A NEW CLASS OF AURIFEUILLIAN FACTORIZATIONS 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 $M^n \pm 1$,e.i.: Let positive integer $m \equiv \epsilon(\text{mod}4), \epsilon = 1, -1, n = mk$, where $n \equiv 1(\text{mod}2), k \in Z^+$. If M is a multiple of m and $\frac{M}{m}$ is a square, then $\Phi_n(\epsilon M) = (\Phi_n(\epsilon M), \Delta_{\epsilon,1})(\Phi_n(\epsilon M), \Delta_{\epsilon,2})$, and $(\Phi_n(\epsilon M), \Delta_{\epsilon,1}) = (\Phi_n(\epsilon M), \text{Norm}_{Q(\eta_m)/Q}(\sqrt{\epsilon M}^k - \eta_m))$ and $(\Phi_n(\epsilon M), \Delta_{\epsilon,2}) = (\Phi_n(M), \text{Norm}_{Q(\eta_m)/Q}(\sqrt{\epsilon M}^k + \eta_m))$, where $\Delta_{\epsilon,r} = mM^{k\frac{m+1}{2}} + (-1)^r(\frac{2}{m})\sqrt{mM}M^{\frac{k-1}{2}} \sum_{\substack{c=1\\(c,m)=1}}^{m} (\frac{c}{m})(\epsilon M)^{kc}$ $r = 1, 2$. Finally we give an example about the Aurifeuillian factorization of a very large cyclotomic number with 362 digits.

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 $p \equiv 1(\text{mod}4)$ and $N = \Phi_p(p) = (p^p - 1)/(p - 1)$, paper[2] gived two Aurifeuillian factorization of N:

$$N = \text{Norm}_{Q(\xi)/Q}(\xi - \sqrt{p})\text{Norm}_{Q(\xi)/Q}(\xi + \sqrt{p}) \tag{1.1}$$

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

$$N = (N, N_1)(N, N_2) \tag{1.2}$$

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

$$N_k = p^{\frac{p+1}{2}} + (-1)^k(\frac{2}{p})\sum_{t=1}^{p-1}(\frac{t}{p})p^t, k = 1, 2.$$

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 $p \equiv 3(\text{mod}4)$ 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 $p \equiv \epsilon(\text{mod}4), \epsilon = 1, -1, q = p^n, n$ is a positive integer, $\eta = e^{\frac{2\pi i}{q}}$. Let $R_\epsilon = \Phi_q(\epsilon q)$, then*

$$R_\epsilon = \text{Norm}_{Q(\eta)/Q}(\eta - \sqrt{\epsilon q})\text{Norm}_{Q(\eta)/Q}(\eta + \sqrt{\epsilon q}) \tag{1.3}$$

Key words and phrases. Aurifeuillian factorization, Cyclotomic field.

and if n is odd, then

$$R_\epsilon = (R_\epsilon, R_{\epsilon,1})(R_\epsilon, R_{\epsilon,2}) \tag{1.4}$$

where

$$R_{\epsilon,k} = q^{\frac{q+1}{2}} + (-1)^k (\frac{2}{p}) \sum_{\substack{t=1 \\ (p,t)=1}}^{p^{\frac{n+1}{2}}} (\frac{t}{p})(\epsilon q^{q/p})^t, k = 1, 2.$$

if n is even, then

$$R_\epsilon = (R_\epsilon, R'_{\epsilon,1})(R_\epsilon, R'_{\epsilon,2}) \tag{1.5}$$

where

$$R'_{\epsilon,k} = q^{\frac{q+1}{2}} + (-1)^k p^{\frac{n-2}{2}} (\sum_{t=1}^{p-1} (\frac{t}{p})(\epsilon q^{q/p})^t)^2, k = 1, 2.$$

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

People naturally hope we have the similar result for any odd. In this paper we get more generous result than the hope. Let $m \equiv \epsilon (\mathrm{mod} 4), \epsilon = 1, -1, n = km, n \equiv 1(\mathrm{mod} 2), k \in Z^+$. Positive integer M is a multiple of m, and $\frac{M}{m}$ is a square. We obtain two factorizations of $\Phi_n(\epsilon M)$ in different way, 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 $M^n \pm 1 (n \equiv 1(\mathrm{mod} 2))$.

Lemma 2.1[5] *The Gauss sum*

$$\sum_{\substack{a=1 \\ (a,m)=1}}^{m} (\frac{a}{m}) \eta_m^a = \{ \begin{array}{ll} \sqrt{m} & if\ m \equiv 1(\mathrm{mod} 4) \\ \sqrt{-m} & if\ m \equiv 3(\mathrm{mod} 4) \end{array}$$

where $\eta_m = e^{\frac{2\pi i}{m}}$.

Lemma 2.2 *Let $k \in Z^+, 1 \le k \le m$, then*

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

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

$$\mathrm{Norm}_{Q(\eta_m)/Q}(1 - \eta_m^{2k}) = \prod_{\substack{a=1 \\ (a,m)=1}}^{m} (1 - \eta_m^{2ka}) = \prod_{\substack{a=1 \\ (a,m)=1}}^{m} (1 - \eta_{m_1}^{k_1 a}) =$$

$$(\prod_{\substack{a=1 \\ (a,m_1)=1}}^{m_1} (1 - \eta_{m_1}^{k_1 a}))^{(k,m)} = (\prod_{\substack{a=1 \\ (a,m_1)=1}}^{m_1} (1 - \eta_{m_1}^{a}))^{(k,m)} = (\Phi_{m_1}(1))^{(k,m)}.$$

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

PROOF. By lemma 2.1

$$\sum_{\substack{c=1 \\ (c,m)=1}}^{m} (\frac{c}{m})\eta_m^c = \sqrt{\epsilon m}.$$

Therefore

$$\sigma_i(\sqrt{\epsilon m}) = \sum_{\substack{c=1 \\ (c,m)=1}}^{m} (\frac{c}{m})\eta_m^{ic} = (\frac{i}{m})\sqrt{\epsilon m} \tag{2.1}$$

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

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

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

(2.2)

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

PROOF. Let $A = \prod_{\substack{s=1 \\ (s,n)=1 \\ (\frac{s}{m})=1}}^{n} (x-\eta_n^s) \prod_{\substack{t=1 \\ (t,n)=1 \\ (\frac{t}{m})=-1}}^{n} (x+\eta_n^t), B = \prod_{\substack{s=1 \\ (s,n)=1 \\ (\frac{s}{m})=-1}}^{n} (x-\eta_n^s) \prod_{\substack{t=1 \\ (t,n)=1 \\ (\frac{t}{m})=1}}^{n} (x+\eta_n^t)$. Since $2 \nmid n$ we have by the definition of cyclotomic polynomial

$$\begin{aligned} \Phi_n(x^2) &= \prod_{\substack{s=1 \\ (s,n)=1}}^{n} (x^2 - \eta_n^s) = \prod_{\substack{s=1 \\ (s,n)=1}}^{n} (x^2 - \eta_n^{2s}) \\ &= \prod_{\substack{s=1 \\ (s,n)=1}}^{n} (x - \eta_n^s) \prod_{\substack{s=1 \\ (s,n)=1}}^{n} (x + \eta_n^s) = AB \end{aligned} \tag{2.3}$$

Hence

$$A = (\Phi_n(x^2), \prod_{\substack{s=1 \\ (\frac{s}{m})=1}}^{n} (x - \eta_n^s) \prod_{\substack{s=1 \\ (\frac{s}{m})=-1}}^{n} (x + \eta_n^s))$$

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

Now we suppose $s = s' + um$, where $1 \le s' \le m, 0 \le u \le k-1$, so we have

$$\begin{aligned}\prod_{\substack{s=1\\(\frac{s}{m})=\epsilon}}^{n} (x \pm \eta_n^s) &= \prod_{\substack{s'=1\\(\frac{s'}{m})=\epsilon}}^{m} \prod_{u=0}^{k-1} (x \pm \eta_n^{s'+um}) \\ &= \prod_{\substack{s'=1\\(\frac{s'}{m})=\epsilon}}^{m} \prod_{u=0}^{k-1} (x \pm \eta_n^{s'} \eta_k^u) \\ &= \prod_{\substack{s'=1\\(\frac{s'}{m})=\epsilon}}^{m} (x^k \pm \eta_n^{s'k}) \\ &= \prod_{\substack{s=1\\(\frac{s}{m})=\epsilon}}^{m} (x^k \pm \eta_m^s)\end{aligned}$$

where $\epsilon = 1, -1$.
Thus

$$A = (\Phi_n(x^2), \prod_{\substack{s=1\\(\frac{s}{m})=1}}^{m} (x^k - \eta_m^s) \prod_{\substack{t=1\\(\frac{t}{m})=-1}}^{m} (x^k + \eta_m^t)) \tag{2.4}$$

$$B = (\Phi_n(x^2), \prod_{\substack{s=1\\(\frac{s}{m})=-1}}^{m} (x^k - \eta_m^s) \prod_{\substack{t=1\\(\frac{t}{m})=1}}^{m} (x^k + \eta_m^t)) \tag{2.5}$$

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

THEOREM 2.1 *Let $n = mk$, where $n \equiv 1(\text{mod}2), m \equiv \epsilon(\text{mod}4), \epsilon = 1, -1, k \in Z$. If M is a multiple of m and $\frac{M}{m}$ is a square, then we have*

(2.6)
$$\Phi_n(\epsilon M) = (\Phi_n(\epsilon M), \text{Norm}_{Q(\eta_m)/Q}(\sqrt{\epsilon M}^k - \eta_m))(\Phi_n(\epsilon M), \text{Norm}_{Q(\eta_m)/Q}(\sqrt{\epsilon M}^k + \eta_m))$$

PROOF. Because $m|M$ and $\frac{M}{m}$ is a square, we can let $\frac{M}{m} = a^2, a \in Z$, and $\sqrt{\epsilon M} = a\sqrt{\epsilon m} \in Z[\eta_m]$ since $\sqrt{\epsilon m} \in Z[\eta_m]$. Let $\text{Gal}(Q(\eta_m)/Q) = \{\sigma_i | \sigma_i : \eta_m \mapsto \eta_m^i, (i,m) = 1, 1 \le i \le m\}$. Since $2 \not| n$, for $(i,m) = 1, 1 \le i \le m$ 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

$$\begin{aligned}\mathrm{Norm}_{Q(\eta_m)/Q}(\sqrt{\epsilon M}^k - \eta_m) &= \prod_{\substack{i=1\\(i,m)=1}}^{m} \sigma(\sqrt{\epsilon M}^k - \eta_m)\\ &= \prod_{\substack{i=1\\(i,m)=1}}^{m} ((\frac{i}{m})\sqrt{\epsilon M}^k - \eta_m^i)\\ &= \prod_{\substack{s=1\\(\frac{s}{m})=1}}^{m} (\sqrt{\epsilon M}^k - \eta_m^s) \prod_{\substack{t=1\\(\frac{t}{m})=-1}}^{m} (-\sqrt{\epsilon M}^k - \eta_m^t)\end{aligned}$$

$$(\Phi_n(\epsilon M), \mathrm{Norm}_{Q(\eta_m)/Q}(\sqrt{\epsilon M}^k - \eta_m)) =$$
$$(\Phi_n(\epsilon M), \prod_{\substack{s=1\\(\frac{s}{m})=1}}^{m} (\sqrt{\epsilon M}^k - \eta_m^s) \prod_{\substack{t=1\\(\frac{t}{m})=-1}}^{m} (\sqrt{\epsilon M}^k + \eta_m^t))$$

In the same way we have

$$(\Phi_n(\epsilon M), \mathrm{Norm}_{Q(\eta_m)/Q}(\sqrt{\epsilon M}^k + \eta_m)) =$$
$$(\Phi_n(\epsilon M), \prod_{\substack{s=1\\(\frac{s}{m})=-1}}^{m} (\sqrt{\epsilon M}^k - \eta_m^s) \prod_{\substack{t=1\\(\frac{t}{m})=1}}^{m} (\sqrt{\epsilon M}^k + \eta_m^t))$$

In lemma 2.4 we replace x by $\sqrt{\epsilon M}$ then we get (2.6). We complete our proof.

LEMMA 2.5 *Let $m|M, k \in Z^+$. Then $(\Phi_m(M^k), m) = 1$.*
PROOF. Since $\Phi_m(M^k)|((M^k)^m - 1)/(M^k - 1)$, so $(\Phi_n(M^k), M) = 1$. And $m|M$, so $(\Phi_m(M^k), m) = 1$.

LEMMA 2.6 *Let positive integer $m \equiv \epsilon(\mathrm{mod} 4), \epsilon = 1, -1, n = mk$, where $n \equiv 1(\mathrm{mod} 2), k \in Z^+$. If M is a multiple of m and $\frac{M}{m}$ is a square. Let*

$$\Delta_{\epsilon,r} = mM^{k\frac{m+1}{2}} + (-1)^r(\frac{2}{m})\sqrt{mM}M^{\frac{k-1}{2}} \sum_{\substack{c=1\\(c,m)=1}}^{m} (\frac{c}{m})(\epsilon M)^{kc} \quad r = 1, 2. \tag{2.7}$$

Then

$$\mathrm{Norm}_{Q(\eta)/Q}(\sqrt{\epsilon M}^k - \eta_m)|\Delta_{\epsilon,1} \tag{2.8}$$

$$\mathrm{Norm}_{Q(\eta)/Q}(\sqrt{\epsilon M}^k + \eta_m)|\Delta_{\epsilon,2} \tag{2.9}$$

PROOF. Suppose $\epsilon = 1$. For $1 \le i \le m, (i, m) = 1$, by Lemma 2.1 we have

$$\sum_{\substack{c=1\\(c,m)=1}}^{m} (\frac{c}{m})M^{kc} \equiv \sum_{\substack{c=1\\(c,m)=1}}^{m} (\frac{c}{m})\eta_m^{2ci} \equiv (\frac{2i}{m}) \sum_{\substack{c=1\\(c,m)=1}}^{m} (\frac{2ci}{m})\eta_m^{2ci} \equiv (\frac{2i}{m})\sqrt{m}(\mathrm{mod}\ \ M^{\frac{k}{2}} - \eta_m^i)$$

Hence if $(\frac{i}{m}) = 1$

$$\Delta_{\epsilon,1} \equiv m\eta_m^{i(m+1)} - (\frac{2}{m})\sqrt{mM}M^{\frac{k-1}{2}}(\frac{2i}{m})\sqrt{m} \equiv m\eta_m^i - mM^{(\frac{k}{2})} \equiv 0(\mathrm{mod}\ \ M^{\frac{k}{2}} - \eta_m^i)$$

In the same way $\Delta_{\epsilon,1} \equiv 0(\text{mod } M^{\frac{k}{2}} + \eta_m^i)$ if $(\frac{i}{m}) = -1$. So for $1 \leq a \leq m, (a,m) = 1$ we have

$$\sigma_a(\sqrt{M}^k - \eta_m)|\sigma_a(\Delta_{\epsilon,1}) = \Delta_{\epsilon,1} \tag{2.10}$$

On the other hand we have by lemma 2.3(be awear that mM is a square since M/m is a square)

$$\sigma_a(\sqrt{M}^k - \eta_m) = \sigma_a(\sqrt{M})^k - \eta_m^a = (\frac{a}{m})\sqrt{M}^k - \eta_m^a$$

Therefore for any $b \neq a, 1 \leq b \leq m, (b,m) = 1$, we have

$$(\sigma_a(\sqrt{M}^k - \eta_m), \sigma_b(\sqrt{M}^k - \eta_m) =$$

$$((\frac{a}{m})\sqrt{M}^k - \eta_m^a, (\frac{b}{m})\sqrt{M}^k - \eta_m^b)|(M^k - \eta_m^{2a}, M^k - \eta_m^{2b})|\text{Norm}_{Q(\eta_m)/Q}(1 - \eta_m^{2(b-a)})$$

Let $m_1 = m/(b-a,m)$. By lemma 2.2 we have

$$(\sigma_a(\sqrt{M}^k - \eta_m), \sigma_b(\sqrt{M}^k - \eta_m)|(\Phi_{m_1}(1))^{(b-a,m)}$$

And

$$\Phi_{m_1}(1) = \prod_{\substack{i=1 \\ (i,m_1)=1}}^{m_1} (1 - \eta_{m_1}^i)| \prod_{i=1}^{m_1-1} (1 - \eta_{m_1}^i) = m_1|m$$

Hence

$$(\sigma_a(\sqrt{M}^k - \eta_m), \sigma_b(\sqrt{M}^k - \eta_m)|m^{(b-a,m)} \tag{2.11}$$

On the other hand we have

$$(\sigma_a(\sqrt{M}^k - \eta_m), \sigma_b(\sqrt{M}^k - \eta_m))|(M^k - \eta_m^{2a}, M^k - \eta_m^{2b})|$$

$$\prod_{\substack{i=1 \\ (i,m)=1}}^{m} (M^k - \eta_m^{2i}) = \prod_{\substack{i=1 \\ (i,m)=1}}^{m} (M^k - \eta_m^i)$$

namely

$$(\sigma_a(\sqrt{M}^k - \eta_m), \sigma_b(\sqrt{M}^k - \eta_m))|\Phi_m(M^k) \tag{2.12}$$

By (2.11), (2.12) and lemma 2.5 we have

$$(\sigma_a(\sqrt{M}^k - \eta_m), \sigma_b(\sqrt{M}^k - \eta_m) = 1 \tag{2.13}$$

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

PROOF. Since $(\Delta_{\epsilon,1}, \Delta_{\epsilon,2})|2mM^{k\frac{m+1}{2}}$ and $\Phi_n(\epsilon M) = \prod_{\substack{i=1 \\ (i,n)=1}}^{n} (\epsilon M - \eta_n^i)| \prod_{i=1}^{n-1} (\epsilon M - \eta_n^i) = \frac{(\epsilon M)^n - 1}{\epsilon M - 1}$, we have $(\Phi_n(\epsilon M), M) = 1$. Because $m|M$ then $(\Phi_n(\epsilon M), mM^{k\frac{m+1}{2}}) = 1$. But $2 \not| m$ which follows $2 \not| \frac{(\epsilon M)^m - 1}{\epsilon M - 1}$, then $2 \not| \Phi_n(\epsilon M)$. Hence $(\Phi_n(\epsilon M), 2mM^{k\frac{m+1}{2}}) = 1$ which follows $(\Phi_n(\epsilon M), \Delta_{\epsilon,1}, \Delta_{\epsilon,2}) = 1$.

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

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

$$(\Phi_n(M), \mathrm{Norm}_{Q(\eta)/Q}(\sqrt{M}^k - \eta_m)) | (\Phi_n(M), \Delta_{\epsilon,1})$$

and

$$(\Phi_n(M), \mathrm{Norm}_{Q(\eta)/Q}(\sqrt{M}^k + \eta_m)) | (\Phi_n(M), \Delta_{\epsilon,2})$$

So by Theorem 2.1 we have

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

On the other hand

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

then by lemma 2.7

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

So we compete 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

$$\begin{aligned}
\Phi_{253}(-44) &= 3709784345450825186315252359342393625622097597033807 2\\
& 4696459118539078992497776911652208818164568018284503 9\\
& 393252706436580824865289578277966809685789933954937 75\\
& 93195841402705471120561689440516827477559406002819048\\
& 94424323005472001320662317966652573523661165656368874\\
& 12917494806145455573196005446169730072632762854659235\\
& 095147223301220590886668114872568041240003 01\\
\Delta_{-1,1} &= -44^{34} \cdot 3444504158952726218526600547691950150968205232\\
& 97857492650170175746544185180003727552761096352713337\\
& 70294179177848671782452407958833164292053459517131078\\
& 34686515928235771051161580969105598826912332516749252\\
& 95188319707121735655291803715040965969853944167108087\\
& 27368572689535094363252515886499722426954448015777548\\
& 1725883542868441384200481800214\\
\Delta_{-1,2} &= 44^{34} \cdot 3444504158952726218526600547691950150968205232 97\\
& 85749265017017574654418518000372755276109635271333770\\
& 29417917784867178245240795883316429205345951713107834\\
& 68651592823577123376169120637350008677859528459871092\\
& 32623093494353633587850215667423809900570469161991937\\
& 30866062009064107376799993559996769294437690473997736
\end{aligned}$$

$$\begin{aligned}
& 708251894956027511649117143 26 \\
(\Phi_{253}(-44), \Delta_{-1,1}) &= 370808211405128493101452727538293696294905001990054 85 \\
& 04948093002539948192457694962513241254988377338102340 \\
& 86264863096527642067848057690638928948383373587326170 \\
& 051260262214314 6599971 \\
(\Phi_{253}(-44), \Delta_{-1,2}) &= 10004590597907985573943582945748620748239251502916976 \\
& 18978239877682278432398712396908419662400063010898795 \\
& 14915269438067251701400814361222822136145387771492736 \\
& 1019333917217066917231 \\
\text{hence} & \\
\Phi_{253}(-44) &= 37080821140512849310145272753829369629490500199005485 \\
& 04948093002539948192457694962513241254988377338102340 \\
& 86264863096527642067848057690638928948383373587326170 \\
& 0512602622143146599971 \cdot 1000459059790798557394358 2945 \\
& 74862074823925150291697601897823987768227843239871239 \\
& 69084196624000630108987951491526943806725170140081436 \\
& 122282213614538777149273610193339172170669172 31
\end{aligned}$$

References

1. John Brillhart, D.H.Lehmer, J.L.Selfridge, Bryant Tuckerman, S.S.Wagstaff Jr., *Factorizations of* $b^n \pm 1, b = 2,3,4,5,6,7,10,11,12$ *up to High Powers*, Second Edition, AMS, 1998.
2. S.Hahn, *A Remark on Aurifeuillian Factorizations*, Math. Japonica, Vol.39. No.3, 1994, 501-502.
3. Sun Qi, Yuan Pingzhi, Han Qing, *A Question about Aurifeui llian Factorizations*, Chinese Sci.Bull., Vol 40, No 20, 1995, 1681-1683.
4. Sun Qi, Hong Shaofang, *Aurifeuillan Factorizations of* $Q^q \pm 1 (q = p^n)$. Advances in Math. (China), vol.26, No.1, 1997, 74-75.
5. Hua Luogeng, *the Introduction To Number Theorem*, Academic Press of Science.
6. S.S Wagstaff Jr.,*Some uses of Microcomputers in Number Theory Research*, Computers Math. Applied, Vol.19, No.3, 1990, 53-58.

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