Mathematical Journal of Okayama University

Volume 48, *Issue* 1 2006 *Article* 1

JANUARY 2006

On Euclidean Algorithm

Kaoru Motose*

*Hirosaki University

Math. J. Okayama Univ. **48** (2006), 1–7

ON EUCLIDEAN ALGORITHM

Kaoru MOTOSE

Recently, using cyclotomic polynomials, Z. Marciniak and S. K. Sehgal [1] obtained excellent results about units in integral group rings of cyclic groups. In this paper, we shall give some improvements and alternative proofs of their results.

For relatively prime polynomials $f(x)$ and $g(x)$ over a field K, it is easy to compute polynomials $u(x), v(x) \in K[x]$ by Euclidean algorithm such that

$$f(x)u(x) + g(x)v(x) = 1.$$

However, over $\boldsymbol{Z}[x]$, situation is different from this. Of course we can compute $u(x), v(x) \in \boldsymbol{Q}[x]$ by Euclidean algorithm for relatively prime polynomials $f(x), g(x) \in \boldsymbol{Z}[x]$. Thus we have

$$f(x)u_0(x) + g(x)v_0(x) = a$$

where $u_0(x), v_0(x) \in \boldsymbol{Z}[x]$ and $0 \neq a \in \boldsymbol{Z}$.

For example, we obtain for cyclotomic polynomials $\Phi_3(x) = x^2 + x + 1$ and $\Phi_6(x) = x^2 - x + 1$,

$$\Phi_3(x)(1 - x) + \Phi_6(x)(x + 1) = 1 - x^3 + 1 + x^3 = 2$$

and we can easily show there is no polynomials $u(x), v(x) \in \boldsymbol{Z}[x]$ such that

$$\Phi_3(x)u(x) + \Phi_6(x)v(x) = 1.$$

In fact $1 = \Phi_6(\omega)v(\omega) = -2\omega v(\omega) = -2\bar{\omega}v(\bar{\omega})$ for two roots $\omega, \bar{\omega}$ of $\Phi_3(x)$. We have a contradiction such that $1 = 4 \cdot v(\omega)v(\bar{\omega})$ and $v(\omega)v(\bar{\omega})$ is an integer.

Thus it is natural to consider the next problem.

For given polynomials $f(x),\ g(x) \in \boldsymbol{Z}[x]$*, does there exist polynomials* $u(x),\ v(x) \in \boldsymbol{Z}[x]$ *such that*

$$f(x)u(x) + g(x)v(x) = 1\ ?$$

It is easy for $f(x) = x$ and $g(x) = x^n - 1$. But in general, it seems to be difficult for me because the ring $\boldsymbol{Z}[x]$ is not Euclidean though it is a unique factorization ring. In this paper, we shall answer to this problem in case $f(x)$ and $g(x)$ are cyclotomic polynomials.

First, we start from

This paper was financially supported by Fund for the Promotion of International Scientific Research B-2, 2004, Aomori, Japan.

Lemma 1. *If monic polynomials $f(x)$ and $g(x) \in \boldsymbol{Z}[x]$ are relatively prime, then there exist polynomials $u(x), v(x) \in \boldsymbol{Z}[x]$ and a positive integer a such that*

$$f(x)u(x) + g(x)v(x) = a.$$

Moreover, we have the following facts.

(1) *there exist unique polynomials $u_0(x), v_0(x) \in \boldsymbol{Z}[x]$ such that $\deg u_0(x) < \deg g(x), \deg v_0(x) < \deg f(x)$ and*

$$f(x)u_0(x) + g(x)v_0(x) = a.$$

(2) *An integer a in (1) is divided by the smallest positive integer b satisfying*

$$f(x)u(x) + g(x)v(x) = b.$$

Proof. The first statement is clear from Euclidean algorithm in $\boldsymbol{Q}[x]$.

(1) We set $u(x) = g(x)q_1(x) + u_0(x)$ and $v(x) = f(x)q_2(x) + v_0(x)$ where $\deg u_0(x) < \deg g(x)$ and $\deg v_0(x) < \deg f(x)$. Then we have

$$s(x) := f(x)g(x)(q_1(x) + q_2(x)) = a - (f(x)u_0(x) + g(x)v_0(x)).$$

If $s(x)$ is not zero, then we have a contradiction by comparing degrees of both sides in the above equation. Uniqueness is almost clear.

(2) is easy to see using division algorithm about a and b. □

We need the following well known results for our purpose about cyclotomic polynomials (see [2, p. 82]).

Lemma 2. *We obtain the next equations*

(1) *Let p be a prime. In case $p \mid m$, $\Phi_{mp}(x) = \Phi_m(x^p)$ and in case $p \nmid m$, $\Phi_m(x)\Phi_{mp}(x) = \Phi_m(x^p)$. Moreover, $\Phi_s(x^t) = \prod_{d|t} \Phi_{sd}(x)$ for $(s,t) = 1$.*

(2) $\Phi_n(1) = \begin{cases} 0 & \text{if } n = 1, \\ p & \text{if } n \text{ is a power of the prime } p, \\ 1 & \text{if } n \text{ has at least two prime divisors.} \end{cases}$

Proof. (1) Classifying divisors d of mp by $p \mid d$ or not, we have the next equation from the definition of μ.

$$\begin{aligned} \Phi_{mp}(x) &= \prod_{d|mp} (x^d - 1)^{\mu(\frac{mp}{d})} \\ &= \prod_{d|m} (x^{pd} - 1)^{\mu(\frac{m}{d})} \cdot \prod_{d|m} (x^d - 1)^{\mu(p\frac{m}{d})} \\ &= \Phi_m(x^p) \quad \text{or} \quad \frac{\Phi_m(x^p)}{\Phi_m(x)}. \end{aligned}$$

according as $p \mid m$ or not.

Thus, we can prove the last equation on induction t. In case $t = 1$, it is trivial. Setting $t = t_1 p^e$ where p is a prime and $(t_1, p) = 1$, we obtain

$$\begin{aligned}\Phi_s(x^t) &= \Phi_{sp}((x^{t_1})^{p^{e-1}})\Phi_s((x^{t_1})^{p^{e-1}}) = \Phi_{sp^e}(x^{t_1}) \prod_{d|p^{e-1}} \Phi_{sd}(x^{t_1}) \\ &= \prod_{d|p^e} \Phi_{sd}(x^{t_1}) = \prod_{d|t} \Phi_{sd}(x).\end{aligned}$$

(2) In case $n = 1$, it is trivial because $\Phi_1(x) = x - 1$.
In case $n = p^r$, it is also trivial because

$$\Phi_{p^r}(x) = \Phi_p(x^{p^{r-1}}) \text{ and } \Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Clearly, $\Phi_n(1) \neq 0$ for $n > 1$ from the definition of cyclotomic polynomials. Thus if $n = sp^e$, where p is prime, $s > 1$ and $(s, p) = 1$, then we have the next equation from (1) and so, using $\Phi_s(1) \neq 0$, we obtain our assertion.

$$\Phi_{sp^e}(x) = \Phi_{sp}(x^{p^{e-1}}) = \frac{\Phi_s(x^{p^e})}{\Phi_s(x^{p^{e-1}})}.$$

□

If $m \neq n$, then we have $\Phi_m(x)u(x) + \Phi_n(x)v(x) = 1$ in $\boldsymbol{Q}[x]$ since $\Phi_m(x), \Phi_n(x)$ are distinct irreducible polynomials in $\boldsymbol{Q}[x]$. Over $\boldsymbol{Z}[x]$, we can see the next theorem.

Theorem 1. *Assume $n > m \geq 1$. Then we have*

(1) *If m is not a divisor of n, then there exist $u(x), v(x) \in \boldsymbol{Z}[x]$ such that*

$$\Phi_m(x)u(x) + \Phi_n(x)v(x) = 1.$$

(2) *If m is a divisor of n, then we set $n = mk$ and k_0 is the product of all distinct prime divisors of k. There exist $u(x), v(x) \in \boldsymbol{Z}[x]$ such that*

$$\Phi_m(x)u(x) + \Phi_n(x)v(x) = \Phi_{k_0}(1).$$

Proof. (1) If we set $n = mq + r,\ 0 < r < m$, then we have easily

$$x^n - 1 = (x^m - 1) \cdot (\frac{x^{mq} - 1}{x^m - 1} \cdot x^r) + x^r - 1.$$

Hence, we can use Euclidean algorithm in $\boldsymbol{Z}[x]$ for the polynomials $x^n - 1$ and $x^m - 1$, and so

$$(x^n - 1)u(x) + (x^m - 1)v(x) = x^d - 1, \quad \text{for some } u(x), v(x) \in \boldsymbol{Z}[x]$$

where $d = (n, m)$. In fact, there exists integers s and t such that $ns+mt = d$. We can see $t \neq 0$. In case $t > 0$, we have $s < 0$ since $m > d$, and

$$(x^n - 1) \cdot (-x^d)\frac{x^{-ns} - 1}{(x^n - 1)} + (x^m - 1) \cdot \frac{x^{mt} - 1}{(x^m - 1)} = x^d - 1.$$

Similarly, in case $t < 0$, we have $s > 0$ and

$$(x^n - 1) \cdot \frac{x^{ns} - 1}{(x^n - 1)} + (x^m - 1) \cdot (-x^d)\frac{x^{-mt} - 1}{(x^m - 1)} = x^d - 1.$$

Thus we have

$$\frac{x^n - 1}{x^d - 1}u(x) + \frac{x^m - 1}{x^d - 1}v(x) = 1.$$

Therefore, we obtain the next equation excluding case $m|n$.

$$\Phi_n(x)u(x) + \Phi_m(x)v(x) = 1 \ \text{ for some } u(x), v(x) \in \boldsymbol{Z}[x].$$

(2) Since $x - 1$ divides $\Phi_{k_0}(x) - \Phi_{k_0}(1)$ in $\boldsymbol{Z}[x]$, we have $x^{hm} - 1$ and so $\Phi_m(x)$ divides $\Phi_{k_0}(x^{hm}) - \Phi_{k_0}(1)$ where $h = \frac{k}{k_0}$. Let n_0 be the product of all distinct prime divisors of n. We set $n_0 = \ell k_0$ and

$$u(x) = \frac{\Phi_{k_0}(1) - \Phi_{k_0}(x^{hm})}{\Phi_m(x)} \text{ and } v(x) = \prod_{\substack{d|\ell \\ d\neq\ell}} \Phi_{k_0 d}(x^{\frac{n}{n_0}})$$

where we consider as $v(x) = 1$ in case $\ell = 1$. Then $u(x)$ and $v(x) \in \boldsymbol{Z}[x]$. Noting $\frac{n}{n_0}\ell = \frac{k}{k_0}m = hm$ and $(\ell, k_0) = 1$, we have from Lemma 2 (1)

$$\begin{aligned}
\Phi_m(x)u(x) + \Phi_n(x)v(x) &= \Phi_m(x)u(x) + \Phi_{n_0}(x^{\frac{n}{n_0}}) \prod_{\substack{d|\ell \\ d\neq\ell}} \Phi_{k_0 d}(x^{\frac{n}{n_0}}) \\
&= \Phi_{k_0}(1) - \Phi_{k_0}(x^{hm}) + \Phi_{k_0}((x^{\frac{n}{n_0}})^{\ell}) \\
&= \Phi_{k_0}(1).
\end{aligned}$$

□

Let m be a natural number and let q be a power of a prime p. Then we can see from Theorem 1 (2) that there exist $u(x), v(x) \in \boldsymbol{Z}[x]$ such that

$$\Phi_m(x)u(x) + \Phi_{mq}(x)v(x) = p.$$

However, the next proposition shows that p is the smallest positive integer satisfying the above equation.

Proposition 1. *The ideal $I_{m,n} = (\Phi_m(x), \Phi_n(x))$ of $\boldsymbol{Z}[x]$ generated by $\Phi_m(x)$ and $\Phi_n(x)$ $(m < n)$ can be calculated as follows:*

$$I_{m,n} = \begin{cases} (p, \Phi_m(x)) & \text{if } n = mq \text{ and } q \text{ is a power of a prime } p, \\ \boldsymbol{Z}[x] & \text{otherwise.} \end{cases}$$

In particular, there exist no $s(x), t(x) \in \boldsymbol{Z}[x]$ *such that*

$$\Phi_m(x)s(x) + \Phi_{mq}(x)t(x) = 1$$

where $q > 1$ *is a power of a prime* p.

Proof. Our assertion is trivial from Theorem 1 excluding case $n = mq$ and q is a power of a prime p. In this case, $I_{m,n}$ contains $(p, \Phi_m(x))$ from Theorem 1 (2). We have from Lemma 2 (1) that

$$\Phi_{mq}(x) = \Phi_m(x^q) \quad \text{or} \quad \Phi_{mq}(x)\Phi_m(x^{\frac{q}{p}}) = \Phi_m(x^q),$$

according as $p \mid m$ or not. Therefore, in any case,

$$\Phi_{mq}(x) \equiv \Phi_m(x)^k \bmod p\boldsymbol{Z}[x] \text{ for some integer } k.$$

Thus we obtain

$$I_{m,n} \equiv (\Phi_m(x), \Phi_m(x)^k) \equiv 0 \bmod (p, \Phi_m(x)) \text{ and so } I_{m,n} = (p, \Phi_m(x)).$$

Assume $I_{m,mq} = \boldsymbol{Z}[x]$, equivalently, that $\Phi_m(x)s(x) + \Phi_{mq}(x)t(x) = 1$ where $s(x), t(x) \in \boldsymbol{Z}[x]$ and $q > 1$ is a power of a prime p. Then we have $(p, \Phi_m(x)) = \boldsymbol{Z}[x]$ from the above, namely, $1 = pu(x) + \Phi_m(x)v(x)$ for some $u(x), v(x) \in \boldsymbol{Z}[x]$ and so we have

$$1 \equiv \Phi_m(\eta)v(\eta) = 0 \bmod p\boldsymbol{Z}[\eta] \text{ for } \eta \in \Delta$$

where Δ is the set of all roots of $\Phi_m(x)$. Thus $p\boldsymbol{Z}[\eta] = \boldsymbol{Z}[\eta]$ and so we have a contradiction such that $\frac{1}{p}$ is an algebraic integer. □

Remark 1. Using elementary number theory, we can prove the last part of Proposition 1 in case $p \nmid m$ (see [3]).

In the remainder of this paper, we consider our problem about $x^n - 1$ and $\Phi_m(x)$.

Theorem 2. *Let* m_0 *be the product of all distinct prime divisors of* m. *If* m_0 *is not a divisor of* n, *then there exist* $u(x), v(x) \in \boldsymbol{Z}[x]$ *such that*

$$(x^n - 1)u(x) + \Phi_m(x)v(x) = \prod_{d \mid (m_0, n)} \Phi_{\frac{m_0}{d}}(1).$$

Proof. We may assume that $m = m_0$ from

$$\Phi_m(x) = \Phi_{m_0}(x^{\frac{m}{m_0}}) \text{ and } (x^{\frac{m}{m_0}})^n - 1 = (x^n - 1) \cdot \frac{(x^n)^{\frac{m}{m_0}} - 1}{x^n - 1}.$$

We assume d is a divisor of n. If d is not a divisor of m, there exist $u_d(x), v_d(x) \in \boldsymbol{Z}[x]$ from Theorem 1 (1) such that

$$\Phi_d(x)u_d(x) + \Phi_m(x)v_d(x) = 1.$$

If d is a divisor of m, there exist $u_d(x), v_d(x) \in \boldsymbol{Z}[x]$ from Theorem 1 (2) such that

$$\Phi_d(x)u_d(x) + \Phi_m(x)v_d(x) = \Phi_{\frac{m}{d}}(1).$$

Thus we have from $x^n - 1 = \prod_{d|n} \Phi_d(x)$,

$$(x^n - 1)u(x) + \Phi_m(x)v(x) = \prod_{d|(m,n)} \Phi_{\frac{m}{d}}(1).$$

□

Theorem 3 (Marciniak and Sehgal [1])**.** *Let m_0 be the product of all distinct prime divisors of m. If $t = \frac{m_0}{(n,m_0)} > 1$ is not a prime, there exist integral polynomials $u(x),\ v(x) \in \boldsymbol{Z}[x]$ such that*

$$\Phi_m(x)u(x) + (x^n - 1)v(x) = 1.$$

Proof. We may assume $m = m_0$ from the same reason as we assumed $m = m_0$ in the proof of Theorem 2.

Proof 1. Since t is the order of ζ_m^n, where ζ_m is a root of $\Phi_m(x)$, we have

$$\Phi_t(1) = \prod_k (1 - \zeta_m^{nk}) = (1 - \zeta_m^n) \cdot \prod_{k>1} (1 - \zeta_m^{nk})$$

where k runs over $1 \leq k < t$ and $(k, t) = 1$. Thus the following polynomial $z(x)$ has a root ζ_m and is divided by $\Phi_m(x)$.

$$z(x) = (1 - x^n) \cdot \prod_{k>1} (1 - x^{nk}) - \Phi_t(1)$$

where k runs over $1 < k < t$ and $(k, t) = 1$.

Proof 2. If t is not a prime, we have $\Phi_{\frac{m}{d}}(1) = 1$ for all $d \mid (m, n)$ because $\frac{m}{d} = \frac{m}{(m,d)}$ is not a prime since $t = \frac{m}{(m,n)}$ is a divisor of $\frac{m}{(m,d)} = \frac{m}{d}$. □

Remark 2. If t is a prime p, then we have from *Proof 1* and Lemma 2 (2).

$$\Phi_m(x)u(x) + (x^n - 1)v(x) = \Phi_t(1) = p.$$

It is easy to see that the product of polynomials with the same equations as $\Phi_n(x)$ in Theorem 3 also satisfy the same condition. Thus we have a corollary.

Corollary 1. *Let $f(x)$ be a product of some x and some cyclotomic polynomials $\Phi_\ell(x)$ such that $\frac{\ell_0}{(\ell_0,n)} > 1$ is not a prime where ℓ_0 is the product of all distinct prime divisors of ℓ. Then we have $f(x)s_n(x) + (x^n - 1)t_n(x) = 1$ where $s_n(x),\ t_n(x) \in \boldsymbol{Z}[x]$.*

References

[1] Z. Marciniak and S. K. Sehgal, *Generic units in abelian group algebras*, Journal of Group Theory, to appear.
[2] R. Lidl and H. Niedereiter, *Finite fields*, 1983, Addison Wesley.
[3] K. Motose, *Integral group algebras and cyclotomic polynomials*, Proceeding of ring theory and representation theory, 2005, Nagoya.

Kaoru Motose
Department of Mathematical Sciences
Faculty of Science and Technology
Hirosaki University
Hirosaki 036-8561, Japan
e-mail address: skm@cc.hirosaki-u.ac.jp

(*Received March 7, 2005*)