Irreducibility of Polynomials

Evan Chen

DAX-IRRED

This will follow my unpublished notes *Polynomial Irreducibility*.

§1 Lecture notes

We outline three different general approaches for showing polynomials are irreducible, namely

- Taking modulo p,
- Looking at the size of complex roots, and
- Manipulations with factorized polynomials.

§1.1 Major results

Worth mentioning off the bat:

Theorem 1.1 (Fundamental Theorem of Algebra)
Every polynomial $f(x)$ in $\mathbb{C}[x]$ of degree n has n complex roots $\alpha_1, \dots, \alpha_n$ (not necessarily distinct) and we have

$$f(x) \equiv c(x - \alpha_1) \dots (x - \alpha_n).$$

Theorem 1.2 (Unique factorization of polynomials)
If R is a unique factorization domain, then $R[x]$ is too. In particular, $R[x_1, \dots, x_n]$ is a unique factorization domain. However $R[x]$ is not a principal ideal domain unless R is a field.

Theorem 1.3 (Gauss's Lemma)
Let $f \in \mathbb{Z}[x]$. Then f is irreducible over $\mathbb{Z}$ if and only if it is irreducible over $\mathbb{Q}$.

§1.2 Modding out

Example 1.4 (Eisenstein)

Let $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]$. Suppose $p \mid a_1, \dots, a_n$ but $p \nmid a_0$ and $p^2 \nmid a_n$. Then f is irreducible over $\mathbb{Z}$.

Problem 1.5 (Schönemann's Criterion)**.** Let

$$f(x) = \phi(x)^e + pM(x)$$

where $f, \phi, M \in \mathbb{Z}[x]$, $\phi \neq 0$, and $e \geq 1$. Suppose $\phi(x)$ is irreducible modulo p, and $\phi(x)$ does not divide $M(x)$ modulo p. Then f is irreducible.

Problem 1.6 (Romania TST 2006, Valentin Vornicu)**.** Let p be an odd prime number. Find the number of pairs $1 \leq \ell < k \leq p-1$ for which

$$x^p + px^k + px^\ell + 1$$

is irreducible over the integers.

§1.3 Size considerations

Fact 1.7 (Triangle Inequality)**.** For z_1, z_2 complex numbers, we have $|z_1 + z_2| \leq |z_1| + |z_2|$ with equality if and only if z_1 and z_2 have the same argument, or one of them is zero.

Lemma 1.8

Let $f \in \mathbb{Z}[x]$ be monic.

(a) Suppose $f(0) \neq 0$ and at most one (complex) root of f has absolute value at least 1. Then f is irreducible over $\mathbb{Z}$.

(b) Suppose $|f(0)|$ is prime, and all complex roots of f have absolute value greater than 1. Then f is irreducible over $\mathbb{Z}$.

Problem 1.9. Let $p > 3$ be a prime number and m, n be distinct positive integers. Prove that $x^m + x^n + p$ is irreducible in $\mathbb{Q}$.

Problem 1.10 (Selmer)**.** For any integer $n \geq 2$, $x^n - x - 1$ is irreducible over the integers.

Theorem 1.11 (Rouché Theorem)

Let γ be a circle. Let f, g be holomorphic functions on and inside γ. Assume $|g| > |f - g|$ on γ. Then f and g have the same number of zeros (with multiplicity) inside γ.

The intuition is that we apply this to functions f with g as a "close approximation" to f, for example, a term that dominates the rest of the terms in size.

Corollary 1.12 (Perron's criterion)
Suppose $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$ and

$$|a_{n-1}| > 1 + |a_{n-2}| + \dots + |a_0|.$$

If $a_0 \neq 0$ then this polynomial is irreducible.

§1.4 Manipulation

Problem 1.13 (MOP)**.** Prove that for any distinct integers $a_1, a_2, \dots, a_n$ the polynomial $(x - a_1)(x - a_2)\dots(x - a_n) - 1$ is irreducible over the integers.

§2 Practice problems

Problem 2.1 (Russia 1997)**.** Do there exist two quadratics $ax^2 + bx + c$ and $(a+1)x^2 + (b+1)x + (c+1)$ with integer coefficients, both of which have two integer roots?

Problem 2.2 (IMO 1993)**.** Prove that $x^n + 5x^{n-1} + 3$ is irreducible over $\mathbb{Z}$.

Problem 2.3 (Brazil 2006)**.** Let p be an irreducible polynomial in $\mathbb{Q}[x]$ and degree larger than 1. Prove that if p has two roots r and s whose product is 1 then the degree of p is even.

Problem 2.4 (Romania TST 2010, Beniamin Bogosel)**.** Let $n_1 > n_2 > \dots > n_p$ be positive integers, and set $d = \gcd(n_1, n_2, \dots, n_p)$. Prove that

$$\frac{X^{n_1} + X^{n_2} + \dots + X^{n_p} - p}{X^d - 1}$$

is irreducible over $\mathbb{Q}$.

Problem 2.5. Let p be a prime and b a positive integer. Prove that if the polynomial $x^n + px + bp^2$ has no integer roots, then it is irreducible over $\mathbb{Q}$.

Problem 2.6 (ELMO 2012/3)**.** Prove that if m, n are relatively prime positive integers, $x^m - y^n$ is irreducible in the complex numbers.

Problem 2.7 (Romania TST 2003, Mihai Piticari)**.** Let $f \in \mathbb{Z}[x]$ be a monic polynomial which is irreducible over the integers, and suppose $|f(0)|$ is not a perfect square. Prove that $f(x^2)$ is also irreducible.