A NEW CLASS OF AURIFEUILLIAN FACTORIZATION OF $M^n \pm 1$

SUN QI, REN DEBIN, HONG SHAOFANG, YUAN PINGZHI AND HAN QING

Received April 20, 1999

Abstract. In this paper, we present a class of new Aurifeuillian factorization of $M^n \pm 1$. Let positive integer $m \equiv \epsilon (\mod 4), \epsilon = 1, -1, n = mk$, where $n \equiv 1 (\mod 2), k \in Z^+$. If $M$ is a multiple of $m$ and $\frac{M}{m}$ is a square, then $\Phi_n(eM) = (\Phi_n(eM), \Delta_{1},) \Phi_n(eM), \Delta_{2}$, and $(\Phi_n(eM), \Delta_{1}) = (\Phi_n(eM), \text{Norm}_{Q(\eta_m)} / Q(\sqrt{\frac{M \pm 1}{m}}))$ and $(\Phi_n(eM), \Delta_{2}) = (\Phi_n(eM), \text{Norm}_{Q(\eta_m)} / Q(\sqrt{\frac{M + 1}{m}}))$, where $\Delta_{r} = m M^{\frac{M+1}{2m}} + (-1)^{r} \left( \frac{2}{m} \right) \sqrt{\frac{M^2}{M^2}} \frac{M^2}{M} \frac{M^2}{M}$.

1. Introduction. Let $b$ and $n$ be positive integers. It’s well known that the factorization of integers having form $b^n \pm 1$ can be reduced to the factorization of $\Phi_n(b)$, where $\Phi_n(x)$ denotes the $n$-th cyclotomic polynomial. For some integers having form $b^n \pm 1$, Aurifeuillian found out a special factorization which called Aurifeuillian factorization. Later on people also call the similar special factorization of integers having the form $b^n \pm 1$ Aurifeuillian factorization.

Let $p$ be an odd prime, $\xi = \xi_p$ denotes the $p$-th primitive root $e^{2\pi i/p}$. If $p \equiv 1 (\mod 4)$ and $N = \Phi_p(p) = (p^p - 1)/(p - 1)$, paper[2] gave two Aurifeuillian factorization of $N$:

\begin{equation}
N = \text{Norm}_{Q(\xi)/Q}(\xi - \sqrt{p}) \text{Norm}_{Q(\xi)/Q}(\xi + \sqrt{p})
\end{equation}

where $Q(\xi)$ denotes the $p$-th cyclotomic field, and

\begin{equation}
N = (N, N_1)(N, N_2)
\end{equation}

where $(N, N_1)$ denotes the great common divisor of $N$ and $N_1$, and

\begin{equation}
N_k = p^{\frac{p+1}{2}} + (-1)^{k} \left( \frac{2}{p} \right) \sum_{t=1}^{p-1} (-1)^{t} p^{t}, k = 1, 2.
\end{equation}

The author of paper[2] asked are (1.1) and (1.2) the same factorization of $N$? Paper[3] answered the question affirmatively, moreover, it showed the similar result is true for $p \equiv 3 (\mod 4)$ and $N = \Phi_p(-p)$. It’s naturally to ask does the similar result hold for $q = p^n$, where $p$ is an odd prime and $n$ is a positive integer? Paper[4] completely solved the above question. It proved the following result.

Theorem[4] Let $p \equiv \epsilon (\mod 4), \epsilon = 1, -1, q = p^n, n$ is a positive integer, $\eta = e^{2\pi i/p}$. Let $R_{c} = \Phi_{c}(eq)$, then

\begin{equation}
R_{c} = \text{Norm}_{Q(\eta)/Q}(\eta - \sqrt{eq}) \text{Norm}_{Q(\eta)/Q}(\eta + \sqrt{eq})
\end{equation}

Key words and phrases. Aurifeuillian factorization, Cyclotomic field.
and if $n$ is odd, then

$$(1.4) \quad R_e = (R_e, R_{e,1})(R_e, R_{e,2})$$

where

$$R_{e,k} = q^{ \frac{\varepsilon+1}{p} } + (-1)^k \left( \frac{2}{p} \right) \sum_{\substack{t=1 \atop (p,t)=1}}^{p-1} \left( \frac{t}{p} \right) (eq/t/p)^{k}, k = 1, 2.$$ 

if $n$ is even, then

$$(1.5) \quad R_e = (R_e, R_{e,1}')(R_e, R_{e,2}')$$

where

$$R_{e,k} = q^{ \frac{\varepsilon+1}{p} } + (-1)^k \left( \frac{p}{p} \right) \sum_{\substack{t=1 \atop (p,t)=1}}^{p-1} \left( \frac{t}{p} \right) (eq/t/p)^{k}, k = 1, 2.$$ 

Furthermore, if $n$ is odd then $(1.3)$ and $(1.4)$ are the same factorization of $R_e$; if $n$ is even then $(1.3)$ and $(1.5)$ are the same factorization of $R_e$.

People naturally hope we have the similar result for any odd. In this paper we get more generous result than the hope. Let $m \equiv 1 \pmod 4, e = 1, -1, n = km, n \equiv 1 \pmod 2, k \in \mathbb{Z}^+$. Positive integer $M$ is a multiple of $m$, and $\frac{M}{m}$ is a square. We obtain two factorizations of $\Phi_n(M)$ in different ways, which are the same one. This result largely improves the previous works. Finally, in order to test the effectiveness of the result, we give an example about the factorization of a very large cyclotomic number.

2. the Aurifeuillian factorization of $M^m \pm 1 (n \equiv 1 \pmod 2)$.

**Lemma 2.1**[5] The Gauss sum

$$\sum_{\substack{m \equiv \eta^m \equiv 1 \pmod m \leq 1 \leq k \leq m}} (\frac{a}{m}) \eta_m = \begin{cases} \sqrt{m} & \text{if } m \equiv 1 \pmod 4 \\ \sqrt{-m} & \text{if } m \equiv 3 \pmod 4 \end{cases}$$

where $\eta_m = e^{2 \pi im/m}$.

**Lemma 2.2** Let $k \in \mathbb{Z}^+, 1 \leq k \leq m$, then

$$\text{Norm}_{Q(\eta_m)/Q}(1 - \eta_m^{2k}) = (\Phi_{\frac{m}{\gcd(m,k)}}(1))^{(k,m)}$$

**Proof.** Let $k_1 = \frac{k}{\gcd(k,m)}, m_1 = \frac{m}{\gcd(m,k)}$, then $(k_1, m_1) = 1$. By the definition of Norm we have

$$\text{Norm}_{Q(\eta_m)/Q}(1 - \eta_m^{2k}) = \prod_{\substack{m_1 \equiv \eta_{m_1} \equiv 1 \pmod{m_1} \leq 1 \leq k \leq m_1}} (1 - \eta_{m_1}^{2ka}) = \prod_{\substack{m_1 \equiv \eta_{m_1} \equiv 1 \pmod{m_1} \leq 1 \leq k \leq m_1}} (1 - \eta_{m_1}^a) = \prod_{\substack{m_1 \equiv \eta_{m_1} \equiv 1 \pmod{m_1} \leq 1 \leq k \leq m_1}} (1 - \eta_{m_1}^{a})^{(k,m)} = (\Phi_{m_1}(1))^{(k,m)}.$$ 

**Lemma 2.3** Let positive integer $m \equiv e \pmod 4, e = 1, -1, M$ be a positive integer , and $mM$ be a square. Let $\text{Gal}(Q(\eta_m)/Q) = \{\sigma_i | \sigma : \eta_m \mapsto \eta_m^i, 1 \leq i \leq m, (i, m) = 1\}$, then for
any $\sigma_i \in \text{Gal}(Q(q_m)/Q)$ we have $\sigma_i(\sqrt{eM}) = (\frac{i}{m})\sqrt{eM}$ if $i, m = 1$.

**Proof.** By lemma 2.1

$$\sum_{(c, m) = 1}^{m} \left(\frac{c}{m}\right)\eta_m^c = \sqrt{eM}.$$ 

Therefore

$$(2.1) \quad \sigma_i(\sqrt{eM}) = \sum_{(c, m) = 1}^{m} \left(\frac{c}{m}\right)\eta_m^c = (\frac{i}{m})\sqrt{eM}$$

And since $MM$ is a square we can let $MM = a^2, a \in Z$. Then $M = (\frac{a^2}{m})^2m$. By (2.1) we have

$$\sigma_i(\sqrt{eM}) = \frac{a}{m}\sigma_i(\sqrt{eM}) = (\frac{i}{m})\sqrt{eM}.$$ 

**Lemma 2.4** Let $n = mk$, where $n \equiv 1(\text{mod}2), m, k \in Z$. Then

$$\Phi_n(x^2) = (\Phi_n(x^2), \prod_{i=1}^{m} (x^k - \eta_m^i), \prod_{i=1}^{m} (x^k + \eta_m^i)) \cdot (\Phi_n(x^2), \prod_{i=1}^{m} (x^k - \eta_m^i), \prod_{i=1}^{m} (x^k + \eta_m^i))$$

**Proof.** Let $A = \prod_{i=1}^{n} (x - \eta_n^i), B = \prod_{i=1}^{n} (x - \eta_n^i), B = \prod_{i=1}^{n} (x - \eta_n^i), B = \prod_{i=1}^{n} (x + \eta_n^i)$. Since

$$2 \mid n$$

we have by the definition of cyclotomic polynomial

$$\Phi_n(x^2) = \prod_{i=1}^{n} (x^2 - \eta_n^i) = \prod_{i=1}^{n} (x^2 - \eta_n^2)$$

$$(2.3) \quad = \prod_{i=1}^{n} (x - \eta_n^i) \prod_{i=1}^{n} (x + \eta_n^i) = AB$$

Hence

$$A = (\Phi_n(x^2), \prod_{i=1}^{n} (x - \eta_n^i), \prod_{i=1}^{n} (x + \eta_n^i))$$

$$B = (\Phi_n(x^2), \prod_{i=1}^{n} (x - \eta_n^i), \prod_{i=1}^{n} (x + \eta_n^i))$$
Now we suppose $s = s' + um$, where $1 \leq s' \leq m$, $0 \leq u \leq k - 1$, so we have

$$
\prod_{(i, \frac{n}{m}) = e}^{n} (x \pm \eta_m^s) = \prod_{(i', \frac{n}{m}) = e}^{m} \prod_{u=0}^{k-1} (x \pm \eta_m^{s'+um})
$$

$$
= \prod_{(i', \frac{n}{m}) = e}^{m} \prod_{u=0}^{k-1} (x \pm \eta_m^{s'} \eta_m^u)
$$

$$
= \prod_{(i', \frac{n}{m}) = e}^{m} (x^k \pm \eta_m^{s'k})
$$

$$
= \prod_{(i', \frac{n}{m}) = e}^{m} (x^k \pm \eta_m^s)
$$

where $e = 1, -1$.

Thus

$$
A = (\Phi_n(x^2), \prod_{(i', \frac{n}{m}) = 1}^{m} (x^k - \eta_m^s) \prod_{(i', \frac{n}{m}) = -1}^{m} (x^k + \eta_m^s))
$$

(2.4)

$$
B = (\Phi_n(x^2), \prod_{(i, \frac{n}{m}) = -1}^{m} (x^k - \eta_m^s) \prod_{(i, \frac{n}{m}) = 1}^{m} (x^k + \eta_m^s))
$$

(2.5)

So we obtain (2.2) from (2.3), (2.4) and (2.5).

**Theorem 2.1** Let $n = mk$, where $n \equiv 1 \pmod{2}, m \equiv \epsilon \equiv 1, -1, k \in Z$. If $M$ is a multiple of $m$ and \( \frac{M}{m} \) is a square, then we have

$$
\Phi_n(\epsilon M) = (\Phi_n(\epsilon M), \text{Norm}_{Q(\eta_m)/Q}(\sqrt{\epsilon M}^k - \eta_m))(\Phi_n(\epsilon M), \text{Norm}_{Q(\eta_m)/Q}(\sqrt{\epsilon M}^k + \eta_m))
$$

(2.6)

**Proof.** Because $m|M$ and $\frac{M}{m}$ is a square, we can let $\sqrt{\frac{M}{m}} = a^2, a \in Z$, and $\sqrt{\epsilon M} = a\sqrt{\frac{M}{m}} \in Z[\eta_m]$ since $\sqrt{\frac{M}{m}} \in Z[\eta_m]$. Let $\text{Gal}(Q(\eta_m)/Q) = \{\sigma_i \} \sigma_i : \eta_m \mapsto \eta_m^i, (i, m) = 1, 1 \leq i \leq m$. Since $2 \mid n$, for $(i, m) = 1, 1 \leq i \leq m$ we have by lemma 2.3

$$
\sigma_i(\sqrt{\epsilon M}^k - \eta_m) = ((\frac{i}{m})\sqrt{\epsilon M})^k - \eta_m^i = (\frac{i}{m})\sqrt{\epsilon M}^k - \eta_m^i
$$
Hence
\[
\text{Norm}_{Q(\eta_m)/Q}(\sqrt{eM^k} - \eta_m) = \prod_{\substack{i=1 \\
(i,m)=1}}^{m} \sigma(\sqrt{eM^k} - \eta_m) \\
= \prod_{\substack{i=1 \\
(i,m)=1}}^{m} ((\frac{i}{m})\sqrt{eM^k} - \eta_m) \\
= \prod_{\substack{i=1 \\
(i,m)=1}}^{m} (\sqrt{eM^k} - \eta_m^i) \prod_{\substack{i=1 \\
(i,m)=1}}^{m} (-\sqrt{eM^k} - \eta_m^i) \\
= \left( \Phi_n(eM), \text{Norm}_{Q(\eta_m)/Q}(\sqrt{eM^k} - \eta_m) \right) \\
\left( \Phi_n(eM), \prod_{\substack{i=1 \\
(i,m)=1}}^{m} (\sqrt{eM^k} - \eta_m^i), \prod_{\substack{i=1 \\
(i,m)=1}}^{m} (\sqrt{eM^k} + \eta_m^i) \right) \\
\text{In the same way we have} \\
\left( \Phi_n(eM), \text{Norm}_{Q(\eta_m)/Q}(\sqrt{eM^k} + \eta_m) \right) = \\
\left( \Phi_n(eM), \prod_{\substack{i=1 \\
(i,m)=1}}^{m} (\sqrt{eM^k} - \eta_m^i), \prod_{\substack{i=1 \\
(i,m)=1}}^{m} (\sqrt{eM^k} + \eta_m^i) \right) \\
\text{In lemma 2.4 we replace } x \text{ by } \sqrt{eM} \text{ then we get (2.6). We complete our proof.} \\
\text{Lemma 2.5 Let } m|\text{ and } k \in \mathbb{Z}^+ \text{. Then } (\Phi_m(M^k), m) = 1. \\
\text{Proof. Since } \Phi_m(M^k)|(\{M^k\})^m - 1)/(M^k - 1), \text{ so } (\Phi_n(M^k), M) = 1. \text{ And } m|\text{, so } (\Phi_m(M^k), m) = 1. \\
\text{Lemma 2.6 Let positive integer } m \equiv e(\text{mod}4), e = 1, -1, n = mk, \text{ where } n \equiv 1(\text{mod}2), k \in \mathbb{Z}^+. \text{ If } M \text{ is a multiple of } m \text{ and } \frac{M}{m} \text{ is a square. Let} \\
\Delta_{r,1} = mM^{\frac{2r}{m}} + (-1)^{r+1}(\frac{2}{m})\sqrt{mM^k} \sum_{\substack{c=1 \\
(c,m)=1}}^{m} (\frac{c}{m})(eM)^{kc} - \eta_m^1 \\
\Delta_{r,2} = mM^{\frac{2r}{m}} + (-1)^{r}(\frac{2}{m})\sqrt{mM^k} \sum_{\substack{c=1 \\
(c,m)=1}}^{m} (\frac{c}{m})(eM)^{kc} - \eta_m^1 \\
\text{Then} \\
\text{Norm}_{Q(\eta)/Q}(\sqrt{eM^k} - \eta_m) \mid \Delta_{r,1} \\
\text{Norm}_{Q(\eta)/Q}(\sqrt{eM^k} + \eta_m) \mid \Delta_{r,2} \\
\text{Proof. Suppose } e = 1. \text{ For } 1 \leq i \leq m, (i, m) = 1, \text{ by Lemma 2.1 we have} \\
\sum_{\substack{c=1 \\
(c,m)=1}}^{m} (\frac{c}{m})M^{kc} = \sum_{\substack{c=1 \\
(c,m)=1}}^{m} (\frac{c}{m})\eta_m^{2ci} = (\frac{2i}{m}) \sum_{\substack{c=1 \\
(c,m)=1}}^{m} (\frac{2i}{m})\eta_m^{2ci} = (\frac{2i}{m}) \sqrt{m(\text{mod} M^k - \eta_m^i)} \\
\text{Hence if } (\frac{1}{m}) = 1 \\
\Delta_{1,1} = m\eta_m^{(m+1)} - (\frac{2}{m})\sqrt{mM^{\frac{2r}{m}}} + (\frac{2i}{m})\sqrt{m} \equiv m\eta_m^i - m(M^k + \eta_m^i) \equiv 0(\text{mod} M^k + \eta_m^i)
In the same way $\Delta_{c,1} \equiv 0 (\text{mod } M^\frac{1}{2} \pm \eta_m^a)$ if $(\frac{m}{M}) = -1$. So for $1 \leq a \leq m, (a, m) = 1$ we have
\[ (2.10) \quad \sigma_a(\sqrt{M^b} - \eta_m)\sigma_a(\Delta_{c,1}) = \Delta_{c,1} \]

On the other hand we have by lemma 2.3 (be aware that $mM$ is a square since $M/m$ is a square)
\[ \sigma_a(\sqrt{M^b} - \eta_m) = \sigma_a(\sqrt{M^b} - \eta_m^a) = (\frac{a}{m})\sqrt{M^b} - \eta_m^a \]

Therefore for any $b \neq a, 1 \leq b \leq m, (b, m) = 1$, we have
\[ (\sigma_a(\sqrt{M^b} - \eta_m), \sigma_b(\sqrt{M^b} - \eta_m)) = ((\frac{a}{m})\sqrt{M^b} - \eta_m^a, (\frac{b}{m})\sqrt{M^b} - \eta_m^b)[(M^k - \eta_m^{2a}, M^k - \eta_m^{2b})]\text{Norm}_Q(\eta_m)/(1 - i_m^{2(b-a)}) \]

Let $m_1 = m/(b-a, m)$. By lemma 2.2 we have
\[ (\sigma_a(\sqrt{M^b} - \eta_m), \sigma_b(\sqrt{M^b} - \eta_m))(\Phi_{m_1}(1))^{(b-a,m)} \]

And
\[ \Phi_{m_1}(1) = \prod_{(i,m_1) = 1} m_1 \prod_{i=1}^{m_1} (1 - \eta_m) = m_1/m \]

Hence
\[ (2.11) \quad (\sigma_a(\sqrt{M^b} - \eta_m), \sigma_b(\sqrt{M^b} - \eta_m)) m^{(b-a,m)} \]

On the other hand we have
\[ (\sigma_a(\sqrt{M^b} - \eta_m), \sigma_b(\sqrt{M^b} - \eta_m))[(M^k - \eta_m^{2a}, M^k - \eta_m^{2b})] \]
\[ \prod_{(i,m) = 1} m \prod_{(i,m) = 1} (M^k - \eta_m^i) = \prod_{(i,m) = 1} (M^k - \eta_m^i) \]

namely
\[ (2.12) \quad (\sigma_a(\sqrt{M^b} - \eta_m), \sigma_b(\sqrt{M^b} - \eta_m)) |\Phi_m(M^k) \]

By (2.11), (2.12) and lemma 2.5 we have
\[ (2.13) \quad (\sigma_a(\sqrt{M^b} - \eta_m), \sigma_b(\sqrt{M^b} - \eta_m)) = 1 \]

So when $\epsilon = 1$ we have proved (2.8) by (2.10) and (2.13). In the same way we can prove (2.8) when $\epsilon = -1$. So we complete the proof of (2.8). Clearly, we can prove (2.9) similarly. Hence the proof is complete.

**Lemma 2.7** Let $n = mk$, where $m \equiv \epsilon (\text{mod} 4), \epsilon = 1, -1, n \equiv 1 (\text{mod} 2)$. If $m|M$ then $(\Phi_n(\epsilon M), \Delta_{c,1}, \Delta_{c,2}) = 1$.

**Proof.** Since $(\Delta_{c,1}, \Delta_{c,2}) |2mM^{k-\frac{a+b}{2}}$ and $\Phi_n(\epsilon M) = \prod_{(i,m) = 1} \prod_{(i,n) = 1}^{n-1} (\epsilon M - \eta_m^i) = (\frac{\epsilon M^{n-1}}{M^{n-1}})$, we have $(\Phi_n(\epsilon M), M) = 1$. Because $m|M$ then $(\Phi_n(\epsilon M), mM^{k-\frac{a+b}{2}}) = 1$. But 2 $|m$ which follows $2 |(\frac{\epsilon M^{n-1}}{M^{n-1}})$, then 2 $|$ $\Phi_n(\epsilon M)$. Hence $(\Phi_n(\epsilon M), 2mM^{k-\frac{a+b}{2}}) = 1$ which follows $(\Phi_n(\epsilon M), \Delta_{c,1}, \Delta_{c,2}) = 1$. 


THEOREM 2.2 Let positive integer $m \equiv \epsilon (\text{mod} 4), \epsilon = 1, -1, n = mk$, where $n \equiv 1 (\text{mod} 2), k \in \mathbb{Z}^+$. If $M$ is a multiple of $m$ and $\frac{M}{m}$ is a square, then $\Phi_n(\epsilon M) = (\Phi_n(\epsilon M), \Delta_{1,1})$, and $(\Phi_n(\epsilon M), \Delta_{1,1}) = (\Phi_n(\epsilon M), \text{Norm}_{Q(\eta_m)}/O(\epsilon\sqrt{M'}, \eta_m))$ and $(\Phi_n(\epsilon M), \Delta_{1,2}) = (\Phi_n(\epsilon M), \text{Norm}_{Q(\eta_m)}/O(\epsilon\sqrt{M'} + \eta_m))$.

PROOF. When $\epsilon = 1$, by Lemma 2.6 we have

$$(\Phi_n(\epsilon M), \text{Norm}_{Q(\eta_m)}/O(\epsilon\sqrt{M'} - \eta_m)) = \Phi_n(\epsilon M)$$

and

$$(\Phi_n(\epsilon M), \text{Norm}_{Q(\eta_m)}/O(\epsilon\sqrt{M'} + \eta_m)) = \Phi_n(\epsilon M)$$

So by Theorem 2.1 we have

$$(\Phi_n(\epsilon M), \Delta_{1,1}) = \Phi_n(\epsilon M), \Delta_{1,2})$$

On the other hand

$$(\Phi_n(\epsilon M), \Delta_{1,1}) | \Phi_n(\epsilon M), \Delta_{1,2})$$

then by Lemma 2.7

$$(\Phi_n(\epsilon M), \Delta_{1,1}) | \Phi_n(\epsilon M), \Delta_{1,2})$$

So we compute the proof of the theorem when $\epsilon = 1$. In the same way we can prove the theorem when $\epsilon = -1$. So the whole proof is complete.

EXAMPLE. Let $n = 253, m = 11, M = 44$, then $k = 23$. Clearly, the conditions of theorem 2.2 are satisfied, so we can compute

$$\Phi_{253}(-44) = 370978434545082518631525235934239362562620975970338072$$

$$+ 46964591185907899249977780116522088181645680182845039$$

$$393252706436580824852289157279680968578993203497375$$

$$93195841402705471120561689405156827477559406002819048$$

$$94424232005472001320662317966652573523661165656368874$$

$$1291749406145155731900544616973072632762854569235$$

$$095147223301209308866681148725680412400301$$

$$\Delta_{1,1} = -44^{\text{odd}} \cdot 3444504158952726218552600547691950130668205232$$

$$+ 9785749265017017546544158158000372552576109635273373$$

$$7029417917784867178245207358833162492035349517131078$$

$$3468651592823577105161580969105598836912332516749252$$

$$951883197071217365552918037150406969859384167108087$$

$$2730857268933094363252515886499722426954448015777548$$

$$1725833482644138420481800214$$

$$\Delta_{1,2} = 44^{\text{odd}} \cdot 34445041589527262185526005476919501306682052327$$

$$+ 8574926501701754654415815800037255257610963527133770$$

$$2941791778486717824520735883316249203534951713107834$$

$$6851392823577123376169120637350008677859528459871092$$

$$3262303494353633587585021566742380900570469161991937$$

$$+ 30866062009066410737679999355999676929437690473997736$$
\[ \Phi_{253}(-44), \Delta_{-1,1} = \begin{array}{c} 70825189495602751164911714326 \\ 37080821140512849310145272753829369629490500199005485 \\ 04948003025339948192457694962513241254988377338102340 \\ 86264863096527642067848057690638982948383373587326170 \\ 051260262214314699971 \\
\end{array} \]

\[ \Phi_{253}(-44), \Delta_{-1,2} = \begin{array}{c} 10004590597907985573943582945748620748239251502916976 \\ 189782398776822784239871239690841966240006301089795 \\ 14915269438067251701400814361228222136145387771492736 \\ 1019333917217066917231 \\
\end{array} \]

\[ \Phi_{253}(-44) = \begin{array}{c} 37080821140512849310145272753829369629490500199005485 \\ 04948003025339948192457694962513241254988377338102340 \\ 86264863096527642067848057690638982948383373587326170 \\ 051260262214314699971 \cdot 10004590597907985573943582945748620748239251502916976 \\ 7486207482392515029169760189782398776822784239871239690841966240006301089795 \\ 69084196624000630108987951491526943806725170140081436 \\ 12228221361453877714927361019333917217066917231 \\
\end{array} \]

References
4. Sun Qi, Hong Shaofang, Aurifeullian Factorizations of $Q^n \pm 1(q = p^n)$. Advances in Math. (China), vol.26, No.1, 1997, 74-75.
5. Hua Luogeng, the Introduction To Number Theorem, Academic Press of Science.

Department of Mathematics, Sichuan University, Chengdu, Sichuan 610064, P. R. China