Irreducibility

Polynomial $P(x)$ with integer coefficients is said to be *irreducible* over $\mathbb{Z}[x]$ if it cannot be written as a product of two nonconstant polynomials with integer coefficients.

Example

Every quadratic or cubic polynomial with no rational roots is irreducible over $\mathbb{Z}$. Such are e.g. $x^2 - x - 1$ and $2x^3 - 4x + 1$.

One analogously defines (ir)reducibility over the sets of polynomials with e.g. rational, real or complex coefficients. However, of the mentioned, only reducibility over $\mathbb{Z}[x]$ is of interest. Gauss' Lemma below claims that the reducibility over $\mathbb{Q}[x]$ is equivalent to the reducibility over $\mathbb{Z}[x]$. In addition, we have already shown that a real polynomial is always reducible into linear and quadratic factors over $\mathbb{R}[x]$, while a complex polynomial is always reducible into linear factors over $\mathbb{C}[x]$.

Theorem 4.1 (Gauss' Lemma)

If a polynomial $P(x)$ with integer coefficients is reducible over $\mathbb{Q}[x]$, then it is reducible over $\mathbb{Z}[x]$, also.

Show proof

From now on, unless otherwise specified, by *irreducibility* we mean irreducibility over $\mathbb{Z}[x]$.

Problem 9

If $a_1, a_2, \ldots, a_n$ are integers, prove that the polynomial $P(x) = (x - a_1)(x - a_2)\cdots(x - a_n) - 1$ is irreducible.

Show solution

Theorem 4.2 (Extended Eisenstein's Criterion)

Let $P(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients. If there exist a prime number p and an integer $k \in \{0, 1, \ldots, n-1\}$ such that

$$p \mid a_0, a_1, \ldots, a_k, \quad p \nmid a_{k+1} \text{ and } p^2 \nmid a_0,$$

then $P(x)$ has an irreducible factor of a degree greater than k.

In particular, if p can be taken so that $k = n - 1$, then $P(x)$ is irreducible.

Show proof

Problem 10 (IMO93.1)

Given an integer $n > 1$, consider the polynomial $f(x) = x^n + 5x^{n-1} + 3$. Prove that there are no nonconstant polynomials $g(x), h(x)$ with integer coefficients such that $f(x) = g(x)h(x)$.

Show solution

Problem 11

If p is a prime number, prove that the polynomial $\Phi_p(x) = x^{p-1} + \cdots + x + 1$ is irreducible.

Show solution

In investigating reducibility of a polynomial, it can be useful to investigate its zeros and their modules. The following problems provide us an illustration.

Problem 12

Prove that the polynomial $P(x) = x^n + 4$ is irreducible over $\mathbb{Z}[x]$ if and only if n is a multiple of 4.

Show solution

If the zeros cannot be exactly determined, one should find a good enough bound. Estimating complex zeros of a polynomial is not always simple. Our main tool is the triangle inequality for complex numbers:

$$|x| - |y| \le |x + y| \le |x| + |y|.$$

Consider a polynomial $P(x) = a_n x^n + a_{n-k} x n - k + \cdots + a_1 x + a_0$ with complex coefficients ($a_n \neq 0$). Let α be its zero. If M is a real number such that $|a_i| < M|a_n|$ for all i, it holds that

$$0 = |P(\alpha)| \ge |a_n||\alpha|^n - M|a_n|(|\alpha|^{n-k} + \cdots + |\alpha| + 1) > |a_n||\alpha|^n \left(1 - \frac{M}{|\alpha|^{k-1}(|\alpha| - 1)}\right),$$

which yields $|\alpha|^{k-1}(|\alpha| - 1) < M$. We thus come to the following estimate:

Theorem 4.3

Let $P(x) = a_n x^n + \cdots + a_0$ be a complex polynomial with $a_n \neq 0$ and $M = \max\limits_{0 \le k < n} \left|\frac{a_k}{a_n}\right|$. If $a_{n-1} = \cdots = a_{n-k+1} = 0$, then all roots of the polynomial P are less than $1 + \sqrt[k]{M}$ in modulus.

In particular, for $k = 1$, each zero of $P(x)$ is of modulus less than $M + 1$.

Problem 13 (Balkan Mathematical Olympiad 1989)

If $\overline{a_n \ldots a_1 a_0}$ is a decimal representation of a prime number and $a_n > 1$, prove that the polynomial $P(x) = a_n x^n + \cdots + a_1 x + a_0$ is irreducible.

Show solution

Problem 14

Let $p > 2$ be a prime number and $P(x) = x^p - x + p$.

- **(a)** Prove that all zeros of polynomial P are less than $p^{\frac{1}{p-1}}$ in modulus.
- **(b)** Prove that the polynomial $P(x)$ is irreducible.

Hide solution

- **(a)** Let y be a zero of P. Then $|y|^p - |y| \leq |y^p - y| = p$. If we assume that $|y| \geq p^{\frac{1}{p-1}}$, we obtain

$$|y|^p - |y| \geq (p-1)p^{\frac{1}{p-1}} > p,$$

a contradiction. Here we used the inequality $p^{\frac{1}{p-1}} > \frac{p}{p-1}$ which follows for example from the binomial expansion of $p^{p-1} = ((p-1)+1)^{p-1}$.

- **(b)** Suppose that $P(x)$ is the product of two nonconstant polynomials $Q(x)$ and $R(x)$ with integer coefficients. One of these two polynomials, say Q, has the constant term equal to $\pm p$. On the other hand, the zeros $x_1, \ldots, x_k$ of Q satisfy $|x_1|, \ldots, |x_k| < p^{\frac{1}{p-1}}$ by part (a), and $x_1 \cdots x_k = \pm p$, so we conclude that $k \geq p$, which is impossible.

Polynomials (Table of contents)