Eisenstein Criterion for Irreducibility of a Polynomial : Algebra

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/

2 June, 2023 (at *20:24*)

ABSTRACT: Proofs of Eisenstein Criterion and the Gauss Lemma.

Nomenclature. Use[♡1] ***poly*** for "polynomial" and ***coeff*** for "coefficient". I will be considering three polys,

1:
$$\begin{aligned} \alpha(x) &= A_0 + A_1 x + A_2 x^2 + \cdots + A_J x^J , \\ \beta(x) &= B_0 + B_1 x + \cdots + B_K x^K , \\ \mu(x) &= M_0 + M_1 x + M_2 x^2 + \cdots + M_L x^L , \end{aligned}$$

with each of A_J, B_K, M_L non-zero.

My convention is that later coefficients are all defined, and equal zero; so $0 = M_{L+1} = M_{L+2}, \ldots$. An ***intpoly*** is a poly whose coefficients are integers. A ***ratpoly*** has rational coefficients. Traditionally, the symbol $\mathbb{Z}[x]$ is used for the set of intpolys, and $\mathbb{Q}[x]$ for the collection of ratpolys. These sets are rings.

A poly α is "a ***unit***" in $\mathbb{Z}[x]$, if its reciprocal is also in $\mathbb{Z}[x]$. There are only two units in $\mathbb{Z}[x]$; the constant polys ± 1. In $\mathbb{Q}[x]$, however, each constant poly $x \mapsto q$ is a unit, where q ranges over the non-zero rationals.

[♡1] Use $\equiv_N$ to mean "congruent mod N". Let $n \perp k$ mean that n and k are co-prime [no prime in common].

Use $k \mid n$ for "k divides n". Its negation $k \nmid n$ means "k does not divide n." Use $n \,|\!\bullet\, k$ and $n \nmid k$ for "n is/is-not a multiple of k." Finally, for p a prime and E a natnum: Use double-verticals, $p^E \parallel n$, to mean that E is the ***highest*** power of p which divides n. Or write $n \parallel p^E$ to emphasize that this is an assertion about n. Use ***PoT*** for Power of Two and ***PoP*** for Power of (a) Prime.

A poly μ is "***irreducible*** over $\mathbb{Z}$" if, whenever it can be factored into intpolys $\mu = \alpha\beta$, then either α or β is a unit (in $\mathbb{Z}[x]$). Thus $6x - 15$ is reducible over $\mathbb{Z}$, since

2:
$$6x - 15 = 3 \cdot [2x - 5] .$$

However $6x - 15$ is irreducible over $\mathbb{Q}$, since 3 is a $\mathbb{Q}$-unit.

Reversing a poly. Below is a "trivial" factoring result; I put it here so that we can apply the Eisenstein criterion to it later.

Say that a poly μ is ***good*** if its constant term is non-zero. The ***reversal*** of a deg-L good μ is

$$M_L + M_{L-1}x + M_{L-2}x^2 + \cdots + M_1 x^{L-1} + M_0 x^L ,$$

denoted by $\overleftarrow{\mu}(x)$. On the set of good polys, "reversal" is an involution.

If a good poly factors as $\mu = \alpha\beta$, then evidently each of α, β is good.

3: Reverse factor lemma. (*Here "factorization" and "irreducible" mean over $\mathbb{Q}$.*) *Suppose*

†:
$$\mu = \alpha\beta$$

is a factorization of a good poly. Then α and β are necessarily good and

‡:
$$\overleftarrow{\mu} = \overleftarrow{\alpha}\overleftarrow{\beta} .$$

Furthermore, (‡) is a non-trivial factorization iff (†) is non-trivial.

In particular, μ is irreducible iff $\overleftarrow{\mu}$ is. So if A is a non-zero algebraic number, then $1/A$ is also an algebraic number, and of the same degree. ◊

Proof. The degrees add, $L = J + K$. Plug $\frac{1}{x}$ into (†), then multiply by x^L. This produces

$$x^L \mu(1/x) \quad = \quad x^J \alpha(1/x) \cdot x^K \beta(1/x)\,.$$

And this is simply (‡), rewritten.

WLOG each of μ, α, β is monic. If (†) is trivial, say $\alpha() = 1$, then $\overleftarrow{\alpha}()$ is also 1; so (‡) is a trivial factorization. [The argument uses that we work with *good* polys, so that reversal is involutory.] ♦

The Gauss Lemma

To rule out the above "uninteresting" factorization (2) over $\mathbb{Z}$, we restrict the polys we look at. A poly μ is ***primitive*** if: *It is an intpoly with positive high-order coefficient* <u>*and*</u> *the* GCD *of its coeffs is* 1.

4: Gauss Lemma. *The product of primitive polys is primitive.* ♢

Proof of Gauss lemma. Take a product $\mu = \alpha \cdot \beta$ of primitive polys. To show μ primitive, ISTFix an arbitrary prime p and produce an index ℓ for which

4a: $$M_\ell \not\mid p\,.$$

Since α, β are primitive, there are *smallest* indices $\widehat{\jmath}, \widehat{k} \in \mathbb{N}$ so that

$$A_{\widehat{\jmath}} \not\mid p \qquad \text{and} \qquad B_{\widehat{k}} \not\mid p\,.$$

Let $\ell := \widehat{\jmath} + \widehat{k}$. Then $\boxed{M_\ell = A_{\widehat{\jmath}} B_{\widehat{k}} + S}$ where S is the sum, of products $A_j B_k$, taken over all <u>*other*</u> pairs $j + k = \widehat{\jmath} + \widehat{k}$. Relation (4a) is equivalent, since $A_{\widehat{\jmath}} B_{\widehat{k}}$ is *not* a multiple of p, to showing that S <u>is</u> a multiple of p. Hence ISTProve that the product

4b: $$A_j \cdot B_k \mid p$$

for each "other" index-pair (j, k). But if $j < \widehat{\jmath}$ then $A_j \mid p$; otherwise $j > \widehat{\jmath}$ and thus $k < \widehat{k}$, in which case $B_k \mid p$. Either case yields (4b). ♦

The ***Gauss content*** of a non-zip ratpoly μ is the unique rational number q, where we write $\mu() = q \cdot \alpha()$, with $\alpha()$ primitive. Write $\mathrm{GC}(\mu) = q$.

5: Corollary. *For non-zip ratpolys μ_1 and μ_2,*

$$\mathrm{GC}(\mu_1 \cdot \mu_2) \;=\; \mathrm{GC}(\mu_1) \cdot \mathrm{GC}(\mu_2)\,. \qquad \diamondsuit$$

Proof. Write $\mu_i() = q_i \cdot \alpha_i()$, with α_i primitive. Hence $\mu_1\mu_2 = [q_1 q_2] \cdot \alpha_1\alpha_2$. By the Gauss Lemma, $\alpha_1\alpha_2$ is primitive. So $\mathrm{GC}(\mu_1\mu_2) = q_1 q_2$. ♦

6: Corollary. *Suppose that a primitive poly μ is irreducible over $\mathbb{Z}$. Then μ is $\mathbb{Q}$-irreducible.* ♢

Proof. Supposing $\mu = \mu_1\mu_2$ over $\mathbb{Q}[x]$, write $\mu_i() = q_i \cdot \alpha_i()$, with α_i primitive. But

$$q_1 q_2 \;=\; \mathrm{GC}(\mu_1\mu_2) \;=\; \mathrm{GC}(\mu) \;=\; 1\,.$$

So $\mu = \alpha_1\alpha_2$. But μ is $\mathbb{Z}[x]$-irreducible, so WLOG $\alpha_2() = \pm 1$. Hence $\mu_2()$ is the constant poly q_2, which is a $\mathbb{Q}[x]$-unit. ♦

7: Coro. (Rational root thm). *Suppose rational number $\frac{p}{q}$, with $p \perp q$, is a root of intpoly $B_N x^N + \cdots + B_1 x + B_0$. Then $q \mid B_N$ and $p \mid B_0$.* ♢

Proof. Factoring the intpoly as

$$[qx-p]\cdot[C_{N-1}x^{N-1}+\cdots+C_1x+C_0]$$

implies that $\boxed{C_{N-1}=\frac{B_N}{q}}$ and $\boxed{C_0=\frac{-B_0}{p}}$. Now $\mathrm{GC}\big(x\mapsto[qx-p]\big)$ is 1, since $p\perp q$. Thus the Gauss content of $C_{N-1}x^{N-1}+\cdots+C_0$ is an integer. In particular, both C_{N-1} and C_0 are integers. ♦

We now come to the induction proof that we have all been waiting for.

8: Eisenstein Criterion (E.C). *Consider an intpoly*

$$\mu(x) = M_0+M_1x+M_2x^2+\ldots+M_{L-1}x^{L-1}+M_Lx^L,$$

with M_L non-zero. Suppose there exists a prime number p such that

8a: $p^2 \nmid M_0$,

8b: $p \nmid M_L$, *yet*

8c: $p \mid M_0, M_1, M_2, \ldots, M_{L-1}$.

Then μ is $\mathbb{Q}$-irreducible. ◊

Example. The poly $\mu(x) := 5+50x+x^2$ is irreducible, using E.C with the prime 5. Since this μ only has degree 2, we can deduce irreducibility just from the discriminant $50^2-4\cdot1\cdot5$, which is not a perfect square. □

Proof of E.C. Courtesy the Gauss Lemma we may assume that μ is primitive and endeavor to show that if $\mu=\alpha\beta$ is a factorization into intpolys as in (1), then degree J or K indeed equals L.

For specificity, suppose that the prime asserted in the hypotheses is 23. Since $23 \mid M_0 = A_0B_0$, WLOG $23 \mid A_0$. Courtesy (8a) then,

8a′: $23 \nmid B_0$.

Suppose we could establish that

8c′: $A_j \mid 23$, for each $j=0,1,2,\ldots,L-1$.

Were J strictly less than L, then this would imply that 23 divides *all* the α-coeffs, hence all the coeffs of μ (since β has integer coeffs). But this latter contradicts (8b). Hence it suffices to establish (**??′**).

Inducting along the coeffs. Were (**??′**) to fail, then there would be a smallest value $j\in[0\,..\,L-1]$ for which $A_j \nmid 23$. Multiplying out, M_j equals

$$A_jB_0 + \Big[A_{j-1}B_1+A_{j-2}B_2+\cdots+A_0B_j\Big].$$

(If $j=0$ then the bracketed sum is empty, hence zero.) Since j is the *smallest* bad index, necessarily 23 divides the bracketed sum. Since 23 divides M_j, we conclude that $23 \mid A_jB_0$. And (**??′**) now assures that $23 \mid A_j$; this contradicts that j was bad. ♦

Example uses of E.C.

Suppose f is an intpoly which has is no prime fulfilling the E.C. (Eisenstein criterion). Sometimes on can find an appropriate integer T so that the translated intpoly

$$g(z) := f(z+T)$$

does fulfill E.C. This end-around shows f to be irreducible. Here is an example.

9: *Cyclo-poly* $\mathbf{C}_p$ *is irreducible.* Fixing a prime p, we endeavor to show that the p^{th} ***cyclotomic polynomial***

$$\mathbf{C}_p(x) = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1 \stackrel{\text{note}}{=\!=} \frac{x^p - 1}{x - 1}$$

is irreducible. Although the E.C (Eisenstein criterion) doesn't directly apply to $\mathbf{C}_p$, we *can* apply E.C to translation $g(z) := \mathbf{C}_p(z+1)$. Expanding,

$$g(z) = \frac{[z+1]^p - 1}{z} = \frac{1}{z} \cdot \sum_{\substack{j+k=p \\ j \in [1..p]}} \binom{p}{j\,,\,k} \cdot z^j \cdot 1^k,$$

by the binomial thm. Letting $\ell := j-1$, rewrite this [using M_ℓ to denote the coeff of z^ℓ] as

$$g(z) = \sum_{\ell=0}^{p-1} \binom{p}{\ell+1} \cdot z^\ell =: \sum_{\ell=0}^{p-1} M_\ell \cdot z^\ell .$$

For each $\ell \in [0..p-2]$: Since p is prime, coeff M_ℓ is a multiple of p; yet $M_{p-1} \stackrel{\text{note}}{=\!=} 1$ is not. And $M_0 \stackrel{\text{note}}{=\!=} p$ fails to be divisible by p^2. The conditions of E.C being satisfied, g is irreducible; hence so is cyclotomic $\mathbf{C}_p$. □

10: *Quartic example.* Here is a pretty application that I read in J. S. Milne's "Fields and Galois Theory" at

http://www.jmilne.org/math/CourseNotes/index.html

in pdf form.

One way to show that an intpoly $f(x)$ is irreducible over $\mathbb{Z}[\![x]\!]$ is to produce a prime p for which $f(x)$ is $\mathbb{Z}_p[\![x]\!]$-irreducible. But there isn't always such a p, and here is a nice example. We will show that this (note: primitive) polynomial

10a: $$f(x) := x^4 - 10x^2 + 1 .$$

is *ir*reducibile as a $\mathbb{Q}$-poly but, for each prime p, factors non-trivially as a $\mathbb{Z}_p$-poly.

In $\mathbb{Z}$, does f have a degree-1 factor, i.e, an integer root? Well, $f(x){=}0$ becomes $1 = [10 - x^2] \cdot x^2$. So both x and $[10 - x^2]$ must be ± 1; this has no solution.

Could f have a quadratic factor? Then

$$f(x) = [x^2 - Ax \pm 1] \cdot [x^2 - Bx \pm 1]$$

for some $A, B \in \mathbb{Z}$. And $f(x)$ has no x^3 term, so $B = -A$. Thus $f(x) = [x^2 + Bx \pm 1] \cdot [x^2 - Bx \pm 1]$, i.e

$$f(x) = x^4 - [B^2 \mp 2]x^2 + 1 .$$

So $[B^2 \mp 2] = 10$. But equation $B^2 = 10 \pm 2$ has no integer solution. The upshot is that

10b: *$f(x)$ is $\mathbb{Z}[\![x]\!]$-irreducible.*

10c: Lemma. *For each prime p: Polynomial $f(x)$ factors non-trivially over $\mathbb{Z}_p[\![x]\!]$.* ♢

Proof. If 2 is a mod-p square (whether or not $2 \perp p$), then

10d: $$f(x) = [x^2 - 2\sqrt{2}x - 1] \cdot [x^2 + 2\sqrt{2}x - 1] .$$

Similarly, if 3 is a mod-p square then

10e: $$f(x) = [x^2 - 2\sqrt{3}x + 1] \cdot [x^2 + 2\sqrt{3}x + 1] .$$

So WLOG $p > 3$.

Now $2 \perp p$ and $3 \perp p$. So if neither (10d) nor (10e) applies, then both 2 and 3 are *non*-quadratic-residues, mod-p. Thus $2 \cdot 3 = 6$ *is* a p-quadratic-residue. And

10f: $$f(x) = [x^2 - A] \cdot [x^2 - B], \text{ where } \begin{array}{l} A := 5 + 2\sqrt{6}; \\ B := 5 - 2\sqrt{6}. \end{array}$$

This, since $A + B = 10$ and $A \cdot B = 1$. ♦

Filename: Problems/Algebra/eisenstein-irred.latex
As of: *Thursday 24May2007.* Typeset: *2Jun2023 at 20:24.*