Advances in Algebra (AA).
ISSN 0973-6964 Volume 15, Number 1 (2022), pp. 5-8

http://www.ripublication.com/aa.htm

Two Extensions of Eisenstein's Criterion

Francesco Laudano, Liceo classico Mario Pagano
Via Scardocchia Campobasso - Italia - 86100

Abstract

We propose two extensions of Eisenstein's irreducibility criterion.

Keywords: Eisenstein's criterion, Polynomial Irreducibility

2020 Mathematics Subject Classification: 12E05; 11R09

1. INTRODUCTION

Probably the best-known result about polynomials irreducibility is Schöne-mann Eisenstein's criterion ([2, §61 p. 100] and [3, p. 166]). Eisenstein's version, published in 1850, provided a sufficient condition for the irreducibility that depends on the divisibility properties of polynomial's coefficients.

In these paper we provide two extensions of Eisenstein's criterion (Theorem 1 and Theorem 2), along the line of the generalization given in [4, Theorem 1, p. 1159] and [5, Theorem 2, p. 154].

2. THEOREMS AND APPLICATIONS

Let m be an integer with $m \geq 2$. We say an integer polynomial $f(x)$ is "m-irreducible" in $\mathbb{Z}[x]$ (respectively in $\mathbb{Q}[x]$) if it cannot be expressed as a product of m nonconstant integer polynomials. Otherwise, we say that $f(x)$ is m-reducible in $\mathbb{Z}[x]$ (respectively in $\mathbb{Q}[x]$).

We recall that, for Gauss's lemma, if an integer polynomial can be factored into two nonconstant rational polynomials, then it can be factored into two nonconstant integer polynomials ([1, Article 42 p. 37]). The following extension of Gauss's lemma can be proved by induction.

Lemma 1. *Let $g(x) \in \mathbb{Z}[x]$ be a polynomial. If $g(x) = G_1(x)G_2(x)\dots G_m(x)$, a factorization in $\mathbb{Q}[x]$, then there is a factorization $g(x) = g_1(x)g_2(x)\dots g_m(x)$ in $\mathbb{Z}[x]$, whit $g_i = c_iG_i$, with $c_i \in F$ for $i = 1, 2, \dots, m$.*
Therefore, if $g(x)$ is m-irreducible in $\mathbb{Z}[x]$, then $g(x)$ is m-irreducible in $\mathbb{Q}[x]$.

Now we attempt to extend Schönemann-Eisenstein's criterion ([2, §61 p. 100] and [3, p. 166]) to provide a simple condition for m-irreducibility.

Theorem 1. *Let $f(x) = a_nx^n + \dots + a_0 \in \mathbb{Z}[x]$ be a polynomial and suppose there is a prime p such that p does not divide a_n, p divides a_i for $i = 0, 1, \dots, n-1$, and for some m with $2 \le m \le n$, p^m does not divide a_0, then $f(x)$ is m-irreducible in $\mathbb{Q}[x]$. In particular, for a primitive polynomial $f(x)$, if $m = 2$, then f(x) is irreducible.*

Proof. Assume that there are m nonconstant integer polynomials

$$g_1(x) = \sum_{k=0}^{r_1} a_{k,1}x^k,\ g_2(x) = \sum_{k=0}^{r_2} a_{k,2}x^k, \dots,\ g_m(x) = \sum_{k=0}^{r_m} a_{k,m}x^k$$

with $n = r_1 + r_2 + \dots + r_m$ and $r_j > 0$, such that $f(x) = g_1(x)g_2(x)\cdots g_m(x)$.

Since $p \mid a_0$ and $p^m \nmid a_0$, there are $m_1, m_2 \in \{1, 2, \dots, m\}$ such that $p \mid a_{0,m_1}$ and $p \nmid a_{0,m_2}$. Then, we have $\emptyset \neq D = \{i \in \{1, 2, \dots, m\} : p \mid a_{0,i}\} \neq \{1, 2, \dots, m\}$. Thus we can assume $D = \{1, 2, \dots, s\}$, in fact, if this were not the case, we could permute the polynomials $g_1(x), g_2(x), \dots, g_m(x)$ so that the first s polynomials have indices in $\{1, 2, \dots, s\}$.

Let $K_j = \{k \in \mathbb{N},\ 1 \le k \le r_j : p \nmid a_{k,j}\}$ for $j = 1, 2, \dots, s$. Since $p \nmid a_n = a_{r_1,1}a_{r_2,2}\cdots a_{r_m,m}$, it follows that $K_j \neq \emptyset$, then there exist the natural $\overline{k}_j = \min(K_j)$. Therefore, being $s < m$ and $r_j > 0$, we have $\overline{k}_1 + \overline{k}_2 + \dots + \overline{k}_s \le r_1 + r_2 + \dots + r_s < r_1 + r_2 + \dots + r_s + r_{s+1} + \dots + r_m = n$. Then $p \mid a_{\overline{k}_1+\overline{k}_2+\dots+\overline{k}_s}$, because, by the hypothesis, p divides a_i for $i = 0, 1, \dots, n-1$.

On the other hand, we have

$$a_{\overline{k}_1+\overline{k}_2+\dots+\overline{k}_s} = \sum_{\substack{k_1+k_2+\dots+k_m=\overline{k}_1+\overline{k}_2+\dots+\overline{k}_s \\ 0\le k_j\le r_j}} a_{k_1,1}a_{k_2,2}\cdots a_{k_m,m}\ ,$$

where the summands having at least one index $j \in \{1, 2, ..., s\}$ such that $k_j < \overline{k}_j$ are multiple of p. Then, p also divides the remaining summand, i.e. $a_{\overline{k}_1,1}a_{\overline{k}_2,2}\cdots a_{\overline{k}_s,s}a_{0,s+1}\cdot\cdot a_{0,m}$, and this is a contradiction. Lemma 1 ensures m-irreducibility in $\mathbb{Q}[x]$. □

Corollary 1.1. *Let $f(x) = ax^n + a_{n-1}p^{r_1}x^{n-1} + \cdots + a_1p^{r_{n-1}}x + p^{m-1}$ be an integer polynomial where $2 \leq m \leq n$, p is a prime that does not divide a and each $r_i > 0$. Then $f(x)$ has at most $m-2$ rational roots.*

Proof. By Theorem 1, $f(x)$ is m-irreducible in $\mathbb{Q}[x]$. If $f(x)$ had $m-1$ rational roots, it would have $m-1$ linear factors. Since $n = \deg(f(x)) > m-1$, $f(x)$ would also have another non-constant factor, so it would be m-reducible in $\mathbb{Q}[x]$, a contradiction. □

The following theorem provides another extension of Eisenstein's criterion along the line of the generalization given in [4, Theorem 1, p. 1159] and [5, Theorem 2, p. 154].

Theorem 2. *Let $f(x) = a_nx^n + \cdots + a_0 \in \mathbb{Z}[x]$ be a polynomial of degree n and suppose there is a prime p and an integer h with $n/2 \leq h < n$ such that p divides a_i for $i = 0, 1, \ldots, h$, p does not divide a_{h+1} and p^2 does not divide a_0.*

If $f(x) = g_1(x)g_2(x)$, a factorization in $\mathbb{Z}[x]$, then $\min\{\deg(g_1(x)), \deg(g_2(x))\} \leq n-h-1$. In particular, for a primitive polynomial $f(x)$, if $h = n-1$, then $f(x)$ is irreducible, and if $f(x)$ has only trivial factors of degree less than $n-h$ in $\mathbb{Z}[x]$, then $f(x)$ is irreducible.

Proof. Assume that $f(x) = g_1(x)g_2(x)$, a factorization in $\mathbb{Z}[x]$, where $g_1(x) = b_0 + b_1x + \cdots + b_kx^k$ and $g_2(x) = c_0 + c_1x + \cdots + c_{n-k}x^{n-k}$ with $h \geq k \geq n/2$.

By the hypothesis $p \nmid a_{h+1}$, there are the smallest indices $\overline{i}$ and $\overline{j}$ for which $p \nmid b_{\overline{i}} \cdot c_{\overline{j}}$.

Note that $a_{\overline{i}+\overline{j}} = \sum_{i+j=\overline{i}+\overline{j}} b_ic_j$, where p divides any summand except $b_{\overline{i}} \cdot c_{\overline{j}}$, then $p \nmid a_{\overline{i}+\overline{j}}$. Since the smallest coefficient of $f(x)$ that is not a multiple of p is a_{h+1}, we have $\overline{i} + \overline{j} \geq h+1$, then $\overline{i} \geq h+1-\overline{j}$ and $\overline{j} \geq h+1-\overline{i}$.

On the other and, since $\overline{i} \leq \deg g_1(x) = k \leq h$ and $\overline{j} \leq \deg(g_2(x)) = n-k \leq k \leq h$, we have:

$$h+1-\overline{j} \leq \overline{i} \leq h \quad \text{and} \quad h+1-\overline{i} \leq \overline{j} \leq h.$$

Then $\overline{i}$ and $\overline{j}$ are both nonzero. In other words, p divides both b_0 and c_0, and this is a contradiction, because $p^2 \nmid a_0 = b_0c_0$.

Since $f(x)$ has no factors of degree k with $n/2 \leq k \leq h$, then $f(x)$ does not even have factors of degree $n-k$. Therefore, being $n/2 \geq n-k \geq n-h$, f(x) does not have factors of degree k with $n-h \leq k \leq h$ in $\mathbb{Z}[x]$. □

In the line of [4, Corollary 2, p. 1160] we can prove the following Corollary.

Corollary 2.1. *Let $f(x) = x^p - ax^{p-1} + p \in \mathbb{Z}[x]$, where $p \geq 5$ is a prime which does not divide a. Then $f(x)$ is not solvable by radicals.*

Proof. Setting $h = p - 2$, by Theorem 2, $f(x)$ does not have factors of degree k with $2 \leq k \leq p - 2$. Moreover we can check that $f(x)$ does not have rational roots, then, being primitive, $f(x)$ is irreducible in $\mathbb{Q}[x]$. Using elementary arguments you can also prove that $f(x)$ has exactly 3 real roots. The thesis follows applying [6, Proposition VIII]. □

REFERENCES

[1] C. F. Gauss, *Disquisitiones Arithmeticae*, Leipzig, 1801.

[2] T. Schönemann, Von denjenigen Moduln, welche Potenzen von Primzahlen sind, *J. reine angew. Math.* 32 (1846), pp. 93-105.

[3] F. G. M. Eisenstein, Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt, *J. reine angew. Math.* 39 (1850), pp. 160-179.

[4] S. H. Weintraub, A mild generalization of Eisenstein's criterion, *Proc. Am. Math. Soc.* 141(4) (2013), pp. 1159-1160.

[5] C. R. Fletcher, 74.21 Eisenstein generalized, *Math. Gaz.* 74(468) (1990), pp. 153-156.

[6] E. Galois, Mémoire sur les conditions de résolubilité des équations par radicaux, *J. Math. Pure Appl.* 11 (1846), pp. 381-444.