Extra handout: The discriminant, and Eisenstein's criterion for shifted polynomials

Steven Charlton, Algebra Tutorials 2015–2016
`http://maths.dur.ac.uk/users/steven.charlton/algebra2_1516/`

Recall the Eisenstein criterion from Lecture 8:

Theorem (Eisenstein criterion)**.** *Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ be a polynomial. Suppose there is a prime $p \in \mathbb{Z}$ such that*
- $p \mid a_i$, *for* $0 \leq i \leq n-1$,
- $p \nmid a_n$, *and*
- $p^2 \nmid a_0$.

Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

You showed the *cyclotomic* polynomial $\Phi_p(X) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible by applying Eisenstein to the shift $\Phi_p(x+1)$. Tutorial 2, Question 1 asks you to find a shift of $x^2 + x + 2$, for which Eisenstein works.

How can we tell what shifts to use, and what primes might work? We can use the discriminant of a polynomial...

1 Discriminant

The *discriminant* of a polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ is a number $\Delta(f)$, which gives some information about the nature of the roots of f. It can be defined as

$$\Delta(f) \coloneqq a_n^{2n-2} \prod_{1 \leq i < j \leq n}^{n} (r_i - r_j)^2 ,$$

where r_i are the roots of $f(x)$.

Example. 1) Consider the quadratic polynomial $f(x) = ax^2 + bx + c$. The roots of this polynomial are

$$r_1, r_2 = \tfrac{1}{a} \left(-b \pm \sqrt{b^2 - 4ac} \right) ,$$

so $r_1 - r_2 = \frac{1}{a}\sqrt{b^2 - 4ac}$. We get that the discriminant is

$$\Delta(f) = a^{2 \cdot 2 - 2} \left(\tfrac{1}{a} \sqrt{b^2 - 4ac} \right)^2 = b^2 - 4ac ,$$

as you probably well know.

2) The discriminant of a cubic polynomial $f(x) = ax^3 + bx^2 + cx + d$ is given by

$$\Delta(f) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd\,.$$

Fact. 1) The discriminant $\Delta(f) = 0$ if and only if f has a repeated root.

2) The discriminant of a general polynomial $f(x)$ can be given algorithmically as some polynomial in terms of the coefficients a_i only, with no knowledge of the roots needed. This works over any commutative ring.

3) If $f \in \mathbb{Z}[x]$, and $\overline{f} \in \mathbb{Z}/p[x]$ is its reduction modulo p, then

$$\Delta(\overline{f}) = \overline{\Delta(f)} \quad \text{in } \mathbb{Z}/p$$

2 Eisenstein primes?

Proposition. *If Eisenstein works for the polynomial $f(x) = a_nx^n + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$, with the prime p, then $p \mid \Delta(f)$.*

Proof. Since Eisenstein works, we have that $p \mid a_i$, for $0 \le i \le n-1$, and $p \nmid a_n$. Reducing modulo p gives that

$$\overline{f}(x) = \overline{a_n}x^n \quad \text{in } \mathbb{Z}/p[x]\,.$$

Therefore $\overline{f}$ has a repeated root $x = \overline{0}$, modulo p. So we find, $\overline{\Delta(f)} = \Delta(\overline{f}) = 0$, in $\mathbb{Z}/p$. This means $\Delta(f)$ is divisible by p, as claimed. □

Observation. Shifting the variable x to $x - b$ does not change the differences of roots $r_i - r_j$, and does not change the leading coefficient a_n. Therefore if $g(x) = f(x-b)$, then $\Delta(g) = \Delta(f)$. So the primes $p \mid \Delta(f)$ are the only primes for which Eisenstein has any chance of working on a shift $f(x-b)$.

Proposition. *Suppose $p \mid \Delta(f)$, and $\overline{f}$ is the reduction of f modulo p. For Eisenstein to work on a shift $g(x) = f(x-b)$, then we must have $\overline{f} = \overline{a_n}(x + \overline{b})^n$. Moreover $h(x) = f(x - b - pk)$ are the only candidate shifts which Eisensein* might *work for p. And checking $k = 0$ suffices.*

Proof. If Eisenstein works for $g(x)$, then reducing modulo p gives $\overline{g}(x) = \overline{a_n}x^n$. So $\overline{f}(x) = \overline{g}(x + \overline{b}) = \overline{a_n}(x + \overline{b})^n$. We must therefore have a shift $h(x) = f(x - b')$ such that $\overline{b'} = \overline{b}$ in $\mathbb{Z}/p$, or equivalently $b' = b + pk$, for some $k \in \mathbb{Z}$.

Now suppose Eisenstein works with the prime p works for some polynomial $h(x) = a'_nx^n + \cdots + a'_1x + a'_0$. We will show it works for any shift $h(x - pk)$. The shift $h(x-pk)$ reduces to $\overline{h}(x - \overline{0}) = \overline{a'_n}x^n$ modulo p, meaning p still divides all non-leading coefficients of $h(x-pk)$. The leading coefficient is unchanged, so p still doesn't divide it. The constant term changes to $h(0-pk) = a'_n(-pk)^n + \cdots + a'_1(-pk) + a'_0$. Since $p \mid a'_1$, we see p^2 divides all terms except a'_0. Therefore p^2 cannot divide the total, and so p^2 does not divide the constant coefficient in $h(x-kp)$. This shows that Eisenstein works with the prime p for $h(x-pk)$.

In our situation, this means if Eisenstein works for any shift $f(x-b-pk)$, then it works for all such shifts. So checking $f(x-b)$ where $k=0$ suffices. $\square$

Warning. You *must* check if Eisenstein works on the candidate shifts. It is very possible that Eisenstein cannot be applied to the shifted polynomial either, for example because $p^2 \nmid a_0$ is not guaranteed when shifting.

3 Examples

1) Consider $f(x) = 128 - 48x + x^2 + x^3$. Currently Eisenstein does not work for f since no primes divide the coefficient 1 of x^2. From the formula for the discriminant of a cubic, given above, we find $\Delta(f) = -2^8 \cdot 5^2 \cdot 17$. So we should check $p = 2, 5, 17$ for possible shifts.

   Modulo 2,
   $$\overline{f}(x) = x^2 + x^3 = x^2(\overline{1} + x) \quad \text{in } \mathbb{Z}/2[x]\,,$$
   which is no good. But reducing modulo 5,
   $$\overline{f}(x) = \overline{3} + \overline{2}x + x^2 + x^3 = (x - \overline{3})^3 \quad \text{in } \mathbb{Z}/5[x]\,.$$
   This is good.

   So we try shifting to $f(x+3) = 20 - 15x + 10x^2 + x^3$. And Eisenstein works with $p = 5$ for this. Success!

2) Consider $f(x) = 684 - 386x - 653x^2 + 123x^3 + x^4$. Eisenstein does not currently work. One can compute that $\Delta(f) = 2^2 \cdot 5^3 \cdot 107^3 \cdot 1741 \cdot 17291$. (Ask `WolframAlpha` for the discriminant...)

   We can check through the possibilities to find that $\overline{f}(x)$ factors the way we want for $p = 107$, namely
   $$\overline{f}(x) = (x + \overline{4})^4 \quad \text{in } \mathbb{Z}/107[x]\,.$$
   Then we have $f(x-4) = -15836 + 10486x - 2033x^2 + 107x^3 + x^4$, and can check Eisenstein for $p = 107$ works, in a 'straightforward' manner.

Challenge. Show that there are irreducible polynomials which Eisenstein cannot detect. More precisely, find an irreducible polynomial $f(x)$ for which Eisenstein fails for all primes p, and all shifts $f(x-a)$. (Hint: try small degrees. You can find a quadratic example, a cubic example might be easier.)