신 용 수 교수지도

석 사 학 위 논 문

Irreducible Polynomials in $\mathbb{Z}[x]$

2009

성신여자대학교 교육대학원

교육학과 수학교육전공

장 서 연

Irreducible Polynomials in $\mathbb{Z}[x]$

신 용 수 교수지도

이 논문을 석사학위논문으로 제출함.

2009월 5월

성신여자대학교 교육대학원

교육학과 수학교육전공

장 서 연

인 준 서

장서연의 석사학위 논문으로 인준함.

심사위원 _____ 인

심사위원 _____ 인

심사위원 _____ 인

성신여자대학교 교육대학원

목 차

논 문 개 요

지수의 밑을 $b(\geq 2)$로 가지는 다항식이 다음과 같이 소수 p, 즉, $p = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b^1 + a_0$ 로 표현될 때, 그 때 만들어진 $f(x)$ 다항식 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x^1 + a_0$ 은 정수계수 안에서 기약이다.

이 논문에서는 위 정리를 상세하게 증명하고, 그 결과를 사용하여 b가 2일 때와 2보다 클 때로 나누어, 정수계수 안에서 기약인 $f(x)$ 다항식을 나타내는 소수 p의 예를 찾아보았다.

1. **Introduction**

The similarity between prime numbers and irreducible polynomials has been a dominant theme in development of number theory and algebraic geometry. It is not difficult to see that if a polynomial represents prime numbers infinitely often, then it is an irreducible polynomial. To see this, let us try to factor $f(x) = g(x)h(x)$ with $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ of positive degree. The fact that $f(x)$ takes prime values infinitely often implies that either $g(x)$ or $h(x)$ takes the value ± 1 infinitely often. This is a contradiction, for a polynomial of positive degree can take a fixed value only finitely often.

There is a stronger converse to Buniakowski's conjecture that is easily derived (see Theorem 2.1). To be specific, if a polynomial $f(x)$ belonging to $\mathbb{Z}[x]$ represents a single prime number for some sufficiently large integer value of x, then the polynomial is irreducible. A classical result of A. Cohn (see [1]) states that, if we express a prime p in base 10 as

$$p = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0,$$

then the polynomial

$$f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0$$

is necessarily irreducible in $\mathbb{Z}[x]$.

In this thesis, we reprove that if we express a prime p in base $b \geq 2$ as

$$p = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0,$$

then the polynomial

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

is necessarily irreducible in $\mathbb{Z}[x]$ (see Theorems 2.7 and 2.13).

Using this result, we make an example for a prime number p in base $b = 2$ and $b > 2$.

2. Irreducible Polynomials in $\mathbb{Z}[x]$

Theorem 2.1. *Let $f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0$ be a polynomial of degree m in $\mathbb{Z}[x]$ and set*

$$H = \max_{0 \leq i \leq m-1} |a_i / a_m|.$$

If $f(n)$ is a prime for some integer $n \geq H + 2$, then $f(x)$ is irreducible in $\mathbb{Z}[x]$.

The proof will be based on the following elementary lemma.

Lemma 2.2. *Let $f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0$ be of degree m and have α in $\mathbb{C}$ as a root. Then*

$$|\alpha| < H + 1,$$

where H is defined as in Theorem 2.1*.*

Proof. Since $f(\alpha) = a_m\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0 = 0$, We have

$$\begin{aligned}
-a_m\alpha^m &= a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0 \\
\Rightarrow \alpha^m &= \left(\frac{-a_{m-1}}{a_m}\right)\alpha^{m-1} + \cdots + \left(\frac{-a_1}{a_m}\right)\alpha + \left(\frac{-a_0}{a_m}\right) \\
|\alpha^m| &= \left|\left(\frac{-a_{m-1}}{a_m}\right)\alpha^{m-1} + \cdots + \left(\frac{-a_1}{a_m}\right)\alpha + \left(\frac{-a_0}{a_m}\right)\right| \\
&\leq \left|\left(\frac{-a_{m-1}}{a_m}\right)\alpha^{m-1}\right| + \cdots + \left|\left(\frac{-a_1}{a_m}\right)\alpha\right| + \left|\left(\frac{-a_0}{a_m}\right)\right| \\
&\leq \left|\left(\frac{-a_{m-1}}{a_m}\right)\right||\alpha^{m-1}| + \cdots + \left|\left(\frac{-a_1}{a_m}\right)\right||\alpha| + \left|\left(\frac{-a_0}{a_m}\right)\right| \\
&\leq H|\alpha|^{m-1} + \cdots + H|\alpha| + H \cdot 1 \\
&= H(|\alpha|^{m-1} + \cdots + |\alpha| + 1) \\
&= H\left(\frac{|\alpha|^m - 1}{|\alpha| - 1}\right).
\end{aligned} \tag{2.1}$$

Case 1. If $|\alpha| \leq 1$, then $|\alpha| \leq 1 < H + 1$. Thus $|\alpha| < H + 1$.

Case 2. If $|\alpha| > 1$, then

$$\begin{aligned}
|\alpha|^m(|\alpha| - 1) &\leq H\left(\frac{|\alpha|^m - 1}{|\alpha| - 1}\right) \cdot (|\alpha| - 1) \quad (\because \text{equation (2.1)}) \\
&\leq H(|\alpha|^m - 1) \\
&< H(|\alpha|^m),
\end{aligned}$$

and thus $|\alpha| - 1 < H$, that is, $|\alpha| < H + 1$, as we wished. □

The theorem can now be proved using this lemma.

Proof of Theorem 2.1. If $f(x)$ is reducible in $\mathbb{Z}[x]$, write $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ are of positive degree. Since $f(n) = g(n)\cdot h(n)$ is a prime for some integer $n \geq H + 2$, we must have either $g(n)$ or $h(n)$ equal to ± 1. Without loss of generality, we may suppose that it is $g(n)$. We can express g in the manner

$$g(x) = c\prod_i (x - \alpha_i),$$

where c is the leading coefficient of g and the product is over a subset of the complex zeros of f. In view of Lemma 2.2,

$$\begin{aligned} |g(n)| = \left|c\prod_i (n-\alpha_i)\right| &= |c|\left|\prod_i (n-\alpha_i)\right| \\ &\geq \prod_i (n - |\alpha_i|) \\ &> \prod_i (n - (H+1)) \geq 1, \end{aligned}$$

which is a contradiction. This completes the proof. □

Theorem 2.1 offers a simple irreducibility criterion that is applicable when most traditional tests fail.

Example 2.3. (1) Consider $f(x) = x^4 + 6x^2 + 1 \in \mathbb{Z}[x]$. Then it is clear that $H = 6$, and $8 \geq 6 + 2$. So $f(8) = 8^4 + 6\cdot 8^2 + 1 = 4481$ is a prime, and hence $f(x)$ is irreducible in $\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$ by Theorem 2.1.

(2) Let $f(x) = x^4 + 3x^2 + 1 \in \mathbb{Z}[x]$. Then $H = 3$, and $5 \geq 3 + 2$. Since $f(5) = 5^4 + 3 \cdot 5^2 + 1 = 701$ is a prime, $f(x)$ is irreducible in $\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$ by Theorem 2.1.

(3) Let $f(x) = x^6 - 2x^5 - 3x^3 + x + 2 \in \mathbb{Z}[x]$. Then $H = 3$, and $5 \geq 3+2$. Since $f(5) = 5^6 - 2 \cdot 5^5 - 3 \cdot 5^3 + 5 + 2 = 9007$ is a prime, $f(x)$ is irreducible in $\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$ by Theorem 2.1.

Example 2.4. (1) Let $f(x) = (x-9)(x^2+1) = x^3-9x^2+x-9 \in \mathbb{Z}[x]$. Then $H = 9$, and $9 + 2 = 11 > 10 = H + 1$. Moreover, $f(10) = 10^3 - 9 \cdot 10^2 + 10 - 9 = 101$ is a prime, but $f(x)$ is reducible in $\mathbb{Z}[x]$.

(2) Let $f(x) = (x-5)(x^2+1) = x^3 - 5x^2 + x - 5 \in \mathbb{Z}[x]$. Then $H = 5$, and $5 + 2 = 7 > 6 = H + 1$. Here $f(6) = 6^3 - 5 \cdot 6^2 + 6 - 5 = 37$ is a prime, but $f(x)$ is also reducible in $\mathbb{Z}[x]$.

Theorem 2.5 (Cohn's Theorem)**.** *If a prime number p is expressed in base 10 as*

$$p = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0 \quad (\textit{where } 0 \leq a_i \leq 9),$$

then the polynomial

$$f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0$$

is irreducible in $\mathbb{Z}[x]$.

Lemma 2.6. *Let* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *belong to* $\mathbb{Z}[x]$. *Suppose that* $a_n \geq 1$, $a_{n-1} \geq 0$, *and* $|a_i| \leq H$ *for* $i = 0, 1, \cdots, n-2$, *where* H *is some positive constant. Then any complex zero* α *of* $f(x)$ *either has nonpositive real part or satisfies*

$$|\alpha| < \frac{1 + \sqrt{1 + 4H}}{2}.$$

Proof. If $|z| > 1$, $\mathrm{Re}(z) > 0$ where $\mathrm{Re}(z)$ is the real part of z. Then we have

$$\begin{aligned} \left|\frac{f(z)}{z^n}\right| &= \left|a_n + \frac{a_{n-1}}{z} + \cdots + \frac{a_1}{z^{n-1}} + \frac{a_0}{z^n}\right| \\ &\geq \left|a_n + \frac{a_{n-1}}{z}\right| - \left|\frac{a_{n-2}}{z^2} + \cdots + \frac{a_1}{z^{n-1}} + \frac{a_0}{z^n}\right|. \end{aligned}$$

Note that

$$\begin{aligned} \left|\frac{a_{n-2}}{z^2} + \cdots + \frac{a_1}{z^{n-1}} + \frac{a_0}{z^n}\right| &\leq \left|\frac{a_{n-2}}{z^2}\right| + \cdots + \left|\frac{a_1}{z^{n-1}}\right| + \left|\frac{a_0}{z^n}\right| \\ &\leq \frac{H}{|z|^2} + \cdots + \frac{H}{|z|^{n-1}} + \frac{H}{|z|^n} \\ &= H\left(\frac{1}{|z|^2} + \cdots + \frac{1}{|z|^{n-1}} + \frac{1}{|z|^n}\right) \\ &= H \times \frac{\frac{1}{|z|^2}\left(1 - \frac{1}{|z|^{n-1}}\right)}{1 - \frac{1}{|z|}} \\ &= H \times \frac{\frac{1}{|z|^2} - \frac{1}{|z|^{n+1}}}{1 - \frac{1}{|z|}} \end{aligned} \tag{2.2}$$

$$\begin{aligned} &= H \times \frac{|z|^{n-1}-1}{|z|^{n+1}-|z|^n} \\ &= H \times \frac{|z|^{n-1}-1}{|z|^{n-1}\left(|z|^2-|z|\right)} \\ &< \frac{H}{|z|^2-|z|}. \end{aligned}$$

Assume $\mathrm{Re}(z) > 0$.

Let $z = a + bi$, $a, b \in \mathbb{R}$, $a > 0$ and $|z| > 1$, $a_n \geq 1$, $a_{n-1} \geq 0$. Then

$$\begin{aligned} \mathrm{Re}\left(a_n + \frac{a_{n-1}}{z}\right) &= \mathrm{Re}\left(a_n + \frac{a_{n-1}\,(a-bi)}{a^2+b^2}\right) \\ &= a_n + \frac{a \cdot a_{n-1}}{a^2+b^2} \\ &\geq a_n \geq 1, \quad \textit{and} \end{aligned} \tag{2.3}$$

$$\frac{|z|^2-|z|-H}{|z|^2-|z|} \geq 0 \Leftrightarrow |z|^2-|z|-H \geq 0 \quad \left(\because |z|^2 > |z| > 1\right). \tag{2.4}$$

By equations (2.2), (2.3), (2.4), we obtain

$$\begin{aligned} \left|\frac{f(z)}{z^n}\right| &= \left|a_n + \frac{a_{n-1}}{z} + \cdots + \frac{a_1}{z^{n-1}} + \frac{a_0}{z^n}\right| \\ &\geq \left|a_n + \frac{a_{n-1}}{z}\right| - \left|\frac{a_{n-2}}{z^2} + \cdots + \frac{a_1}{z^{n-1}} + \frac{a_0}{z^n}\right| \\ &> \mathrm{Re}\left(a_n + \frac{a_{n-1}}{z}\right) - \frac{H}{|z|^2-|z|} \\ &\quad \left(\because |a+bi| = \sqrt{a^2+b^2} \geq |a| \geq \mathrm{Re}\,(a+bi)\right) \\ &\geq 1 - \frac{H}{|z|^2-|z|} \quad (\because \text{equation(2.3)}) \\ &= \frac{|z|^2-|z|-H}{|z|^2-|z|} \geq 0 \quad (\because \text{equation(2.4)}) \end{aligned} \tag{2.5}$$

whenever

$$|z| \geq \frac{1+\sqrt{1+4H}}{2} > 1 \quad (\because H > 0)\,.$$

Now suppose $|\alpha| > 1$ and $\mathrm{Re}(\alpha) > 0$.

Then $|\alpha| \geq \dfrac{1+\sqrt{1+4H}}{2} > \dfrac{1+\sqrt{1}}{2} = 1$, that is, by equation (2.5) $\left|\dfrac{f(\alpha)}{\alpha^n}\right| \gneq 0$. In other words, $f(\alpha) \neq 0$ for such α, and so if $f(\alpha) = 0$ and $|\alpha| > 1$, then $\mathrm{Re}(\alpha) \leq 0$.

Moreover, if $|\alpha| \leq 1$, then

$$|\alpha| \leq 1 < \frac{1+\sqrt{1+4H}}{2},$$

this means that if $f(\alpha) = 0$, $|\alpha| \leq 1$, then

$$|\alpha| \lneq \frac{1+\sqrt{1+4H}}{2},$$

which completes the proof. □

Theorem 2.7. *Let $b > 2$ and let p be a prime with b-adic expansion*

$$p = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0.$$

Then the polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ is irreducible over $\mathbb{Q}$.

Lemma 2.8. *For integer b, if $b > 2$, then*

$$1 + \sqrt{1 + 4(b-1)} \leq 2(b-1).$$

Proof.

$$\begin{aligned}
& 1+\sqrt{1+4(b-1)} \le 2(b-1) \\
\Leftrightarrow \quad & \sqrt{1+4(b-1)} \le 2(b-1)-1 \\
\Leftrightarrow \quad & \left(\sqrt{1+4(b-1)}\right)^2 \le (2b-3)^2 \\
\Leftrightarrow \quad & 1+4(b-1) \le 4b^2-12b+9 \\
\Leftrightarrow \quad & 0 \le 4b^2-16b+12 \\
\Leftrightarrow \quad & 0 \le b^2-4b+3 \\
\Leftrightarrow \quad & b \le 1 \quad \text{or} \quad b \ge 3.
\end{aligned}$$

That is, for integer $b > 2$, i.e., $b \ge 3$, then satisfies $1+\sqrt{1+4(b-1)} \le 2(b-1)$. □

Remark 2.9. Theorem 2.7 is also true for $b = 2$, as follows from Lemma 2.12 and the discussion following the proof of Theorem 2.7.

Proof of Theorem 2.7. By a celebrated lemma of Gauss(see [4]), it suffices to consider reducibility over $\mathbb{Z}[x]$. If $f(x) = g(x)h(x)$ with $g(x)$ and $h(x)$ nonconstant polynomials in $\mathbb{Z}[x]$, then $f(b) = p$ implies either $g(b) = \pm 1$ or $h(b) = \pm 1$. Without loss of generality we may assume that $g(b) = \pm 1$. As in the proof of Theorem 2.1, we write

$$g(x) = c\prod_i (x-\alpha_i),$$

where the α_i range over a certain subset of the zeros of f and c is a nonzero integer (namely, the leading coefficient of $g(x)$). Note that $0 \leq b_i \leq b-1$ for every i, and hence we can take $H = b-1$. By Lemma 2.6, every zero α of f either has nonpositive real part or has absolute value less than

$$\frac{1+\sqrt{1+4(b-1)}}{2}.$$

Assume $\alpha = c + di (c, d \in \mathbb{R})$ and $\mathrm{Re}(\alpha) = \mathrm{c} \leq 0$. Then

$$\begin{aligned} |b-\alpha| &= |b-(c+di)| \\ &= |(b-c)-di| \\ &= \sqrt{(b-c)^2+d^2} \\ &\geq \sqrt{b^2+d^2} \quad (\because c \leq 0) \\ &\geq \sqrt{b^2} = b, \end{aligned} \tag{2.6}$$

and so

$$\begin{aligned} |g(b)| &= |c|\left|\prod_i (b-\alpha_i)\right| \\ &= |c|\prod_i |(b-\alpha_i)| \\ &\geq |c| \cdot b^{\deg g(x)} \quad (\because \text{equation(2.6)}) \\ &\geq b > 1, \end{aligned}$$

a contradiction. In other words, $g(x)$ has to be a constant polynomial. Note that for integer $b > 2$, then by Lemma 2.8,

$$1+\sqrt{1+4(b-1)} \leq 2(b-1).$$

Now assume $|\alpha| < \dfrac{1+\sqrt{1+4(b-1)}}{2}$. Then

$$\begin{aligned} |\alpha| &< \frac{1+\sqrt{1+4(b-1)}}{2} \\ &\leq \frac{2(b-1)}{2} \quad (\because \text{Lemma(2.8)}) \\ &= (b-1). \end{aligned}$$

In particular,

$$\begin{aligned} |b-\alpha_i| &\geq |b| - |\alpha_i| \\ &> b-(b-1) = 1 \end{aligned}$$

for every i. Thus

$$\begin{aligned} |g(b)| &= |c|\left|\prod_i (b-\alpha_i)\right| \\ &\geq \prod_i |b-\alpha_i| > 1, \end{aligned}$$

which is a contradiction. Therefore, $f(x)$ is irreducible in $\mathbb{Z}[x]$, as we wanted. □

Example 2.10. (1) Let $b = 6$ and $p = 131$. Then $131 = 108+18+5 = 3\cdot 6^2+3\cdot 6+5$, i.e., the polynomial $f(x) = 3x^2+3x+5$ is irreducible over $\mathbb{Q}$.

(2) Let $b = 16$ and $p = 709$. Then $709 = 512+192+5 = 2\cdot 16^2+12\cdot 16+5$, i.e., the polynomial $f(x) = 2x^2+12x+5$ is irreducible over $\mathbb{Q}$.

(3) Let $b = 12$ and $p = 4481$. Then $4481 = 3456 + 1008 + 12 + 5 = 2\cdot 12^3 + 7\cdot 12^2 + 12 + 5$, i.e., the polynomial $f(x) = 2x^3 + 7x^2 + x + 5$ is irreducible over $\mathbb{Q}$.

Lemma 2.11. *Let α be a root of the polynomial*

$$x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0,$$

where the coefficients $c_0, c_1, \cdots, c_{n-1}$ are integers. Then α is either an integer or an irrational number.

Lemma 2.12. *Suppose that α is a complex root of a polynomial*

$$f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$$

with cofficients a_i equal to 0 or 1. If $|\arg\alpha| \le \frac{\pi}{4}$, then $|\alpha| < \frac{3}{2}$. Otherwise $\mathrm{Re}(\alpha) < \frac{1+\sqrt{5}}{2\sqrt{2}} < \frac{3}{2} < \frac{1+\sqrt{5}}{2}$.

Proof. Case 1. $m = 1$. $f(x) = x$ or $x + 1$. Then $\alpha = 0$ or -1, that is, $|0| = 0 < \frac{3}{2}$ and $\mathrm{Re}(-1) = -1 < \frac{1+\sqrt{5}}{2\sqrt{2}}$.

Case 2. $m = 2$. $f(x) = x^2$, $x^2 + x$, $x^2 + 1$, $x^2 + x + 1$. Then $\alpha = 0$, -1, $\pm i$, $\frac{-1 \pm \sqrt{3}i}{2}$, that is, $|0| = 0 < \frac{3}{2}$, $\mathrm{Re}(-1) = -1 < \frac{1+\sqrt{5}}{2\sqrt{2}}$,

$$\mathrm{Re}(\pm i) = 0 < \frac{1+\sqrt{5}}{2\sqrt{2}}, \text{ and } \mathrm{Re}\left(\frac{-1\pm\sqrt{3}i}{2}\right) = -\frac{1}{2} < \frac{1+\sqrt{5}}{2\sqrt{2}}.$$

Now suppose $m \geq 3$, we compute for $|z| > 1$. Note that if $f(0) = 0$, that is, $a_0 = 0$, $f(x) = x$. Hence $a_0 \neq 0$, i.e., $f(0) \neq 0$.

$$\begin{aligned}
\left|\frac{f(z)}{z^m}\right| &= \left|1 + \frac{a_{m-1}}{z} + \frac{a_{m-2}}{z^2} + \cdots + \frac{a_1}{z^{m-1}} + \frac{a_0}{z^m}\right| \\
&\geq \left|1 + \frac{a_{m-1}}{z} + \frac{a_{m-2}}{z^2}\right| - \left|\frac{a_{m-3}}{z^3} + \cdots + \frac{a_1}{z^{m-1}} + \frac{a_0}{z^m}\right| \\
&\geq \left|1 + \frac{a_{m-1}}{z} + \frac{a_{m-2}}{z^2}\right| - \left(\left|\frac{a_{m-3}}{z^3}\right| + \cdots + \left|\frac{a_1}{z^{m-1}}\right| + \left|\frac{a_0}{z^m}\right|\right) \\
&\geq \left|1 + \frac{a_{m-1}}{z} + \frac{a_{m-2}}{z^2}\right| - \left(\frac{1}{|z|^3} + \cdots + \frac{1}{|z|^{m-1}} + \frac{1}{|z|^m}\right).
\end{aligned}$$

Note that

$$\begin{aligned}
\frac{1}{|z|^3} + \cdots + \frac{1}{|z|^{m-1}} + \frac{1}{|z|^m} &= \frac{\frac{1}{|z|^3}\left(1 - \frac{1}{|z|^{m-2}}\right)}{1 - \frac{1}{|z|}} \\
&= \frac{\frac{1}{|z|^3} - \frac{1}{|z|^{m+1}}}{1 - \frac{1}{|z|}} \\
&= \frac{|z|^{m-2} - 1}{|z|^{m+1} - |z|^m} \\
&= \frac{|z|^{m-2} - 1}{|z|^{m-2}\left(|z|^3 - |z|^2\right)} \\
&< \frac{1}{|z|^2(|z| - 1)} \quad (\because |z| > 1).
\end{aligned} \tag{2.7}$$

For z satisfying $|\arg z| \leq \frac{\pi}{4}$ it is true that $\mathrm{Re}(z) > 0$ and hence $\mathrm{Re}\left(1 + \frac{a_{m-1}}{z} + \frac{a_{m-2}}{z^2}\right) = 1 + \mathrm{Re}\left(\frac{a_{m-1}}{z}\right) + \mathrm{Re}\left(\frac{a_{m-2}}{z^2}\right) > 1$. Thus, for such z, we have

$$\begin{aligned}
\left|\frac{f(z)}{z^m}\right| &\geq \left|1 + \frac{a_{m-1}}{z} + \frac{a_{m-2}}{z^2}\right| - \left(\frac{1}{|z|^3} + \cdots + \frac{1}{|z|^{m-1}} + \frac{1}{|z|^m}\right) \\
&> \mathrm{Re}\left(1 + \frac{a_{m-1}}{z} + \frac{a_{m-2}}{z^2}\right) - \left(\frac{1}{|z|^3} + \cdots + \frac{1}{|z|^{m-1}} + \frac{1}{|z|^m}\right) \\
&= \mathrm{Re}\left(1 + \frac{a_{m-1}}{z} + \frac{a_{m-2}}{z^2}\right) - \left(\frac{|z|^{m-2} - 1}{|z|^{m-2}\left(|z|^3 - |z|^2\right)}\right) \\
&> 1 - \left(\frac{|z|^{m-2} - 1}{|z|^{m-2}\left(|z|^3 - |z|^2\right)}\right) \\
&> 1 - \frac{1}{|z|^2(|z| - 1)} \quad (\because \text{equation(2.7)}) \\
&= \frac{|z|^3 - |z|^2 - 1}{|z|^2(|z| - 1)}.
\end{aligned}$$

The polynomial $f(x) = x^3 - x^2 - 1$ has exactly one real root, and this root is less than $\frac{3}{2}$.

Indeed, the derivative of this function is $3x^2 - 2x = x(3x - 2)$, revealing that $x^3 - x^2 - 1$ has negative slope only for x in $\left(0, \frac{3}{2}\right)$. Since the value of $x^3 - x^2 - 1$ at $x = \frac{3}{2}$ is positive, i.e., $f\left(\frac{3}{2}\right) = \left(\frac{3}{2}\right)^3 - \left(\frac{3}{2}\right)^2 - 1 = \frac{1}{8}$, the one real root lies in the open interval $\left(\frac{2}{3}, \frac{3}{2}\right)$.

If $|z| \geq \frac{3}{2}$, then

$$\left|\frac{f(z)}{z^m}\right| > \frac{|z|^3 - |z|^2 - 1}{|z|^2(|z| - 1)} > 0 \quad \text{for} \quad |\arg z| \leq \frac{\pi}{4}.$$

Therefore, $|f(z)| > 0$ for $|z| \geq \frac{3}{2}$ and $|\arg z| \leq \frac{\pi}{4}$, whence the first part of the lemma is established.

For the second part, we separate the condition by two parts, i.e., $|\arg \alpha| \geq \frac{\pi}{2}$, i.e., $\mathrm{Re}(\alpha) \leq 0$ or $\frac{\pi}{4} < |\arg \alpha| \lneq \frac{\pi}{2}$. However, if $|\arg \alpha| > \frac{\pi}{2}$, then $\mathrm{Re}(\alpha) \leq 0 < \frac{1+\sqrt{5}}{2\sqrt{2}}$. So it suffices to verify the case $\frac{\pi}{4} < |\arg \alpha| < \frac{\pi}{2}$. Note that $|\alpha| < \frac{1+\sqrt{5}}{2}$ by Lemma 2.6 in this case. It is not difficult to see that these conditions force $\mathrm{Re}(\alpha)$ to be smaller than $\frac{1+\sqrt{5}}{2\sqrt{2}}$. This completes the proof.

Hence for such an α and $\frac{\pi}{4} \lneq |\arg \alpha| < \frac{\pi}{2}$, $\mathrm{Re}(\alpha) = |\alpha| \cos\theta \lneq |\alpha| \frac{1}{\sqrt{2}} < \frac{1+\sqrt{5}}{2\sqrt{2}}$, which completes the proof. □

Theorem 2.13. *Let $b = 2$ and p be a prime with 2-adic expansion*

$$p = a_n 2^n + \cdots + a_1 2 + a_0.$$

Then the polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ is irreducible over $\mathbb{Q}$.

Proof. Since $b = 2$ and p be a prime with 2-adic expansion

$$p = a_n 2^n + \cdots + a_1 2 + a_0,$$

$f(x) = a_n x^n + \cdots + a_1 x + a_0$, and we have $a_i = 0$ or 1, and $H = 1$.

$f(2)$ is a prime, that is, $f(2) = a_n 2^n + \cdots + a_1 2 + a_0 = p$ is a prime.

If $a_0 = 0$, then

$$\begin{aligned} f(2) &= a_n 2^n + \cdots + a_2 2^2 + a_1 2 \\ &= 2(a_n 2^{n-1} + \cdots + a_2 2 + a_1) \\ &= p, \end{aligned}$$

which is a prime, that is, $p = 2$, and $a_n 2^{n-1} + \cdots + a_2 2 + a_1 = 1$, so $a_1 = 1$, $a_i = 0\,(i \geq 2)$. Thus $f(x) = x$ is irreducible.

Hence, if $p > 2$, then a_0 cannot be zero. If $f(x)$ has any rational roots, they can only be ± 1. Since $f(1) = a_n + \cdots + a_1 + a_0 > a_0 = 1$, $x = 1$ is not a root.

If $0 = f(-1)$, then

$$0 = f(-1) \equiv f(2) \equiv p \pmod 3 \quad (\because -1 \equiv 2 \pmod 3),$$

implying that $p = 3$ and $f(x) = x + 1$, which is irreducible.

Thus when $p > 3$, $f(x)$ has no rational root, i.e., only irrational roots α_i. Hence, by Lemma 2.6, α_i has $\mathrm{Re}(\alpha_i) \leq 0$ or satisfies $|\alpha_i| < \dfrac{(1 + \sqrt{1 + 4H})}{2} = \dfrac{(1 + \sqrt{5})}{2}$.

If $f(x) = g(x)h(x)$ with $g(x)$ and $h(x)$ nonconstant polynomials in $\mathbb{Z}[x]$, then $f(b) = p$ implies either $g(b) = \pm 1$ or $h(b) = \pm 1$. Without loss of generality we may assume that $g(b) = \pm 1$. As in the proof of Theorem 2.1, we write

$$g(x) = c \prod_i (x - \alpha_i),$$

where the α_i range over a certain subset of the zeros of f and c is a nonzero integer (namely, the leading coefficient of $g(x)$).

We may assume that $f(\alpha_i) = 0$ satisfy $\mathrm{Re}(\alpha_i) < v$ by Lemma 2.6. Then it is readily seen that the coefficients of the polynomial

$$g(x+v) = c\prod_i (x+v-\alpha_i),$$

are all nonnegative.

Indeed, if α_i is real, then $\mathrm{Re}(\alpha_i) = \alpha_i < v$. That is, $x+v-\alpha_i > 0$ has nonnegative coefficients.

If α_i is not real, we pair it with its complex conjugate and notice that

$$\begin{aligned}(x+v-\alpha_i)(x+\overline{v-\alpha_i}) &= (x+v-\alpha_i)(x+v-\overline{\alpha}_i)\\ &= x^2 + 2\mathrm{Re}(v-\alpha_i)x + |v-\alpha_i|^2\end{aligned} \tag{2.8}$$

has nonnegative coefficients. Observe that $g(x)$ is a polynomial with real coefficients and therefore, if α is a root of $g(x)$, so is $\overline{\alpha}$.

As v is real, the same property applies to the polynomial $g(x+v)$. Because $g(x+v)$ is a product of polynomials of equation (2.8), it is a polynomial in x with nonnegative coefficients. Hence $g(-x+v)$ is a polynomial with alternating coefficients. Thus, for any $x > 0$, we have $\pm g(-x+v) < g(x+v)$. Therefore, $|g(-x+v)| < g(x+v)$.

If $v < b$, then we set $x = b - v > 0$ to deduce that

$$|g(-x+v)| < g(x+v) \quad \text{for} \quad x > 0 \quad \Rightarrow \quad |g(-b+2v)| < g(b).$$

If $v = \frac{3}{2} < 2 = b$, then

$$g(-b + 2v) = g(1) \quad \text{and} \quad g(b) = g(2)$$

$$1 \leq |g(1)| < g(2) \quad (\because |g(1)| \neq 0, \quad \text{integer}).$$

Therefore, $g(2) \neq \pm 1$, a contradiction.

The proof of Theorem 2.7 then applies to establish the irreducibility of $f(x)$.

However, the bound given by Theorem 2.1 is

$$\begin{aligned} \frac{(1+\sqrt{1+4H})}{2} &= \frac{(1+\sqrt{1+4(b-1)}}{2} \\ &= \frac{(1+\sqrt{5})}{2} \\ &> \frac{3}{2} = v. \end{aligned}$$

This suggests the following refinement of Lemma 2.6. It is all that is required to extend the proof of Theorem 2.7 so as to cover the case $b = 2$. □

Example 2.14. (1) Let $b = 2$ and p be a prime with 2-adic expansion. Since $17 = 16 + 1 = 2^4 + 1$ is a prime, we see that the polynomial $f(x) = x^4 + 1$ is irreducible over $\mathbb{Q}$.

(2) Let $b = 2$ and let $p = 97$. Then $97 = 64 + 32 + 1 = 2^6 + 2^5 + 1$, i.e., the polynomial $f(x) = x^6 + x^5 + 1$ is irreducible over $\mathbb{Q}$.

(3) Let $b = 2$ and let $p = 107$. Then $107 = 64 + 32 + 8 + 2 + 1 = 2^6 + 2^5 + 2^3 + 2 + 1$, i.e., the polynomial $f(x) = x^6 + x^5 + x^3 + x + 1$ is irreducible over $\mathbb{Q}$.

References

[1] G. Pólya and G. Szegö *Problems and Theorems in Analysis* , Forth Edition, *Springer-Verlag New York Heidelberg Berlin*, (1976)

[2] Kenneth H. Rosen, *Elementary Number Theory and Its Applications*, Fifth Edition, *Addison Wesley*, (2005)

[3] M. Ram Murty, *Prime Numbers and Irredueible Polynomials*, The American Mathematical Monthly **109**, (2002), pp. 452–458.

[4] S. Lang, *Algebra*, 3rd ed., *Addison Wesley*, Reading, MA, (1993)

Abstract

Irreducible Polynomials in $\mathbb{Z}[x]$

Chang Seo Yeon
Major in Mathematics Education
Graduate school of Education
Sungshin Women's University
supervised by professor Shin Yong Su Ph.D.

If we express a prime p in base $b \geq 2$ as $p = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b^1 + a_0$, then the polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x^1 + a_0$ is necessarily irreducible in $\mathbb{Z}[x]$.

In this thesis, we reprove adding precise details about this theorem and using this result, we make an example for a prime number p in base $b = 2$ and $b > 2$.