha_2, \ldots, \alpha_r)$. In this paper, for a special symmetric polynomial sequence g, we investigate the numerical factors of $\Delta_n(f,g)$. If p is a prime, we establish an analogue of Iwasawa's theorem in algebraic number theory for the orders $\mathrm{ord}_p(\Delta_{np^t}(f,g))$ of the p-primary part of $\Delta_{np^t}(f,g)$ when t varies.

Key words : Recurring series; Iwasawa theory; cyclotomic polynomial.

1. INTRODUCTION

Throughout this paper, let $\mathbb{Q}$, $\mathbb{Z}$ and $\mathbb{N}$ denote the field of rational numbers, the ring of rational integers and the set of nonnegative integers, respectively. Let $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$. As usual, let ord_p denote the p-adic valuation of $\mathbb{Q}_p$ such that $\mathrm{ord}_p(p) = 1$.

Let $\alpha_1, \alpha_2, \ldots, \alpha_r$ be the roots of the polynomial

$$f(x) = x^r + a_1x^{r-1} + \cdots + a_{r-1}x + a_r \tag{1}$$

whose coefficients are rational integers. Suppose $g = \{g_n(X)\}_{n\in\mathbb{N}}$ is a polynomial sequence, where $g_n(X) = g_n(x_1, x_2, \ldots, x_r) \in \mathbb{Z}[x_1, x_2, \ldots, x_r]$ is a symmetric polynomial in r variables. For each n, put

$$\Delta_n(f,g) = g_n(\alpha_1, \alpha_2, \ldots, \alpha_r). \tag{2}$$

[1]Supported by NSFC (Nos. 11171141, 11471154, 11271177), NSFJ (Nos. BK2010007, BK2010362), PAPD and the Cultivation Fund of the Key Scientific and Technical Innovation Project, Ministry of Education of China (No. 708044).

It is clear that $\Delta_n(f,g) \in \mathbb{Z}$. For example, if $g_n(x_1, x_2, \ldots, x_r) = \prod_{i=1}^{r}(1 - x_i^n)$, then

$$\Delta_n(f,g) = \prod_{i=1}^{r}(1 - \alpha_i^n) \in \mathbb{Z}. \tag{3}$$

This function was introduced by Pierce [4] who studied the forms of its primitive factors. Later, Lehmer [3] made a detailed study of this sequence of numbers.

The theory of $\mathbb{Z}_p$-extensions is one of the most fruitful areas of research in number theory. A beautiful result in this area is the theorem of Iwasawa which describes the behavior of the p-part of the class number in a $\mathbb{Z}_p$-extension of number fields.

Iwasawa Theorem ([7], Theorem 13.13.) — *Let K_∞/K be a $\mathbb{Z}_p$-extension and $K_\infty = \bigcup_{n=0}^{+\infty} K_n$ with $[K_n : K] = p^n$. Let p^{e_n} be the exact power of p dividing the class number of K_n. Then there exist integers $\lambda \geq 0,\ \mu \geq 0$ and ν, all independent of n, and an integer n_0 such that*

$$e_n = \lambda n + \mu p^n + \nu, \quad for \ \ all \ \ n \geq n_0.$$

By the structure of Λ-modules, one sees that p^{e_n} is indeed the value of the characteristic polynomial of some Λ-module at special points. From this viewpoint, in [2], the authors prove an analogue of Iwasawa's theorem for higher K-groups of curves over finite fields. Let X be a smooth projective curve of genus g over a finite field $\mathbb{F}$ with q elements. For $m \geq 1$, let X_m be the curve X over the finite field $\mathbb{F}_m$, the m-th extension of $\mathbb{F}$. For $1 \leq i \leq 2g$, denote by π_i the characteristic roots of the Frobenius endomorphism ϕ. Set

$$g_{n,m}(x_1, x_2, \cdots, x_{2g}) = \prod_{i=1}^{2g}(1 - (q^n x_i)^m).$$

We have $\sharp K_{2n}(X_m) = g_{n,m}(\pi_1, \pi_2, \cdots, \pi_{2g})$, where $K_{2n}(X_m)$ is the K-group of the smooth projective curve X_m. Let p be a prime. Denote the p-primary part of the order of $K_{2n}(X_{p^t})$ by $p^{e_{n,p}(t)}$, i.e., $e_{n,p}(t) = \mathrm{ord}_p(\sharp K_{2n}(X_{p^t}))$.

***Theorem* 1.1** ([2]) — *There exist integers $\lambda_{n,p} \geq 0$, $\nu_{n,p}$ and a positive integer $T_{n,p}$ such that*

$$e_{n,p}(t) = \lambda_{n,p} t + \nu_{n,p}, \quad for \ \ all \ \ t \geq T_{n,p}.$$

Let $f(x) = x^2 - Px - Q \in \mathbb{Z}[x]$ and $g = \{g_n(x_1, x_2)\}_{n \in \mathbb{N}}$, where $g_0(x_1, x_2) = 0$, $g_n(x_1, x_2) = \sum_{k=0}^{n-1} x_1^k x_2^{n-1-k},\ n \geq 1$. It is well-known that the recurring series $\Delta_n(f,g)$ is the Lucas sequences L_n with parameters P and Q. The following results are consequences of the well-known properties of the Primitive Divisor Theorem for Lucas sequences.

***Theorem* 1.2** — ([1]) *Let $n \in \mathbb{N}^*$ and p a prime.*

(1) *If $p \nmid L_nL_p$, then $\mathrm{ord}_p(L_{np^t}) = 0$, for all $t \in \mathbb{N}$.*

(2) *If $p|L_nL_p$, then there exist integers $\nu_{n,p}$ and $T_{n,p}$ such that*

$$\mathrm{ord}_p(L_{np^t}) = t + \nu_{n,p}, \quad for \;\; all \;\; t \geq T_{n,p}.$$

(3) *Let $n \in \mathbb{N}^*$ and p, q be two different primes. Then there exists a positive integer $T_{n,p,q}$ such that*

$$\mathrm{ord}_q(L_{np^t}) = \mathrm{ord}_q(L_{np^{T_{n,p,q}}}), \;\; \text{for all} \;\; t \geq T_{n,p,q},$$

i.e., the numbers $\mathrm{ord}_q(L_{np^t})$ are stable when t is sufficiently large.

(4) *Let $S_{n,p}(t)$ be the set of all primes which divide L_{np^t}. Then $\sharp S_{n,p}(t) \longrightarrow +\infty$ as $t \longrightarrow +\infty$.*

In this paper, we generalize Pierce's recurring series $\{\Delta_n\}_{n\in\mathbb{N}}$ defined by (3) and $\{g_{n,m}(\pi_1, \pi_2, \cdots, \pi_{2g})\}_{m\in\mathbb{N}}$ defined above to the recurring series $\{\Delta_{n,m}\}_{n\in\mathbb{N}}$ for any integer $m \in \mathbb{N}^*$, where $\Delta_{n,m} = \prod_{i=1}^{r}(m^n - \alpha_i^n)$. We give a detailed study of essential and characteristic factors of $\Delta_{n,m}$ especially as regards sequences of numbers. Let p be a prime and $n, m \in \mathbb{N}^*$, we establish an analogue of Iwasawa's theorem for the orders $\mathrm{ord}_p(\Delta_{np^t,m})$ as follows.

***Theorem* 3.7** — *Let p be a prime. Fix integers $n, m \in \mathbb{N}^*$, let $p^{e_{n,m,p}(t)}$ be the p-primary part of $\Delta_{np^t,m}$ for $t \in \mathbb{N}$.*

(1) *If $p \nmid \Delta_{n,m}$, then $e_{n,m,p}(t) = 0$ for all $t \in \mathbb{N}$.*

(2) *If $p|\Delta_{n,m}$, then there exist integers $\lambda_{n,m,p} \geq 1$ and $\nu_{n,m,p}$, both independent of t, and an integer $T_{n,m,p}$ such that*

$$e_{n,m,p}(t) = \lambda_{n,m,p}t + \nu_{n,m,p}, \quad for \;\; all \;\; t \geq T_{n,m,p}.$$

On the other hand, let p, q be two different primes, we prove that the numbers $\mathrm{ord}_q(\Delta_{np^t,m})$ are stable when t is sufficiently large (See Theorem 3.9). We also prove that the number of prime factors of $\Delta_{np^t,m}$ goes to infinity as t goes to infinity. (See Corollary 3.10).

2. FACTORIZATION OF $\Delta_{n,m}$

Let the notation be as in §1. In this section, fix an integer $m \in \mathbb{N}^*$, define $g_m = \{g_n^{(m)}(X)\}_{n\in\mathbb{N}}$ as follows

$$g_n^{(m)}(x_1, x_2, \ldots, x_r) = \prod_{i=1}^{r}(m^n - x_i^n).$$

2.1 *Definition of* $\Delta_{n,m}$ — Let $\alpha_1, \dots, \alpha_r$ be the roots of the polynomial $f(x) \in \mathbb{Z}[x]$ defined by (1). Then $\Delta_{n,m}$ is defined by

$$\Delta_{n,m} = \Delta_n(f, g_m) = g_n^{(m)}(\alpha_1, \alpha_2, \dots, \alpha_r) = \prod_{i=1}^{r}(m^n - \alpha_i^n). \tag{4}$$

Pierce [4] and Lehmer [3] listed many properties of $\Delta_n = \Delta_{n,1}$. In this section, we will generalize all results in [3] concerning Δ_n to the case $\Delta_{n,m}$, for all $n, m \in \mathbb{N}^*$. We would like point out that the idea used here is similar to that in [3].

Remark 2.2 : (1) The polynomial $f(x)$ can be viewed as a characteristic polynomial of some $r \times r$ matrix A, for example,

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_r \\ 1 & 0 & \cdots & 0 & -a_{r-1} \\ 0 & 1 & \cdots & 0 & -a_{r-2} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_1 \end{pmatrix}.$$

Then $f(x) = |xE - A|$ and

$$\Delta_{n,m} = |m^n E - A^n|, \tag{5}$$

where $|B| = \det(B)$ for any square matrix B.

(2) Let α be a root of $f(x)$. If $f(x)$ is irreducible, then

$$\Delta_{n,m} = N_{K/\mathbb{Q}}(m^n - \alpha^n),$$

where $K = \mathbb{Q}(\alpha)$ and $N_{K/\mathbb{Q}}$ is the norm map from the field K to $\mathbb{Q}$.

(3) Since $(m, a_r)|\Delta_{n,m}$, for our purposes, we always assume $(m, a_r) = 1$ in this section.

2.3 *Essential and characteristic factors of* $\Delta_{n,m}$

Let $\Phi_\delta(x, y)$ be the δth homogeneous cyclotomic polynomial, *i.e.*,

$$\Phi_\delta(x, y) = \prod_{\substack{i=1 \\ (i,\delta)=1}}^{\delta} (x - y\zeta_\delta^i) \tag{6}$$

where ζ_δ is a primitive δth root of unity. Then we define the integer $\Phi^*_{\delta,m}$ by

$$\Phi^*_{\delta,m} = \prod_{i=1}^{r} \Phi_\delta(m, \alpha_i). \tag{7}$$

It follows from the formula $x^n - y^n = \prod_{\delta|n} \Phi_\delta(x, y)$ that

$$\Delta_{n,m} = \prod_{\delta|n} \Phi^*_{\delta,m}. \tag{8}$$

This gives a partial factorization of $\Delta_{n,m}$ into integer factors. If we assume that each Δ, whose first subscript is a proper divisor of n, has been factored, the complete factorization of $\Delta_{n,m}$ depends only on that of $\Phi^*_{n,m}$. For this reason we call this latter number the *essential* factor of $\Delta_{n,m}$. On the other hand, we may consider the prime factors of $\Delta_{n,m}$. Similarly, the prime factors of $\Delta_{n,m}$ which do not divide $\Delta_{d,m}$, where d is a proper divisor of n, are called the *characteristic prime factors* of $\Delta_{n,m}$. The concepts of *essential* factor and *characteristic prime factors* were introduced by Lehmer [3].

Lemma 2.4 — The essential factor $\Phi^*_{n,m}$ of $\Delta_{n,m}$ contains all the characteristic prime factors of $\Delta_{n,m}$.

PROOF : By (8) a characteristic prime factor p of $\Delta_{n,m}$ must divide $\Phi^*_{\delta,m}$ for some divisor δ of n. If δ were less than n, and hence p would divide $\Delta_{\delta,m}$, contrary to the definition of p. Therefore $\delta = n$ and the lemma follows. □

Lemma 2.5 — A characteristic prime factor p of $\Delta_{n,m}$ cannot divide n.

PROOF : If possible, let $n = p\delta$. Suppose $f(x) = |xE - A|$ for some matrix A. Then by the multinomial theorem modulo p and (5), we have

$$\begin{aligned} 0 \equiv \Delta_{n,m} &\equiv \Delta_{p\delta,m} \\ &\equiv |m^{p\delta}E - A^{p\delta}| \\ &\equiv |m^{\delta}E - A^{\delta}|^p \\ &\equiv |m^{\delta}E - A^{\delta}| \\ &\equiv \Delta_{\delta,m} \pmod p. \end{aligned}$$

This contradicts the hypothesis that p is a characteristic factor of $\Delta_{n,m}$. □

Remark : (1) It is not true that the essential factor of $\Delta_{n,m}$ is made up exclusively of characteristic prime factors (See [3], p. 462).

(2) The essential factor $\Phi^*_{n,m}$ may, however, have a factor in common with n.

(3) If f is reducible over the rational field so that $f = f_1 f_2$, then

$$\Delta_{n,m}(f) = \Delta_{n,m}(f_1)\Delta_{n,m}(f_2)$$

is a factorization into integers. Hence for our purposes we may suppose that f is irreducible. The following result is a generalization of [7], Lemma 2.9.

***Theorem* 2.6** — *If p^e($e > 0$) is the highest power of a characteristic prime factor p of $\Delta_{n,m}(f)$, where f is irreducible and of degree r, and if w is the order of p mod n, then $w \le r$ and e is divisible by w.*

PROOF : It is similar to the proof of [3], Theorem 3. □

2.7 *The recurring series for* $\Delta_{n,m}$

In order to render the factorization of $\Delta_{n,m}$ practical, it is first necessary to have a simple method of calculating its actual value. This is done with the help of a polynomial $M_m(x)$ uniquely determined by $f(x)$ and m in the following manner. Let

$$\begin{array}{ll} f_0(x) & = x - m^r, \\ f_1(x) & = \prod_{i=1}^{r}(x - m^{r-1}\alpha_i), \\ f_2(x) & = \prod_{1\le j<i\le r}(x - m^{r-2}\alpha_i\alpha_j), \\ \cdots & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ f_r(x) & = x - \alpha_1\alpha_2\cdots\alpha_r = x - (-1)^r a_r. \end{array}$$

$M_m(x)$ is defined as the least common multiple of these f's. That is,

$$M_m(x) = [f_0(x), f_1(x), \ldots, f_r(x)] = x^q + A_1x^{q-1} + A_2x^{q-2} + \cdots + A_q.$$

Definition 2.8 — Let $\{x_n\}_{n=0}^{\infty}$ be a recurring series such that

$$x_{n+e} + a_1x_{n+e-1} + \cdots + a_{e-1}x_{n+1} + a_ex_n = 0, \quad \text{for all } \; n \ge 0.$$

Then the polynomial $x^e + a_1x^{e-1} + \cdots + a_{e-1}x + a_e$ is called the scale of the recurring series $\{x_n\}_{n=0}^{\infty}$.

***Theorem* 2.9** — *The numbers*

$$\Delta_{0,m},\; \Delta_{1,m},\; \Delta_{2,m},\; \Delta_{3,m}, \cdots$$

form a recurring series whose scale is $M_m(x)$. That is, for every $n \ge 0$,

$$\Delta_{n+q,m} + A_1\Delta_{n+q-1,m} + \cdots + A_{q-1}\Delta_{n+1,m} + A_q\Delta_{n,m} = 0. \tag{9}$$

PROOF : By the definition (4) of $\Delta_{n,m}$, we have

$$\Delta_{n,m} = \prod_{i=1}^{r}(m^n - \alpha_i^n) = \sum_{k=0}^{r}\sum_{1\le i_1<\cdots<i_k\le r}(-1)^k m^{(r-k)n}\alpha_{i_1}^n\cdots\alpha_{i_k}^n.$$

Hence we obtain

$$\sum_{i=0}^{q} A_i \Delta_{n+q-i,m} = \sum_{k=0}^{r} \sum_{1\le i_1<\cdots<i_k\le r} (-1)^k m^{(r-k)n} \alpha_{i_1}^n \cdots \alpha_{i_k}^n M_m(m^{(r-k)} \alpha_{i_1} \cdots \alpha_{i_k}) = 0,$$

where $A_0 = 1$. This completes the theorem. □

2.10 q-periodic Δ's

Lehmer [3] has proved that $\Delta_{n,1}$ is a periodic function of proper period τ if and only if $f(x) = \Phi_\tau(x,1)$. In this subsection, for a fixed integer m, we will consider the periodic properties of $\Delta_{n,m}$.

Definition 2.11 — Suppose $F:\ \mathbb{Z} \longrightarrow \mathbb{C}$ is a number theory function. We call F a q-periodic function of period τ, if there exists a function $\lambda(n)$ such that

$$F(q\tau + k) = \lambda(q)F(k), \text{ for all } q,\ k \in \mathbb{Z}. \tag{10}$$

The function λ is called a periodic factor of F. We also call F q-periodic with respect to λ. A positive integer τ is called a proper period of a q-periodic function F, if for any positive integer $T < \tau$, F is not q-periodic of period T.

Remark 2.12 : (1) It is obvious that a periodic function F is q-periodic, in this case $\lambda(n) = 1, \text{ for all } n \in \mathbb{Z}$.

(2) If the function F is defined over $\mathbb{N}$ and τ is a positive integer such that

$$F(q\tau + k) = \lambda(q)F(k), \text{ for all } q,\ k \in \mathbb{N},$$

for some function $\lambda(n)$ defined over $\mathbb{N}$, then F can be extended to a q-periodic function defined over $\mathbb{Z}$. In this case we also call F a q-periodic function defined over $\mathbb{N}$.

Lemma 2.13 — If $F \neq 0$ is a q-periodic function with respect to a function λ, then $\lambda(n) \neq 0$ for all $n \in \mathbb{Z}$ and $\lambda:\ \mathbb{Z} \longrightarrow \mathbb{C}^*$ is a group homomorphism.

PROOF : Suppose there exists an integer $n_0 \in \mathbb{Z}$ such that $\lambda(n_0) = 0$. By (10), for any $n \in \mathbb{Z}$, we have

$$F(n) = F(n_0T + (n - n_0T)) = \lambda(n_0)F(n - n_0T) = 0.$$

This contradicts the assumption $F \neq 0$. It is easy to see that $\lambda(0) = 1$ and $\lambda(m+n) = \lambda(m)\lambda(n)$ for all $m, n \in \mathbb{Z}$. Hence λ is a group homomorphism. □

Lemma 2.14 — Suppose τ is a proper period of a q-periodic function F. If T is a period of F, then $\tau|T$.

PROOF : First we prove that q-periodic functions have properties similar to those of periodic functions. Let $T > 0$ be a period of a q-periodic function $F(n)$, *i.e.*, there exists a function $\lambda(n)$ such that

$$F(qT + k) = \lambda(q)F(k), \text{ for all } q, k \in \mathbb{Z}.$$

Then we have

(i) for any $a \in \mathbb{Z}$, aT is a period of F. In fact, set $\lambda_a(n) = \lambda(an)$, then

$$F(qaT + k) = \lambda(aq)F(k) = \lambda_a(q)F(k), \text{ for all } q, k \in \mathbb{Z}.$$

(ii) if T_1 and T_2 are two periods of F, then $T_1 + T_2$ is also a period of F. Assume λ_i is corresponding to T_i, $i = 1, 2$. Set $\lambda(n) = \lambda_1(n)\lambda_2(n)$, then

$$F(q(T_1 + T_2) + k) = \lambda_1(q)F(qT_2 + k) = \lambda_1(q)\lambda_2(q)F(k) = \lambda(q)F(k), \text{ for all } q, k \in \mathbb{Z}.$$

Suppose $\tau \nmid T$. Then $T = q_0\tau + b$ where $q_0, b \in \mathbb{Z}$ and $0 < b < \tau$. By (i) and (ii) above, we obtain that $b = T - q_0\tau$ is a period of F. This contradicts the fact that τ is a proper period of F. □

For a fixed integer m, it may happen that $\Delta_{n,m}$ is a λ-periodic function of n. In this case we have

***Theorem* 2.15** — *A necessary and sufficient condition for $\Delta_{n,m}$ to be q-periodic function of n of proper period τ is that $f(x) = \Phi_\tau(x, m)$, where $\Phi_\tau(x, y)$ is the τ-th homogeneous cyclotomic polynomial defined by (6).*

PROOF : If $\Delta_{n,m}$ is q-periodic of proper period τ, then $\Delta_{\tau,m} = 0$. Hence f has a root α for which $\alpha^\tau = m^\tau$. Then there exists a primitive kth root ζ_k of unity such that $\alpha = m\zeta_k$. Since f is irreducible all its roots are $m\zeta_k^i,\ 1 \le i \le k,\ (k, i) = 1$, so that $f(x) = \Phi_k(x, m)$, where k is some divisor of τ. But $\Delta_{n,m}$ is of period k, for if n, j are any integers ≥ 0,

$$\Delta_{nk+j,m} = \prod_i (m^{nk+j} - \alpha_i^{nk+j}) = m^{\varphi(k)kn} \prod_i (m^j - \alpha_i^j) = \lambda(n)\Delta_{j,m},$$

where $\lambda(n) = m^{\varphi(k)kn}$ is the periodic factor. Hence by Lemma 2.14, τ is a divisor of k. Therefore $\tau = k$ and $f(x) = \Phi_\tau(x, m)$. □

3. IWASAWA THEORY OF $\Delta_{n,m}$

Let the notation be as in §2. For our purposes, in this section, we make the following hypothesis:

(H 1) $f(x)$ is defined by (1) and irreducible.

(H 2) Fix an integer m satisfying $(m, a_r) = 1$.

(H 3) $f(x) \neq \Phi_T(x,m)$ for all $T \in \mathbb{N}^*$.

Let $\mathbb{K} = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_r)$ be the splitting field of $f(x)$ over the rational number field $\mathbb{Q}$, $O_{\mathbb{K}}$ the ring of algebraic integers of $\mathbb{K}$. For any prime p, let $\mathfrak{P}$ be a prime ideal of $\mathbb{K}$ lying above p.

***Theorem* 3.1** — *Let $n \in \mathbb{N}$ and p be a prime factor of $\Delta_{n,m}$. Then, for any positive integer t satisfying $p|t$, we have $p|\frac{\Delta_{nt,m}}{\Delta_{n,m}}$.*

PROOF : By the formula (4), the condition $p|\Delta_{n,m}$ implies $m^n \equiv \alpha_i^n \pmod{\mathfrak{P}}$ for some $i (1 \leq i \leq r)$. If $p|t$, then we have

$$\frac{\Delta_{nt,m}}{\Delta_{n,m}} = \prod_{j=1}^{r} \frac{m^{nt} - \alpha_j^{nt}}{m^n - \alpha_j^n} \equiv t m^{n(t-1)} \prod_{\substack{j=1 \\ j \neq i}}^{r} \sum_{k=0}^{t-1} m^{nk} \alpha_j^{n(t-1-k)} \equiv 0 \pmod{\mathfrak{P}}.$$

Hence $p|\frac{\Delta_{nt,m}}{\Delta_{n,m}}$. □

Corollary 3.2 — (1) Let $n \in \mathbb{N}^*$ and p a prime factor of $\Delta_{n,m}$. Then, for all $t \in \mathbb{N}$, we have $p^{e+t}|\Delta_{np^t,m}$, where $e = \mathrm{ord}_p(\Delta_{n,m})$.

(2) Let $n,\ t \in \mathbb{N}^*$. Then we have $(\Delta_{n,m})^t|\Delta_{n(\Delta_{n,m})^{t-1},m}$.

PROOF : (1) It follows easily by induction on t. (2) It follows trivially from (1) and the fact: $\Delta_{n_1,m}|\Delta_{n_2,m}$, if $n_1|n_2$. □

Theorem 3.1 is about divisibility. The next result will be about non-divisibility. First, a definition. If p is a prime, put $d(p) = \mathrm{lcm}_{1 \leq i \leq [\mathbb{K}:\mathbb{Q}]}\{p^i - 1\}$. □

***Theorem* 3.3** — *Let $n,\ t \in \mathbb{N}^*$. Suppose p is a prime such that $p \nmid \Delta_{n,m}$ and $(t,\ d(p)) = 1$. Then* (i) $p \nmid \Delta_{nt,m}$; (ii) $p \nmid \Delta_{np^x,m}$ *for any $x \in \mathbb{N}$.*

PROOF : It is clear that (ii) follows (i). Hence it suffices to prove (i). If $p|\Delta_{nt,m}$, then

$$m^{nt} \equiv \alpha_i^{nt} \pmod{\mathfrak{P}} \ \text{ for some } \ i \ (1 \leq i \leq r). \tag{11}$$

If $\alpha_i \equiv 0 \pmod{\mathfrak{P}}$, then $m \equiv 0 \pmod{\mathfrak{P}}$. Hence $p|(a_r, m)$, this contradicts the assumption $(a_r, m) = 1$. So $m, \alpha_i \notin \mathfrak{P}$. By (11), we have

$$\left(\frac{\alpha_i^n}{m^n}\right)^t \equiv 1 \pmod{\mathfrak{P}}.$$

But $(\frac{\alpha_i^n}{m^n})^{d(p)} \equiv 1 \pmod{\mathfrak{P}}$ and $(t,\ d(p)) = 1$, we have $\frac{\alpha_i^n}{m^n} \equiv 1 \pmod{\mathfrak{P}}$, *i.e.*, $m^n \equiv \alpha_i^n \pmod{\mathfrak{P}}$. Hence $\Delta_{n,m} = \prod_{j=1}^r (m^n - \alpha_j^n) \equiv 0 \pmod{\mathfrak{P}}$ contradicts $p \nmid \Delta_{n,m}$. Hence $p \nmid \Delta_{nt,m}$. This completes the proof. □

Lemma 3.4 — Let n be the smallest integer such that $p|\Delta_{n,m}$. Then $n|d(p)$.

PROOF : From the proof of Theorem 3.3, if $p|\Delta_{n,m}$, then there exists an index i $(1 \leq i \leq r)$ such that $m^n \equiv \alpha_i^n \pmod{\mathfrak{P}}$ and $m, \alpha_i \notin \mathfrak{P}$.

(i) Assume $m \equiv \alpha_i \pmod{\mathfrak{P}}$. Then $\Delta_{1,m} = \prod_{j=1}^{r}(m - \alpha_j) \equiv 0 \pmod{\mathfrak{P}}$, so $n = 1$.

(ii) Assume $m \not\equiv \alpha_i \pmod{\mathfrak{P}}$. Then $\frac{\alpha_i}{m} \not\equiv 1 \pmod{\mathfrak{P}}$ and

$$(\frac{\alpha_i}{m})^n \equiv 1 \pmod{\mathfrak{P}}.$$

From the definition of n, it follows that n is the order of $\frac{\alpha_i}{m} \pmod{\mathfrak{P}}$. On the other hand, $(\frac{\alpha_i}{m})^{d(p)} \equiv 1 \pmod{\mathfrak{P}}$. Hence $n|d(p)$ as asserted. □

Corollary 3.5 — Let p be a prime. Then $p|\Delta_{1,m}$ if and only if $m \equiv \alpha_i \pmod{\mathfrak{P}}$ for some i $(1 \leq i \leq r)$.

Let $\mathbb{Q}_p$ be the p-adic completion of $\mathbb{Q}$. Let $\overline{\mathbb{Q}}$ and $\overline{\mathbb{Q}_p}$ be the algebraic closures of $\mathbb{Q}$ and $\mathbb{Q}_p$, respectively. Let ρ be an embedding of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}_p}$. We simply rename $\rho(a)$ as a.

We will keep the notation ord_p for the additive valuation from $\overline{\mathbb{Q}_p}$ to $\mathbb{Q}\bigcup\{\infty\}$, extended by the standard additive valuation ord_p from $\mathbb{Q}_p$ to $\mathbb{Z}\bigcup\{\infty\}$, namely, if $\alpha \in \overline{\mathbb{Q}_p}$, then

$$\mathrm{ord}_p(\alpha) = [\mathbb{Q}_p(\alpha) : \mathbb{Q}_p]^{-1}\mathrm{ord}_p(N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)).$$

Here $N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}$ is the usual norm map from $\mathbb{Q}_p(\alpha)$ to $\mathbb{Q}_p$.

Lemma 3.6 ([6], p. 172-174) — Let p and q be different primes. For $n \geq 1$, let $\xi \in \overline{\mathbb{Q}_p}$ be any primitive p^n-th root of unity. Then the following results hold.

(1) $\mathrm{ord}_p(\xi - 1) = \frac{1}{p^{n-1}(p-1)}$ and $\mathrm{ord}_q(\xi - 1) = 0$.

(2) Let $\alpha \in \overline{\mathbb{Q}_p}$ be integral over $\mathbb{Z}_p$.

(i) If $\mathrm{ord}_p(\alpha - 1) = 0$, then $\mathrm{ord}_p(\alpha^{p^t} - 1) = 0$ for all positive integers $t \geq 1$.

(ii) If $\mathrm{ord}_p(\alpha - 1) > 0$, then there exist an integer t_0 and a constant c depending on α such that

$$\mathrm{ord}_p(\alpha^{p^t} - 1) = t + c,$$

for all $t \geq t_0$. In fact, t_0 and c can be chosen as

$$t_0 = \min\{t \in \mathbb{Z}| \frac{1}{p^{t-1}(p-1)} < \mathrm{ord}_p(\alpha - 1)\},$$

and

$$c = \mathrm{ord}_p(\alpha - 1) + \sum_{1 \neq \xi \in S} [\mathrm{ord}_p(\alpha - \xi) - \mathrm{ord}_p(1 - \xi)],$$

where S is the set of p^i-th roots of unity, $1 \leq i < t_0$.

(3) Let $\beta \in \overline{\mathbb{Q}_q}$ be integral over $\mathbb{Z}_q$.

(i) If $\mathrm{ord}_q(\beta - 1) > 0$, then $\mathrm{ord}_q(\beta^{p^t} - 1) = \mathrm{ord}_q(\beta - 1) > 0$, for all $t \geq 1$.

(ii) If $\mathrm{ord}_q(\beta - 1) = 0$, then there exists an integer $t_0 \geq 0$ such that, for all $t \geq t_0$,

$$\mathrm{ord}_q(\beta^{p^t} - 1) = \mathrm{ord}_q(\beta^{p^{t_0}} - 1).$$

Let $n \in \mathbb{N}^*$ and p a prime. Set $e_{n,m,p}(t) = \mathrm{ord}_p(\Delta_{np^t,m})$ for $t \in \mathbb{N}$.

***Theorem* 3.7** — *Let $n \in \mathbb{N}^*$ and p a prime.*

(1) *If $p \nmid \Delta_{n,m}$, then $e_{n,m,p}(t) = 0$ for all $t \in \mathbb{N}$.*

(2) *If $p|\Delta_{n,m}$, then there exist integers $\lambda_{n,m,p} \geq 1, \nu_{n,m,p}$ and $T_{n,m,p}$ such that*

$$e_{n,m,p}(t) = \lambda_{n,m,p} t + \nu_{n,m,p}, \quad for \;\; all \;\; t \geq T_{n,m,p}.$$

PROOF : By Theorem 3.3, if $p \nmid \Delta_{n,m}$, then $e_{n,m,p}(t) = 0$, for all $t \in \mathbb{N}$. Hence, it suffices to prove (2). Assume $p|\Delta_{n,m}$. Without loss of generality, we may assume n is the smallest integer such that $p|\Delta_{n,m}$. By Lemma 3.4, $n|d(p)$, hence $(p, n) = 1$. Let ζ_n be a primitive nth root of unity. Then

$$\Delta_{n,m} = \prod_{i=1}^{r} (m^n - \alpha_i^n) = \prod_{i=1}^{r} \prod_{j=0}^{n-1} (m - \alpha_i \zeta_n^j) = m^{rn} \prod_{i=1}^{r} \prod_{j=0}^{n-1} (1 - \frac{\alpha_i}{m} \zeta_n^j).$$

Note that $p|\Delta_{n,m}$ implies $\mathrm{ord}_p(m) = 0$ (see the proof of Theorem 3.3). Hence we have $\mathrm{ord}_p(1 - \frac{\alpha_i}{m}\zeta_n^j) \geq 0$ for all $1 \leq i \leq r, \; 0 \leq j \leq n - 1$. For each i $(1 \leq i \leq r)$, we claim that there is at most one index j_0 $(0 \leq j_0 \leq n - 1)$ such that $\mathrm{ord}_p(1 - \frac{\alpha_i}{m}\zeta_n^{j_0}) > 0$. In fact, if there exist $0 \leq j_1 < j_2 \leq n-1$ such that $\mathrm{ord}_p(1 - \frac{\alpha_i}{m}\zeta_n^{j_1}) > 0$ and $\mathrm{ord}_p(1 - \frac{\alpha_i}{m}\zeta_n^{j_2}) > 0$, then $\mathrm{ord}_p(\alpha_i) = 0$ and

$$\mathrm{ord}_p(1 - \zeta_n^{j_2 - j_1}) = \mathrm{ord}_p(\frac{\alpha_i}{m}\zeta_n^{j_1}(1 - \zeta_n^{j_2 - j_1})) = \mathrm{ord}_p((1 - \frac{\alpha_i}{m}\zeta_n^{j_2}) - (1 - \frac{\alpha_i}{m}\zeta_n^{j_1})) > 0.$$

This contradicts $(p, n) = 1$.

Set

$$\lambda_{n,m,p} = \sharp\{i \mid 1 \leq i \leq r, \text{ there exists an index } j \text{ such that } \mathrm{ord}_p(1 - \frac{\alpha_i}{m}\zeta_n^j) > 0\}.$$

The condition $p|\Delta_{n,m}$ implies $\lambda_{n,m,p} \geq 1$. On the other hand, we have

$$\begin{aligned} \Delta_{np^t,m} &= \prod_{i=1}^{r}(m^{np^t} - \alpha_i^{np^t}) \\ &= \prod_{i=1}^{r}\prod_{j=0}^{n-1}(m^{p^t} - \alpha_i^{p^t}\zeta_n^j) \\ &= m^{rnp^t}\prod_{i=1}^{r}\prod_{j=0}^{n-1}(1 - (\frac{\alpha_i}{m})^{p^t}\zeta_n^j) \\ &= m^{rnp^t}\prod_{i=1}^{r}\prod_{j=0}^{n-1}(1 - (\frac{\alpha_i}{m}\zeta_n^j)^{p^t}) \end{aligned} \tag{12}$$

since $(n,p) = 1$. By (2) of Lemma 3.6, there exist integers $\nu_{n,m,p}$ and $T_{n,m,p}$ such that for all $t \geq T_{n,m,p}$, we have

$$\begin{aligned} e_{n,m,p}(t) &= \mathrm{ord}_p(\Delta_{np^t,m}) \\ &= \sum_{i=1}^{r}\sum_{j=0}^{n-1}\mathrm{ord}_p(1 - (\frac{\alpha_i}{m}\zeta_n^j)^{p^t}) \\ &= \lambda_{n,m,p}t + \nu_{n,m,p}, \end{aligned}$$

where the integers $\lambda_{n,m,p}$and $\nu_{n,m,p}$ are independent of t. □

Remark 3.8 : For each $n \in \mathbb{N}$, set $f_n(x) = \prod_{i=1}^{r}(x - \alpha_i^n)$. Let p be a prime factor of $\Delta_{n,m}$. Factor $f_n(x)$ over $\mathbb{F}_p[x]$ as follows:

$$f_n(x) = p_1(x)^{e_1}p_2(x)^{e_2}\cdots p_s(x)^{e_s}$$

where $p_1(x), p_2(x), \ldots, p_s(x) \in \mathbb{F}_p[x]$ are non-associate irreducible polynomials with multiplicity $e_i \geq 1$ $(1 \leq i \leq s)$. If $e_1 = e_2 = \cdots = e_s = 1$, then $\lambda_{n,m,p} = 1$, *i.e.*, there exists a unique index i_0 such that $\mathrm{ord}_p(m^n - \alpha_{i_0}^n) > 0$. In fact, if there exist $1 \leq i < j \leq r$ such that $\mathrm{ord}_p(m^n - \alpha_i^n) > 0$ and $\mathrm{ord}_p(m^n - \alpha_j^n) > 0$, then $\mathrm{ord}_p(m) = 0$ and so

$$\mathrm{ord}_p(\alpha_i^n - \alpha_j^n) = \mathrm{ord}_p((m^n - \alpha_j^n) - (m^n - \alpha_i^n)) > 0.$$

Hence α_i^n is a root of $f_n(x)$ with multiplicity at least 2 over $\overline{\mathbb{F}_p}$ which is the algebraic closure of $\mathbb{F}_p$. This contradicts the assumptions $e_1 = e_2 = \cdots = e_s = 1$.

***Theorem* 3.9** — *Let $n \in \mathbb{N}^*$ and p, q be two different primes. Then there exists a positive integer $T_{n,m,p,q}$ such that*

$$\mathrm{ord}_q(\Delta_{np^t,m}) = \mathrm{ord}_q(\Delta_{np^{T_{n,m,p,q}},m}), \quad for \;\; all \;\; t \geq T_{n,m,p,q},$$

i.e., the numbers $\mathrm{ord}_q(\Delta_{np^t,m})$ are stable when t is sufficiently large.

PROOF : Without loss of generality, we may assume $(n,p) = 1$ and $\mathrm{ord}_q(m) = 0$. On the other hand, by (12), we have

$$\Delta_{np^t,m} = m^{rnp^t}\prod_{i=1}^{r}\prod_{j=0}^{n-1}(1 - (\frac{\alpha_i}{m}\zeta_n^j)^{p^t}).$$

For each i $(1 \leq i \leq r)$, we divide the set $\{j | 0 \leq j \leq n-1\} = S_1^{(i)} \cup S_2^{(i)}$ in such a way that for each $j \in S_1^{(i)}$, there is a $t_j^{(i)} \geq 0$ such that $\mathrm{ord}_q(1 - (\frac{\alpha_i}{m}\zeta_n^j)^{p^{t_j^{(i)}}}) > 0$, and for $j \in S_2^{(i)}$, the equality $\mathrm{ord}_q(1 - (\frac{\alpha_i}{m}\zeta_n^j)^{p^t}) = 0$ holds, for all $t \geq 0$. Set $T_{n,m,p,q} = \max_{\substack{1 \leq i \leq r \\ j \in S_1^{(i)}}} \{t_j^{(i)}\}$. Then, for all $t \geq T_{n,m,p,q}$, by Lemma 3.6, we have

$$\begin{aligned} \mathrm{ord}_q(\Delta_{np^t,m}) &= \textstyle\sum_{i=1}^r \sum_{j=0}^{n-1} \mathrm{ord}_q(1 - (\frac{\alpha_i}{m}\zeta_n^j)^{p^t}) \\ &= \textstyle\sum_{i=1}^r \sum_{j \in S_1^{(i)}} \mathrm{ord}_q(1 - (\frac{\alpha_i}{m}\zeta_n^j)^{p^{t_j^{(i)}}}). \end{aligned}$$

Since the last sum does not depend on t, the result follows. □

Corollary 3.10 — Let $S_{n,m,p}(t)$ be the set of all primes which divide $\Delta_{np^t,m}$. Then $\sharp S_{n,m,p}(t) \longrightarrow +\infty$ as $t \longrightarrow +\infty$.

PROOF : Suppose that there exists integer t_0 such that for all $t \geq t_0$, $S_{n,m,p}(t) = S_{n,m,p}(t_0)$. By Theorem 3.7 and Theorem 3.9, it would follow that $\Delta_{np^t,m}$ would be equal to a constant times $p^{\lambda_{n,m,p}t}$ for large t, *i.e.,* there exist positive constant numbers T and c such that

$$|\Delta_{np^t,m}| = cp^{\lambda_{n,m,p}t} \tag{13}$$

for all $t \geq T$. On the other hand, the assumption (H3) implies that $m \neq |\alpha_i|, \ \ 1 \leq i \leq r$. Set

$$S_1 = \{i \mid m > |\alpha_i|\}, \ \ S_2 = \{i \mid m < |\alpha_i|\}, \ \ b = \prod_{1 \leq i \leq r} \max\{|m|^n, \ |\alpha_i|^n\}.$$

If $m = 1$, then $S_2 \neq \emptyset$. Hence, for all $m \geq 1$, we have $b > 1$ and

$$\begin{aligned} \lim_{t \longrightarrow +\infty} \frac{|\Delta_{np^t,m}|}{b^{p^t}} &= \lim_{t \longrightarrow +\infty} \frac{\prod_{1 \leq i \leq r} |m^{np^t} - \alpha_i^{np^t}|}{b^{p^t}} \\ &= \lim_{t \longrightarrow +\infty} \textstyle\prod_{i \in S_1} \frac{|m^{np^t} - \alpha_i^{np^t}|}{m^{np^t}} \cdot \prod_{i \in S_2} \frac{|m^{np^t} - \alpha_i^{np^t}|}{|\alpha_i|^{np^t}} \\ &= \lim_{t \longrightarrow +\infty} \textstyle\prod_{i \in S_1} |1 - (\frac{\alpha_i}{m})^{np^t}| \cdot \prod_{i \in S_2} |1 - (\frac{m}{\alpha_i})^{np^t}| \\ &= 1. \end{aligned}$$

Therefore for sufficiently large t, we have $|\Delta_{np^t,m}| > ab^{p^t}$ for some constant $a > 0$. Clearly, this is incompatible with (13) just given. □

At last, we give the following definition.

Definition 3.11 — A sequence of integers $\{a_n\}$ is called an *Iwasawa sequence* if for any positive integer m and prime p, there exist integers $\lambda, T \in \mathbb{N}$ and $\nu \in \mathbb{Z}$ such that

$$\mathrm{ord}_p(a_{mp^t}) = \lambda t + \nu, \ \ \mathit{for} \ \ \mathit{all} \ \ t \geq T.$$

Example 3.12 : Let m be any positive integer. Then the sequence of binomial coefficients $\{C_n^m\}_{n\geq m}$ is an Iwasawa sequence. In fact, by Kummer Theorem,

$$\mathrm{ord}_p(C^m_{np^t}) = t+\nu, \quad for \ \ all \ \ t\geq T,$$

where $T=\max\{0, [\log_p m]-\mathrm{ord}_p(n)+1\}$ and $\nu=\mathrm{ord}_p(n)-\mathrm{ord}_p(m)$.

ACKNOWLEDGEMENT

We would like to thank the referee for reading the manuscript carefully and providing valuable comments and suggestions.

REFERENCES

1. Yu. F. Bilu, G. Hanrot and P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, *J. reine angew Math.*, **539** (2001), 75-122.
2. Q. Ji and H. Qin, Higher K-groups of smooth projective curves over finite fields, *Finite Fields and Their Applications*, **18** (2012), 645-660.
3. D. H. Lehmer, Factorization of certain cyclotomic funtions, *Annals of Math.*, **34**(2) (1933), 461-479.
4. T. A. Pierce, The numerical factors of the arithmetic forms $\prod_{i=1}^{n}(1\pm\alpha_i^m)$, *Annals of Math.*, **18** (1916), 53-64.
5. P. Ribenboim, *My Numbers, My Friends*, Springer-Verlag 2000.
6. M. Rosen, *Number Theory in Function Fields*, GTM 210, Springer-Verlag, New York, 2002.
7. L. C. Washington, *Introduction to cyclotomic fields (Second Edition)*, GTM 83, Springer-Verlag, New York, 1996.