A MILD GENERALIZATION OF EISENSTEIN'S CRITERION

STEVEN H. WEINTRAUB

ABSTRACT. We state and prove a mild generalization of Eisenstein's Criterion for a polynomial to be irreducible, correcting an error that Eisenstein made himself.

Eisenstein originally stated and proved the irreducibility criterion we now name after him in [2]. Both his statement and proof are virtually identical to how we would formulate them today. In that paper Eisenstein was actually concerned with the lemniscate, where the relevant question was irreducibility of polynomials with coefficients in the Gaussian integers, rather than in the ordinary integers, but, as he observed, the statement and proof are identical in either case. Indeed, in [2], he applied his citerion to show that, for a prime p, the p-th cyclotomic polynomial $\Phi_p(x) = (x^p - 1)/(x - 1)$ is irreducible. He used the same trick we still use today, observing that his criterion applies to the polynomial $\Phi_p(x+1)$. The first proof of the irreducibility of $\Phi_p(x)$ had been given by Gauss [4, Article 341], with a simpler proof having been given by Kronecker [5], but Eisenstein's proof was simpler still. Also, as Eisenstein observed, Gauss's and Kronecker's proofs used particular properties of p-th roots of 1, and so only could be applied to $\Phi_p(x)$, while his criterion applies far more generally. (Actually, Schönemann had given an irreducibility criterion in [6] that is easily seen to be equivalent to Eisenstein's criterion, and had used it to prove the irreducibility of $\Phi_p(x)$, but this had evidently been overlooked by Eisenstein; for a discussion of this see [1].)

Eisenstein then went on to remark that the proof of his criterion goes through to show the following more general result: *Let $f(x) = a_n x^n + \ldots + a_0$ be any primitive polynomial with integer coefficients and suppose there is a prime p such that p does not divide a_n, p divides a_i for $i = 0, \ldots, n-1$, and for some k with $0 \leq k \leq n-1$, p^2 does not divide a_k. Then $f(x)$ is irreducible (in $\mathbb{Z}[x]$).* However, this claim is false, as we see from the following factorization, valid for any $k \geq 1$ and any $m \geq 0$: $(x^k + p)(x^{k+m} + (p^2 - p)x^m + p) = x^{2k+m} + p^2 x^{k+m} + (p^3 - p^2)x^m + px^k + p^2$. The point of this note is to establish a correct result along these lines.

Theorem 1. *Let $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$ be a polynomial and suppose there is a prime p such that p does not divide a_n, p divides a_i for $i = 0, \ldots, n-1$, and for some k with $0 \leq k \leq n-1$, p^2 does not divide a_k. Let k_0 be the smallest such value of k. If $f(x) = g(x)h(x)$, a factorization in $\mathbb{Z}[x]$, then $\min(\deg(g(x)), \deg(h(x))) \leq k_0$. In particular, for a primitive polynomial $f(x)$, if $k_0 = 0$ then $f(x)$ is irreducible, and if $k_0 = 1$ and $f(x)$ does not have a root in $\mathbb{Q}$, then $f(x)$ is irreducible.*

Proof. Suppose we have a factorization $f(x) = g(x)h(x)$. Let $g(x)$ have degree d_0 and $h(x)$ have degree e_0. Let d be the smallest power of x whose coefficient in $g(x)$ is not divisible by

2000 *Mathematics Subject Classification.* 12E05, Secondary 01A55.
Key words and phrases. Eisenstein's criterion, irreducibility.

p, and similarly for e and $h(x)$. Then $g(x) = x^d g_1(x) + pg_2(x)$ and $h(x) = x^e h_1(x) + ph_2(x)$ for polynomials $g_1(x), g_2(x), h_1(x), h_2(x) \in \mathbb{Z}[x]$, with the constant terms of $g_1(x)$ and $h_1(x)$ not divisible by p. Then

$$f(x) = g(x)h(x) = x^{d+e} g_1(x)h_1(x) + p(x^e h_1(x)g_2(x) + x^d h_2(x)g_1(x)) + p^2 g_2(x)h_2(x).$$

The condition that all of the coefficients of $f(x)$ except a_n be divisible by p forces $d+e = n$ and hence $d = d_0$ and $e = e_0$. Thus $g(x) = b_{d_0}x^{d_0} + pg_2(x)$ and $h(x) = c_{e_0}x^{e_0} + ph_2(x)$, in which case

$$f(x) = g(x)h(x) = a_n x^n + ph_2(x)b_{d_0}x^{d_0} + pg_2(x)c_{e_0}x^{e_0} + p^2 g_2(x)h_2(x),$$

and so $k_0 \geq \min(d_0, e_0)$. □

Corollary 2. *Let $p \geq 5$ be prime and let $f_0(x) = x^p - p^p x + p$ and $f_1(x) = x^p - p2^p x + p^2$. Then neither $f_0(x)$ nor $f_1(x)$ is solvable by radicals.*

Proof. Let $f(x) = f_0(x)$ or $f_1(x)$. By Theorem 1, $f(x)$ is irreducible, and it is easy to check that $f(x)$ has exactly 3 real roots. We now apply Galois's original criterion for an equation to be solvable by radicals [3, Proposition VIII]: *An irreducible equation of prime degree is solvable by radicals if and only if each of its roots can be expressed as a rational function of any two of them.* □

REFERENCES

[1] Cox, D. A. Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it first, Normat 57 (2009), 49-73.

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

[3] Galois, E., Mémoire sur les conditiona de résolubilité des équations par radicaux, J. math. pure appl. 11 (1846), 381-444.

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

[5] Kronecker, L., Beweis dass für jede Primzahl p die Gleichung $1 + x + \ldots + x^{p-1} = 0$ irreductibel ist, J. reine angew. Math. 29 (1845), 280.

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

DEPARTMENT OF MATHEMATICS, LEHIGH UNIVERSITY, BETHLEHEM, PA 18015-3174, USA
E-mail address: shw2@lehigh.edu