IRREDUCIBILITY OF HURWITZ POLYNOMIALS OVER
THE RING OF INTEGERS

DONG YEOL OH† AND YE LIM SEO

Abstract. Let \( \mathbb{Z} \) be the ring of integers and \( \mathbb{Z}[X] \) (resp., \( h(\mathbb{Z}) \)) be
the ring of polynomials (resp., Hurwitz polynomials) over \( \mathbb{Z} \). In this
paper, we study the irreducibility of Hurwitz polynomials in \( h(\mathbb{Z}) \).
We give a sufficient condition for Hurwitz polynomials in \( h(\mathbb{Z}) \) to be
irreducible, and we then show that \( h(\mathbb{Z}) \) is not isomorphic to \( \mathbb{Z}[X] \).
By using a relation between usual polynomials in \( \mathbb{Z}[X] \) and Hurwitz
polynomials in \( h(\mathbb{Z}) \), we give a necessary and sufficient condition
for Hurwitz polynomials over \( \mathbb{Z} \) to be irreducible under additional
conditions on the coefficients of Hurwitz polynomials.

1. Introduction

Let \( R \) be a commutative ring with identity, \( R[X] \) (resp., \( R[X] \)) the
ring of formal power series (resp., polynomials) over \( R \), and \( H(R) \) the
set of formal expressions of the form \( \sum_{n=0}^{\infty} a_n X^n \), where \( a_n \in R \) for all
\( n \geq 1 \). We define an addition on \( H(R) \) as usual and a multiplication,
called \( \ast \)-product, on \( H(R) \) as follows: for \( f(X) = \sum_{n=0}^{\infty} a_n X^n \), \( g(X) = \sum_{n=0}^{\infty} b_n X^n \in H(R) \),
\[
f(X) \ast g(X) = \sum_{n=0}^{\infty} c_n X^n, \quad c_n = \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k} \]

† This work was supported by Research Fund from Chosun University, 2016.

This is an Open Access article distributed under the terms of the Creative com-
mons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-
-nc/3.0/) which permits unrestricted non-commercial use, distribution and repro-
duction in any medium, provided the original work is properly cited.
where \( \binom{n}{k} = \frac{n!}{k!(n-k)!} \) for nonnegative integers \( n \geq k \). It is shown in [3] that \( H(R) \) is a commutative ring with identity under these two operations, i.e., \( H(R) = (R[X], +, \ast) \). The ring \( H(R) \) is called the ring of Hurwitz series over \( R \). The ring \( h(R) \) of Hurwitz polynomials over \( R \) is the subring of \( H(R) \) consisting of formal expressions of the form \( \sum_{k=0}^{n} a_k X^k \), i.e., \( h(R) = (R[X], +, \ast) \). Keigher introduced the ring of Hurwitz series and studied its properties [3, 4]. Since then, many works on the ring of Hurwitz series have been done ([1, 2, 5–7]).

It is known that \( h(R) \) is an integral domain if and only if \( R \) is an integral domain with \( \text{char}(R) = 0 \) [1, Proposition 1.1], [3, Corollary 2.8]. For an integral domain \( R \) with \( \text{char}(R) = 0 \), it is shown that \( h(R) \) satisfies the ascending chain condition on principal ideals (ACCP) if and only if \( R \) satisfies ACCP [5, Theorem 2.4]. So the ring \( h(Z) \) of Hurwitz polynomials over \( Z \) is an integral domain satisfying ACCP. Hence \( h(Z) \) is atomic, that is, every nonzero nonunit element can be written as a finite product of irreducible elements.

In this paper, we investigate the irreducibility of Hurwitz polynomials in \( h(Z) \). This paper consists of four sections including introduction. In Section 2, we give a sufficient condition for Hurwitz polynomials in \( h(Z) \) to be irreducible. We then show that \( h(Z) \) is not a UFD, thus \( h(Z) \) is not isomorphic to \( Z[X] \). For a nonzero element \( f(X) = \sum_{i=0}^{n} a_i X^i \in h(Z) \), where \( a_n \neq 0 \), \( n \) is called the degree of \( f(X) \) and write \( \deg(f) = n \). In Section 3, we completely characterize the irreducible Hurwitz polynomials over \( Z \) of degree 2, and give a necessary and sufficient condition for Hurwitz polynomials \( f(X) \) over \( Z \) of degree 3 under some additional conditions on the coefficients of \( f(X) \). In Section 4, we give a necessary and sufficient condition for Hurwitz polynomials \( f(X) \) over \( Z \) of degree \( n \geq 4 \) under some additional conditions on the coefficients of \( f(X) \).

2. Irreducible Hurwitz Polynomials

Let \( R \) be a commutative ring with identity and \( U(R) \) be the set of units of \( R \). We start this section with the following simple observation without proof.

**Lemma 2.1.** Let \( D \) be an integral domain with \( \text{char}(D) = 0 \). Then \( U(h(D)) = U(D) \).
For a nonzero element \( f(X) = \sum_{i=0}^{n} a_i X^i \in h(Z) \), we say that \( f(X) \) is primitive if \( \gcd(a_0, a_1, \ldots, a_n) = 1 \) (i.e., if \( d \) divides all \( a_i \), then \( d \) is a unit). If a nonzero nonunit element of \( h(Z) \) is not primitive, then it is reducible. Clearly every primitive Hurwitz polynomial in \( h(Z) \) of degree one is irreducible.

**Proposition 2.2.** Let \( f(X) = \sum_{i=0}^{n} a_i X^i \in h(Z) \) be a primitive Hurwitz polynomial of degree \( n \geq 2 \). If \( |a_n| < n \), then \( f(X) \) is irreducible in \( h(Z) \).

**Proof.** Suppose that \( f(X) \) is reducible in \( h(Z) \). Since \( f(X) \) is primitive, there exist \( g(X) = \sum_{j=0}^{s} b_j X^j, h(X) = \sum_{k=0}^{t} c_k X^k \in h(Z) \) with \( 1 \leq s, t \leq n - 1 \) and \( s + t = n \) such that \( f(X) = g(X) \ast h(X) \). Hence

\[
a_n = \binom{s + t}{s} b_s c_t = \binom{n}{s} b_s c_t.
\]

Thus \( |a_n| \geq n \), which is a contradiction. \( \square \)

The following is a sufficient condition for a Hurwitz polynomial over \( Z \) of a prime power degree to be irreducible, which is an analog of Eisenstein’s criterion which gives a sufficient condition for a polynomial in \( Z[X] \) to be irreducible.

**Proposition 2.3.** Let \( n = p^m \), where \( p \) is a prime number and \( m \geq 1 \). Let \( f(X) = \sum_{i=0}^{n} a_i X^i \in h(Z) \) be a primitive Hurwitz polynomial of degree \( n \). If \( p \nmid a_n \), then \( f(X) \) is irreducible in \( h(Z) \).

**Proof.** Suppose that \( f(X) \) is reducible in \( h(Z) \). Since \( f(X) \) is primitive, there exist \( g(X) = \sum_{j=0}^{s} b_j X^j, h(X) = \sum_{k=0}^{t} c_k X^k \in h(Z) \) with \( 1 \leq s, t \leq n - 1 \) and \( s + t = n \) such that \( f(X) = g(X) \ast h(X) \). Hence

\[
a_n = \binom{s + t}{s} b_s c_m = \binom{p^m}{s} b_s c_m.
\]

Thus \( p \mid a_n \), a contradiction. \( \square \)

**Corollary 2.4.** Let \( f(X) = \sum_{i=0}^{n} a_i X^i \) be a primitive Hurwitz polynomial over \( Z \) of prime degree \( p \). If \( p \nmid a_p \), then \( f(X) \) is irreducible in \( h(Z) \).

**Remark 2.5.** It is known that if \( R \) is an integral domain containing the field \( Q \) of rational numbers, then \( h(R) \cong R[X] \) [4, Proposition 2.4]. In general, when \( R \) is an integral domain not containing \( Q \), we do not
know whether $h(R)$ is isomorphic to $R[X]$. Since $h(Z)$ satisfies ACCP [5, Theorem 2.4], $h(Z)$ is atomic. Clearly, 2 and $X$ are irreducible in $h(Z)$. Note that $X^2$ is irreducible in $h(Z)$ by Proposition 2.2. Since $2 \ast X^2 = X \ast X$, $h(Z)$ is not a UFD. Hence $h(Z)$ is not isomorphic to $Z[X]$.

3. Irreducible Hurwitz Polynomials of degree $\leq 3$

It is well known that a primitive polynomial over $Z$ is irreducible over $Z$ if and only if it is irreducible over $Q$, which is called Gauss Lemma. Hence a necessary and sufficient condition for a polynomial $f(X)$ over $Z$ of degree 2 or 3 to be irreducible is that $f(X)$ has no rational zeros. Thus it is easy to determine whether a polynomial over $Z$ of degree $\leq 3$ is irreducible or not. In this section, we give a necessary and sufficient condition for Hurwitz polynomials over $Z$ of degree $\leq 3$ to be irreducible by using the irreducibility of polynomials in $Z[X]$.

We note that every primitive polynomial of degree one in $Z[X]$ (resp., $h(Z)$) is irreducible. We start this section with Hurwitz polynomials over $Z$ of degree 2. Let $f(X) = a_2X^2 + a_1X + a_0 \in h(Z)$, where $a_2 \neq 0$. By Corollary 2.4, we only consider the case when $a_2$ is even.

**Theorem 3.1.** Let $f(X) = \sum_{i=0}^{2} a_iX^i$ be a primitive Hurwitz polynomial over $Z$ of degree 2 with $2 \mid a_2$. Then the following are equivalent.

1. $f(X) = a_2X^2 + a_1X + a_0$ is irreducible in $h(Z)$.
2. $g(X) = \frac{1}{2}a_2X^2 + a_1X + a_0$ is irreducible in $Z[X]$.

**Proof.** Note that

$$(b_1X + b_0) \ast (c_1X + c_0) = \binom{2}{1}b_1c_1X^2 + \binom{1}{1}b_1c_0 + \binom{1}{0}b_0c_1X + b_0c_0 = 2b_1c_1X^2 + (b_1c_0 + b_0c_1)X + b_0c_0.$$

Since $\gcd(a_0, a_1, a_2) = 1$, $f(X)$ and $g(X)$ are both primitive. Thus if $f(X)$ (resp., $g(X)$) is reducible in $h(Z)$ (resp., $Z[X]$), then $f(X)$ (resp., $g(X)$) is a $\ast$-product (resp., usual product) of two polynomials of degree one. Hence $f(X) = (b_1X + b_0) \ast (c_1X + c_0)$ in $h(Z)$ if and only if $g(X) = (b_1X + b_0)(c_1X + c_0)$ in $Z[X]$. Therefore $f(X)$ is irreducible in $h(Z)$ if and only if $g(X)$ is irreducible in $Z[X]$. □
Remark 3.2. The condition \( \gcd(a_2, a_1, a_0) = 1 \) in Theorem 3.1 is necessary since \( X^2 + 2X + 4 \in \mathbb{Z}[X] \) is irreducible, but \( 2X^2 + 2X + 4 = 2(X^2 + X + 2) \in h(\mathbb{Z}) \) is reducible.

For a primitive Hurwitz polynomial \( f(X) = \sum_{i=0}^{3} a_i X^i \in h(\mathbb{Z}) \) of degree 3, we only consider the case when \( 3 \mid a_3 \) by Corollary 2.4. We first give a sufficient condition for a primitive Hurwitz polynomial \( f(X) = \sum_{i=0}^{3} a_i X^i \in h(\mathbb{Z}) \) of degree 3 with \( 3 \mid a_3 \) to be irreducible.

**Proposition 3.3.** Let \( f(X) = \sum_{i=0}^{3} a_i X^i \) be a primitive Hurwitz polynomial over \( \mathbb{Z} \) of degree 3 with \( 3 \mid a_3 \). If \( g(X) = \frac{1}{3} a_3 X^3 + a_2 X^2 + 2a_1 X + 2a_0 \) is irreducible in \( \mathbb{Z}[X] \), then \( f(X) \) is irreducible in \( h(\mathbb{Z}) \).

Proof. Suppose that \( f(X) \) is reducible in \( h(\mathbb{Z}) \). Then \( f(X) = h(X) \ast k(X) \), where \( h(X) \) and \( k(X) \) are Hurwitz polynomials over \( \mathbb{Z} \) of degree one and two, respectively. Write \( h(X) = b_1 X + b_0 \) and \( k(X) = c_2 X^2 + c_1 X + c_0 \). So we obtain

\[
\begin{align*}
f(X) &= (b_1 X + b_0) \ast (c_2 X^2 + c_1 X + c_0) \\
&= 3b_1 c_2 X^3 + (2b_1 c_1 + b_0 c_2) X^2 + (b_1 c_0 + b_0 c_1) X + b_0 c_0 \\
&= a_3 X^3 + a_2 X^2 + a_1 X + a_0.
\end{align*}
\]

Hence, \( \frac{1}{3} a_3 = b_1 c_2, a_2 = 2b_1 c_1 + b_0 c_2, 2a_1 = 2(b_1 c_0 + b_0 c_1), \) and \( 2a_0 = 2b_0 c_0 \). Therefore, \( g(X) = (b_1 X + b_0)(c_2 X^2 + 2c_1 X + 2c_0) \), which is a contradiction to that \( g(X) \) is irreducible in \( \mathbb{Z}[X] \).

To find an equivalent condition for a primitive Hurwitz polynomial \( f(X) = \sum_{i=0}^{3} a_i X^i \in h(\mathbb{Z}) \) of degree 3 with \( 3 \mid a_3 \), we divide it into two cases: \( 2 \mid a_3 \) or \( 2 \nmid a_3 \).

**Theorem 3.4.** Let \( f(X) = \sum_{i=0}^{3} a_i X^i \) be a primitive Hurwitz polynomial over \( \mathbb{Z} \) of degree 3 with \( 3 \mid a_3 \). If \( 2 \mid a_3 \) and \( 2 \nmid a_2 \), then the following are equivalent.

1. \( f(X) = a_3 X^3 + a_2 X^2 + a_1 X + a_0 \) is irreducible in \( h(\mathbb{Z}) \).
2. \( g(X) = \frac{1}{3} a_3 X^3 + \frac{1}{2} a_2 X^2 + a_1 X + a_0 \) is irreducible in \( \mathbb{Z}[X] \).
3. \( g(X) \) has no rational roots.

Proof. Note that for each \( b_i, c_j \in \mathbb{Z} \),

\[
\begin{align*}
&\left\{ (b_1 X + b_0) \ast (c_2 X^2 + c_1 X + c_0) = 3b_1 c_2 X^3 + (2b_1 c_1 + b_0 c_2) X^2 + (b_1 c_0 + b_0 c_1) X + b_0 c_0, \\
&(b_1 X + b_0)(\frac{1}{2} c_2 X^2 + c_1 X + c_0) = \frac{1}{2} b_1 c_2 X^3 + (b_1 c_1 + \frac{1}{2} b_0 c_2) X^2 + (b_1 c_0 + b_0 c_1) X + b_0 c_0.
\end{align*}
\]

Since \( \gcd(a_0, a_1, a_2, a_3) = 1 \), \( f(X) \) and \( g(X) \) are both primitive. Thus if \( f(X) \) (resp., \( g(X) \)) is reducible in \( h(\mathbb{Z}) \) (resp., \( \mathbb{Z}[X] \)), then \( f(X) \) (resp.,
$g(X)$ is a $*$-product (resp., usual product) of polynomials of degree one and two.

(1) $\Leftrightarrow$ (2) By the equation above, $f(X) = (b_1X+b_0)\ast(c_2X^2+c_1X+c_0)$ in $h(\mathbb{Z})$ if and only if $g(X) = (b_1X+b_0)((\frac{1}{2}c_2X^2+c_1X+c_0)$ in $\mathbb{Q}[X]$. Since $g(X)$ is primitive in $\mathbb{Z}[X]$, $g(X)$ is reducible in $\mathbb{Q}[X]$ if and only if $g(X)$ is reducible in $\mathbb{Z}[X]$ by Gauss Lemma. Therefore $f(X)$ is irreducible in $h(\mathbb{Z})$ if and only if $g(X)$ is irreducible in $\mathbb{Z}[X]$.

(2) $\Leftrightarrow$ (3) Clear.

**Theorem 3.5.** Let $f(X) = \sum_{i=0}^{3} a_iX^i$ be a primitive Hurwitz polynomial over $\mathbb{Z}$ of degree 3 with $3 \mid a_3$.

1. If $2 \nmid a_3$, $2 \mid a_2$, $2 \mid a_1$, and $4 \mid a_0$, then the following are equivalent.
   
   (a) $f(X) = a_3X^3 + a_2X^2 + a_1X + a_0$ is irreducible in $h(\mathbb{Z})$.
   
   (b) $g(X) = \frac{1}{3}a_3X^3 + \frac{1}{2}a_2X^2 + \frac{1}{3}a_1X + \frac{1}{2}a_0$ is irreducible in $\mathbb{Z}[X]$.
   
   (c) $g(X)$ has no rational roots.

2. If $2 \nmid a_3$, $2 \nmid a_2$, and $2 \nmid a_0$, then the following are equivalent.

   (a) $f(X) = a_3X^3 + a_2X^2 + a_1X + a_0$ is irreducible in $h(\mathbb{Z})$.
   
   (b) $g(X) = \frac{1}{3}a_3X^3 + a_2X^2 + 2a_1X + 2a_0$ is irreducible in $\mathbb{Z}[X]$.
   
   (c) $g(X)$ has no rational roots.

**Proof.** (1) : (b) $\Leftrightarrow$ (c) Clear. (a) $\Leftrightarrow$ (b) Note that for each $b_i, c_j \in \mathbb{Z}$,

\[
\begin{cases}
(b_1X+b_0)\ast(c_2X^2+c_1X+c_0) = 3b_1c_2X^3 + (2b_1c_1 + b_0c_2)X^2 + (b_1c_0 + b_0c_1)X + b_0c_0,

(b_1X + \frac{1}{2}b_0)(c_2X^2 + c_1X + \frac{1}{2}c_0) = b_1c_2X^3 + (b_1c_1 + \frac{1}{2}b_0c_2)X^2 + \frac{1}{2}(b_1c_0 + b_0c_1)X + \frac{1}{4}b_0c_0.
\end{cases}
\]

By the equation above, $f(X) = (b_1X+b_0)\ast(c_2X^2+c_1X+c_0)$ in $h(\mathbb{Z})$ if and only if $g(X) = (b_1X + \frac{1}{2}b_0)(c_2X^2 + c_1X + \frac{1}{2}c_0)$ in $\mathbb{Q}[X]$. Since $g(X)$ is primitive in $\mathbb{Z}[X]$, $g(X)$ is reducible in $\mathbb{Q}[X]$ if and only if $g(X)$ is reducible in $\mathbb{Z}[X]$ by Gauss Lemma. Therefore $f(X)$ is irreducible in $h(\mathbb{Z})$ if and only if $g(X)$ is irreducible in $\mathbb{Z}[X]$.

(2) : (b) $\Leftrightarrow$ (c) Clear. (b) $\Rightarrow$ (a) It follows from Proposition 3.3.

(a) $\Rightarrow$ (b) Let $f(X)$ be irreducible in $h(\mathbb{Z})$. Suppose that $g(X)$ is reducible in $\mathbb{Z}[X]$. Then $g(X) = h(X)k(X)$, where $h(X)$ and $k(X)$ are polynomials over $\mathbb{Z}$ of degree one and two, respectively. Write $h(X) = b_1X + b_0$ and $k(X) = c_2X^2 + c_1X + c_0$. So we obtain

\[
g(X) = (b_1X + b_0)(c_2X^2 + c_1X + c_0)
= b_1c_2X^3 + (b_1c_1 + b_0c_2)X^2 + (b_1c_0 + b_0c_1)X + b_0c_0
= \frac{1}{3}a_3X^3 + a_2X^2 + 2a_1X + 2a_0.
\]
By assumption, we obtain

\begin{align}
\left\{ \begin{array}{ll}
2 \nmid a_3 = 3b_1c_2, & 2 \nmid a_2 = b_1c_1 + b_0c_2, \\
2a_1 = b_1c_0 + b_0c_1, & 4 \nmid 2a_0 = b_0c_0.
\end{array} \right.
\end{align}

If \(2 \mid b_0\), then \(2 \nmid c_0\). So \(2 \mid b_1\) and \(2 \mid a_2\), a contradiction. Hence,
\(2 \nmid b_0\), \(2 \mid c_0\), and \(2 \mid c_1\). Thus \(c_2X^2 + \frac{1}{2}c_1X + \frac{1}{2}c_0 \in h(\mathbb{Z})\). Therefore,
\(f(X) = (b_1X + b_0) \ast (c_2X^2 + \frac{1}{2}c_1X + \frac{1}{2}c_0)\), which is a contradiction to that \(f(X)\) is irreducible in \(h(\mathbb{Z})\).

\[\square\]

**Remark 3.6.** For primitive Hurwitz polynomials \(f(X)\) over \(\mathbb{Z}\) of degree \(3\) except ones in Theorems 3.4 and 3.5, we could not find an equivalent condition for \(f(X)\) to be irreducible.

**4. Irreducible Hurwitz Polynomials of degree \(n \geq 4\)**

In this section, we give an equivalent condition for Hurwitz polynomials \(f(X)\) over \(\mathbb{Z}\) of degree \(n \geq 4\) under additional conditions on the coefficients of \(f(X)\) to be irreducible. We also give a sufficient condition for some Hurwitz polynomials over \(\mathbb{Z}\) of degree \(4\) to be irreducible.

**Theorem 4.1.** Let \(f(X) = \sum_{i=0}^{n} a_iX^i\) be a primitive Hurwitz polynomial of degree \(n \geq 4\). If \(k! \mid a_k\) for each \(0 \leq k \leq n\), then the following are equivalent.

1. \(f(X)\) is irreducible in \(h(\mathbb{Z})\).
2. \(g(X) = \sum_{k=0}^{n} \frac{1}{k!}a_kX^k\) is irreducible in \(\mathbb{Z}[X]\).

**Proof.** \((1) \Rightarrow (2)\) Let \(f(X)\) be irreducible in \(h(\mathbb{Z})\). Suppose that \(g(X)\) is reducible in \(\mathbb{Z}[X]\). Since \(f(X)\) is primitive, \(g(X)\) is also primitive. Then there exist two polynomials \(h(X) = \sum_{i=0}^{s} b_iX^i, k(X) = \sum_{j=0}^{t} c_jX^j \in \mathbb{Z}[X]\) with \(1 \leq s, t \leq n - 1\) and \(s + t = n\) such that
\[g(X) = h(X)k(X)\]

For each \(0 \leq i \leq n\), we obtain

\[a_i = i! \sum_{k+l=i} b_kc_l,\]

where the sum is taken over all the pairs \((k, l)\) such that \(k + l = i\) for \(0 \leq k \leq s\) and \(0 \leq l \leq t\). We now consider \(h_1(X) = \sum_{i=0}^{s} l!b_iX^i, k_1(X) = \sum_{j=0}^{t} \frac{1}{j!}c_jX^j\)
\[
\sum_{j=0}^{t} j!c_j X^j \in h(\mathbb{Z}). \quad \text{Put } h_1(X) \ast k_1(X) = \sum_{i=0}^{n} d_i X^i. \quad \text{Then for each } 0 \leq i \leq n, \text{ we obtain}
\]
\[
(3) \quad d_i = \sum_{k+l=i} \binom{i}{k} k!b_k l!c_l = \sum_{k+l=i} i!b_k c_l = i! \sum_{k+l=i} b_k c_l,
\]
where the sum is taken over all the pairs \((k, l)\) such that \(k + l = i\) for \(0 \leq k \leq s\) and \(0 \leq l \leq t\). It follows from Equations (2) and (3) that \(f(X) = h_1(X) \ast k_1(X)\), which is a contradiction to that \(f(X)\) is irreducible in \(h(\mathbb{Z})\).

(2) \Rightarrow (1) Let \(g(X)\) be irreducible in \(\mathbb{Z}[X]\). Suppose that \(f(X)\) is reducible in \(h(\mathbb{Z})\). Since \(f(X)\) is primitive, there exist \(h(X) = \sum_{i=0}^{s} b_i X^i, k(X) = \sum_{j=0}^{t} c_j X^j \in h(\mathbb{Z})\) with \(1 \leq s, t \leq n - 1\) and \(s + t = n\) such that \(f(X) = h(X) \ast k(X)\).

For each \(0 \leq i \leq n\), we obtain
\[
(4) \quad a_i = \sum_{k+l=i} \binom{i}{k} b_k c_l,
\]
where the sum is taken over all the pairs \((k, l)\) such that \(k + l = i\) for \(0 \leq k \leq s\) and \(0 \leq l \leq t\). We now consider \(h_2(X) = \sum_{i=0}^{s} \frac{1}{i!} b_i X^i, k_2(X) = \sum_{j=0}^{t} \frac{1}{j!} c_j X^j\). Note that \(h_2(X), k_2(X) \in \mathbb{Q}[X]\). Put \(h_2(X)k_2(X) = \sum_{i=0}^{n} e_i X^i\). Then for each \(0 \leq i \leq n\), we obtain
\[
(5) \quad e_i = \sum_{k+l=i} \frac{1}{k!} b_k \frac{1}{l!} c_l = \frac{1}{i!} \sum_{k+l=i} \binom{i}{k} b_k c_l,
\]
where the sum is taken over all the pairs \((k, l)\) such that \(k + l = i\) for \(0 \leq k \leq s\) and \(0 \leq l \leq t\). It follows from Equations (4) and (5) that \(e_i = \frac{1}{i!} a_i\) for each \(0 \leq i \leq n\). Hence \(g(X) = h_2(X)k_2(X)\) in \(\mathbb{Q}[X]\). By Gauss lemma, \(g(X)\) is reducible in \(\mathbb{Z}[X]\). It is a contradiction to that \(g(X)\) is irreducible in \(\mathbb{Z}[X]\).

By applying Theorem 4.1 to a primitive Hurwitz polynomial \(f(X) = \sum_{i=0}^{4} a_i X^i\) of degree 4, we only consider the cases when \(k! \mid a_k\) for \(0 \leq k \leq 4\). Among the cases when \(4! \nmid a_4\), we consider the case when \(4 \nmid a_4\) and \(6 \mid a_4\) for \(f(X) = \sum_{i=0}^{4} a_i X^i\). We start with the following simple observation without proof.

**Lemma 4.2.** Let \(f(X) = \sum_{i=0}^{4} a_i X^i\) be a primitive Hurwitz polynomial over \(\mathbb{Z}\) of degree 4. Then
Irreducibility of Hurwitz polynomials

1. if \( f(X) = g(X) \ast h(X) \), where \( \deg(g) = 1 \) and \( \deg(h) = 3 \), then \( 4 \mid a_4 \).
2. if \( f(X) = g(X) \ast h(X) \), where \( \deg(g) = \deg(h) = 2 \), then \( 6 \mid a_4 \).
3. if \( 4 \nmid a_4 \) and \( 6 \nmid a_4 \), then \( f(X) \) is irreducible.

**Theorem 4.3.** Let \( f(X) = \sum_{i=0}^{4} a_i X^i \) be a primitive Hurwitz polynomial of degree 4 such that \( 6 \mid a_4 \) and \( 4 \nmid a_4 \). Suppose that \( g(X) = \frac{1}{6}a_4X^4 + \frac{1}{3}a_3X^3 + \frac{1}{2}a_2X^2 + \frac{1}{3}a_1X + \frac{1}{3}a_0 \in \mathbb{Z}[X] \). If \( g(X) \) is irreducible in \( \mathbb{Z}[X] \), then \( f(X) \) is irreducible in \( \mathbb{h}(\mathbb{Z}) \).

**Proof.** Suppose that \( f(X) \) is reducible in \( h(\mathbb{Z}) \). Since \( 6 \mid a_4 \) and \( 4 \nmid a_4 \), there exist \( h(X), k(X) \in h(\mathbb{Z}) \) of degree 2 such that \( f(X) = h(X) \ast k(X) \) by Lemma 4.2. Let \( h(X) = b_2X^2 + b_1X + b_0 \) and \( k(X) = c_2X^2 + c_1X + c_0 \). Then we obtain

\[
\begin{align*}
   a_4 &= 6b_2c_2, \\
   a_3 &= 3b_2c_1 + 3b_1c_2, \\
   a_2 &= b_2c_0 + 2b_1c_1 + b_0c_2, \\
   a_1 &= b_1c_0 + b_0c_1, \\
   a_0 &= b_0c_0.
\end{align*}
\]

Let \( h_1(X) = 2b_2X^2 + 2b_1X + b_0 \) and \( k_1(X) = 2c_2X^2 + 2c_1X + c_0 \). Put \( \frac{1}{4}h_1(X)k_1(X) = \sum_{i=0}^{4} d_i X^i \). It follows from Equation (6) that

\[
\begin{align*}
   d_4 &= b_2c_2 = \frac{1}{6}a_4, \\
   d_3 &= b_2c_1 + b_1c_2 = \frac{1}{3}a_3, \\
   d_2 &= \frac{1}{2}b_1c_0 + b_1c_1 + \frac{1}{2}b_0c_2 = \frac{1}{2}a_2, \\
   d_1 &= \frac{1}{2}b_1c_0 + b_0c_1 = \frac{1}{2}a_1, \\
   d_0 &= \frac{1}{4}b_0c_0 = \frac{1}{4}a_0.
\end{align*}
\]

It follows from Equation (7) that \( g(X) = \frac{1}{4}h_1(X)k_1(X) \). Thus \( g(X) \) is reducible over \( \mathbb{Q} \), and hence it is reducible over \( \mathbb{Z} \), which is a contradiction. 

**Acknowledgments**

We would like to thank the referees for several valuable suggestions. This paper contains part of a master’s thesis of Y.L.Seo done at Chosun University.
References


Dong Yeol Oh
Department of Mathematics Education
Chosun University, Gwangju 61452, Republic of Korea
E-mail: dyoh@chosun.ac.kr, dongyeol70@gmail.com

Ye Lim Seo
Department of Mathematics Education
Chosun University, Gwangju 61452, Republic of Korea
E-mail: nar4.rim@naver.com