1-29-1994

Eisenstein's criterion.

Theorem. Let

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

be a polynomial with integer coefficients, and let p be a prime number. Suppose that:

(a) $p \not| a_n$.

(b) $p \mid a_i$ for $i = 0, \ldots, n-1$.

(c) $p^2 \not| a_0$.

Then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof. It suffices to show that $f(x)$ is irreducible over $\mathbb{Z}$. Suppose there is a factorization

$$f(x) = (b_r x^r + \cdots + b_0)(c_s x^s + \cdots + c_0)$$

where the b_i's and c_i's are integers, $b_r, c_s \neq 0$, and $r + s = n$.

$p \mid a_0 = b_0 c_0$, so $p \mid b_0$ or $p \mid c_0$. On the other hand, $p^2 \not| a_0 = b_0 c_0$, so *exactly* one of b_0, c_0 is divisible by p. Suppose without loss of generality that $p \not| b_0$ and $p \mid c_0$.

It is also given that $p \not| a_n = b_r c_s$, so $p \not| b_r$ and $p \not| c_s$. The c_i's look like this:

$$p \mid c_0, \ldots, p \not| c_s.$$

Hence, there is a smallest index m such that $p \not| c_m$. It follows that $p \mid c_i$ for $i = 0, \ldots m-1$.

Look at

$$a_m = b_0 c_m + \cdots + b_{m-i} c_i.$$

Here $i > 0$, and it could be as large as m. Now c_0 through c_m are present, and b_0 is surely there, but the b_i's might disappear before b_m if $m > r$.

By assumption, $p \mid c_i$ for $i = 0, \ldots m-1$, but $p \not| b_0$ and $p \not| c_m$. Thus, $p \not| a_m$. However, the only a_i that is not divisible by p is a_n, so $m = n$.

Now what is m? It is the smallest index such that $p \not| c_m$. Thus, $p \not| c_n$, so $c_n \neq 0$. At this point, the c-polynomial must contain a term of degree n. Evidently, this forces the b-polynomial to have degree 0 — it is constant. The factorization is a trivial one, and $f(x)$ is irreducible. □

Examples.

1. $x^3 - 5$ is irreducible over $\mathbb{Q}$. Take $p = 5$ and apply Eisenstein.

More generally, if $n \geq 1$ and p is prime, $x^n - p$ is irreducible over $\mathbb{Q}$. □

---

2. (**Cyclotomic polynomials**) Let n be a positive integer.

$$\Phi_n(x) = \frac{x^n - 1}{x - 1} = 1 + x + \cdots + x^{n-1}$$

is the n-th **cyclotomic polynomial**.

Suppose that p is prime. I'll show that $\Phi_p(x)$ is irreducible.

Eisenstein doesn't apply to $\Phi_n(x)$ as it stands. The trick is to change variables.

Let $x = y + 1$. Then

$$\psi(y) = \Phi_p(y+1) = \frac{(y+1)^p - 1}{y+1-1} = \frac{y^p + \binom{p}{1} y^{p-1} + \cdots + py}{y} = x^{p-1} + \binom{p}{1} x^{p-2} + \cdots + \binom{p}{k} x^{p-k-1} + \cdots + p.$$

$\psi(y)$ is irreducible, by Eisenstein for the prime p.

Now if $\Phi_p(x) = f(x)g(x)$, then $\Phi_p(y+1) = f(y+1)g(y+1)$, so $\Phi_p(x)$ must be irreducible as well. $\square$

Here is another technique which is useful for showing an integer polynomial is irreducible.

Proposition. Let $f(x) \in \mathbb{Z}[x]$, and let p be a prime. Suppose that $f(x)$ mod p is nonzero and has the same degree as $f(x)$. If $f(x)$ mod p is irreducible over $\mathbb{Z}_p$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof. If ϕ is an integer polynomial, I'll write $\tilde{\phi}$ for its reduction mod p. (Reduce a polynomial mod p by reducing all its coefficients mod p.)

Suppose under the hypotheses above that $f(x) = g(x)h(x)$ in $\mathbb{Z}[x]$. Reduce mod p to obtain $\tilde{f} = \tilde{g}\tilde{h}$. Then

$$\deg \tilde{g} \le \deg g, \quad \deg \tilde{h} \le \deg h, \quad \text{but} \quad \deg \tilde{f} = \deg f.$$

It follows that the inequalities are really equalities:

$$\deg \tilde{g} = \deg g, \quad \deg \tilde{h} = \deg h.$$

Now $\tilde{f}$ is irreducible, so $\deg \tilde{f}$ is equal to either $\deg \tilde{g}$ or $\deg \tilde{h}$. Suppose without loss of generality that $\deg \tilde{f} = \deg \tilde{g}$. Then

$$\deg f = \deg \tilde{f} = \deg \tilde{g} = \deg g.$$

Hence, the factorization of f was trivial. $\square$

Example. Consider $x^3 + 6x^2 + 5x + 4$. Reducing mod 3 yields $x^3 + 2x + 1$. This factors over $\mathbb{Z}_3$ if and only if it has a root in $\mathbb{Z}_3$.

x	$x^3 + 2x + 1$
0	1
1	1
2	1

$x^3 + 2x + 1$ is irreducible over $\mathbb{Z}_3$, so $x^3 + 6x^2 + 5x + 4$ is irreducible over $\mathbb{Q}$. $\square$