Emro Science and Education
International open-access scientific journal
Journal homepage: https://journal.emro.uz

OPEN ACCESS

CONFERENCE PAPER OPEN ACCESS

Vol. 1 No. 1 (2023) · "Axborot oqimlari va intellektual tizimlarning ijtimoiy, iqtisodiy va texnik-texnol... DOI: 10.5281/zenodo.24319610

materiallar to'plami

Integer Polynomials

Mamurov Mansurbek, The master's student of Andijan Machine Building Institute

Key words: modulo redaction, problem, theorem, perron's criterion, polynomial, coefficients, functions, Lemma, constant, principle.

Annotation

This article will fully reveal all the features of Polynomials. For example, their signs of division and a number of excellent lemmas are **mentioned.**

We will use $\mathbb{Z}[x]$ to denote the ring of polynomials with integer coefficients. We begin by summarizing some of the common approaches used in dealing with integer polynomials.

- Looking at the coefficients
  - Bound the size of the coefficients
  - Modulos reduction. In particular, $a - b \mid P(a) - P(b)$ whenever $P(x) \in \mathbb{Z}[x]$ and a, b are distinct integers.
- Looking at the roots
  - Bound their location on the complex plane.
  - Examine the algebraic degree of the roots, and consider field extensions. Minimal polynomials.

Many problems deal with the irreducibility of polynomials. A polynomial is *reducible* if it can be written as the product of two nonconstant polynomials, both with rational coefficients. Fortunately, if the original polynomial has integer coefficients, then the concepts of (ir)reducibility over the integers and over the rationals are equivalent. This is due to **Gauss' Lemma**.

Theorem 1 (Gauss)**.** If a polynomial with integer coefficients is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.

Thus, it is generally safe to talk about the reducibility of integer polynomials without being pedantic about whether we are dealing with $\mathbb{Q}$ or $\mathbb{Z}$.

Modulo Reduction

It is often a good idea to look at the coefficients of the polynomial from a number theoretical standpoint. The general principle is that any polynomial equation can be reduced mod m to obtain another polynomial equation whose coefficients are the residue classes mod m.

Many criterions exist for testing whether a polynomial is irreducible. Unfortunately, none are powerful enough to be universal. One of the most well-known criteria is **Eisenstein's criterion**.

Theorem 2 (Eisenstein)**.** Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients 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.

Proof. Suppose that $f = gh$, where g and h are nonconstant integer polynomials. Consider the reduction mod p (i.e., apply the ring homomorphism $\mathbb{Z}[x] \to \mathbb{F}_p[x]$), and let $\bar{f}, \bar{g}, \bar{h}$ denote the residues of f, g, h (i.e. the coefficients are residues mod p). We have $\bar{f}(x) = a_0 x^n$. Since $\mathbb{F}_p[x]$ is a unique factorization domain, we see that the only possibilities for $\bar{g}$ and $\bar{h}$ are cx^k for some integers c and $k \geq 1$. Then, the constant terms of g and h are both divisible by p, so $p^2 \mid a_0$. Contradiction. □

The most typical example for the application of Eisenstein's criterion is to show that the cyclotomic polynomial $\Phi_p(x)$ is irreducible for prime p:

Problem 1. Let p be a prime number. Show that $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible.

Published: 10.11.2023

Cite this article: Mamurov Mansurbek (2023). Integer Polynomials. Emro Science and Education, 1(1). https://doi.org/10.5281/zenodo.24319610

© 2023 The Author(s). Published by Emro Science and Education. This is an open access article.

Solution. The polynomial $f(x)$ is irreducible if and only if $f(x+1)$ is irreducible. We have

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-2}x + p.$$

Note that $f(x+1)$ fails the Eisenstein criterion for the prime p. Therefore $f(x)$ is irreducible. □

Note that the proof of Eisenstein's criterion extends to other rings with similar properties. For instance, to show that $x^4 + 5x + 5$ is irreducible over the Gaussian integers $\mathbb{Z}[i]$, we can simply apply Eisenstein with the Gaussian prime $2 + i$.

The proof of Eisenstein's Criterion can be slightly generalized to the following. The proof is more or less the same, and so it's left as exercise.

Theorem 3 (Extended Eisenstein)**.** Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients such that $p \mid a_i$ for $0 \le i < k$, $p \nmid a_k$ and $p^2 \nmid a_0$. Then $f(x)$ has an irreducible factor of degree greater than k.

We give one more result that relates to looking at the modulo reduction of polynomials, known as **Hensel's lemma**.

Theorem 4 (Hensel)**.** Let $a_0, a_1, \ldots, a_k$ be integers, and let $P(x) = a_n x^k + \cdots a_1 x + a_0$, and let $P'(x)$ denote the derivative of $P(x)$. Suppose that x_1 is an integer such that $P(x_1) \equiv 0 \pmod{p}$ and $P'(x_1) \not\equiv 0 \pmod{p}$. Then, for any positive integer k, there exists an unique residue $x \pmod{p^k}$, such that $P(x_k) \equiv 0 \pmod{p^k}$ and $x \equiv x_1 \pmod{p}$.

The proof of Hensel's lemma closely mimics Newton's method of finding roots. We work up the powers of p, and find the a zero of $P(x) \mod p^k$ for $k = 2, 3, \ldots$. The details of the proof are omitted here.

Root Hunting

When working with integer polynomials, it is often not enough to stay in $\mathbb{Z}$. We have to think outside the box and move our scope to the complex numbers. A lot can be a said about a polynomial if we know something about its complex zeros. Many irreducibility problems hinge on placing bounds on the zeros of the polynomial in the complex plane. We begin with a familiar example.

Problem 2. Let $f(x) = a_n x^n + a_{n-1}x^n + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients, such that $|a_0|$ is prime and

$$|a_0| > |a_1| + |a_2| + \cdots + |a_n|.$$

Show that $f(x)$ is irreducible.

Solution. Let α be any complex zero of f. Suppose that $|\alpha| \le 1$, then

$$|a_0| = |a_1\alpha + \cdots + a_n\alpha^n| \le |a_1| + \cdots + |a_n|,$$

a contradiction. Therefore, all the zeros of f satisfies $|\alpha| > 1$.

Now, suppose that $f(x) = g(x)h(x)$, where g and g are nonconstant integer polynomials. Then $a_0 = f(0) = g(0)h(0)$. Since $|a_0|$ is prime, one of $|g(0)|, |h(0)|$ equals 1. Say $|g(0)| = 1$, and let b be the leading coefficient of g. If $\alpha_1, \ldots, \alpha_k$ are the roots of g, then $|\alpha_1\alpha_2 \cdots \alpha_k| = 1/|b| \le 1$. However, $\alpha_1, \ldots, \alpha_k$ are also zeros of f, and so each has an magnitude greater than 1. Contradiction. Therefore, f is irreducible. □

Next, we present a **Perron's criterion**, which has a similar statement but a much more difficult proof compared with the previous result.

Theorem 5 (Perron)**.** Let $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with $a_0 \neq 0$ and

$$|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_1| + |a_0|.$$

Then $P(x)$ is irreducible.

Again, the idea is to put bounds on the modulus of the roots of f. The key lies in the following lemma.

Lemma 1. Let $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a polynomial with

$$|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_1| + |a_0|.$$

Then exactly one zero of P satisfies $|z| > 1$, and the other $n-1$ zeros of P satisfy $|z| < 1$.

Let us see how we can prove Perron's criterion if we have this lemma. Suppose that $P(x) = f(x)g(x)$, where f and g are integer polynomials. Since P has only one zero with modulus not less than 1, one of the polynomials f, g, has all its zeros strictly inside the unit circle. Suppose that $z_1, \ldots, z_k$ are the zeros of f, and $|z_1|, \ldots, |z_k| < 1$. Note that $f(0)$ is a nonzero integer, and $|f(0)| = |z_1 \cdots z_k| < 1$, contradiction. Therefore, f is irreducible.

Now, let us prove Lemma 1. We offer two proofs. The first proof is an elementary proof that uses only the triangle inequality. The second proof invokes theorems from complex analysis, but it is much more intuitive and instructive.

First proof of the Lemma 1. (due to Laurentiu Panaitopol) Let us suppose wolog that $a_0 \neq 0$ since we can remove any factors of the form x^k . Let's first prove that there is no root α of $P(x)$ with $|\alpha| = 1$. Suppose otherwise, then we have that

$$-a_{n-1}\alpha^{n-1} = \alpha^n + a_{n-2}\alpha^{n-2} + \cdots + a_1\alpha + a_0,$$

thus

$$\begin{aligned} |a_{n-1}| = |a_{n-1}\alpha^{n-1}| &= |\alpha^n + a_{n-2}\alpha^{n-2} + \cdots + a_1\alpha + a_0| \\ &\leq |\alpha^n| + |a_{n-2}\alpha^{n-2}| + \cdots + |a_1\alpha| + |a_0| \\ &= 1 + |a_{n-2}| + \cdots + |a_1| + |a_0|. \end{aligned}$$

This contradicts the given inequality. Therefore, no zero of $f(x)$ lies on the unit circle.

Let's denote with α_1, α_2, …, α_n be the zeros of P. Since $|\alpha_1\alpha_2 \cdots \alpha_n| = a_0$, it follows that at least one of the roots is larger than 1 in absolute value. Suppose that $|\alpha_1| > 1$ and let

$$Q(x) = x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1x + b_0$$

be the polynomial with roots α_2, α_3, …, α_n. Then,

$$P(x) = (x - \alpha_1)Q(x) = x^n + (b_{n-2} - \alpha_1)x^{n-1} + (b_{n-3} - b_{n-2}\alpha_1)x^{n-2} + \cdots + (b_0 - b_1\alpha_1)x - b_0\alpha_1$$

It follows that $b_{n-1} = 1$, $a_0 = -b_0\alpha_1$, and $a_k = b_{k-1} - b_k\alpha_1$ for all $1 \leq k \leq n-1$. Then, using the given inequality, we have

$$\begin{aligned} |b_{n-2} - \alpha_1| = |a_{n-1}| &> 1 + |a_{n-2}| + \cdots + |a_1| + |a_0| \\ &= 1 + |b_{n-3} - b_{n-2}\alpha_1| + \cdots + |b_0\alpha_1| \\ &\geq 1 + |b_{n-2}||\alpha_1| - |b_{n-3}| + |b_{n-3}||\alpha_1| - |b_{n-4}| + \cdots + |b_1||x_1| - |b_0| + |b_0||x_1| \\ &= 1 + |b_{n-2}| + (|\alpha_1| - 1)\left(|b_{n-2}| + |b_{n-3}| + \cdots + |b_1| + |b_0|\right). \end{aligned}$$

On the other hand, $|b_{n-2} - \alpha_1| \leq |b_{n-2}| + |\alpha_1|$, so

$$|b_{n-2}| + |\alpha_1| > 1 + |b_{n-2}| + (|\alpha_1| - 1)\left(|b_{n-2}| + |b_{n-3}| + \cdots + |b_1| + |b_0|\right)$$

and therefore

$$|b_{n-2}| + |b_{n-3}| + \cdots + |b_1| + |b_0| < 1.$$

Then, for any complex number α with $|\alpha| \geq 1$, we have

$$\begin{aligned}|Q(\alpha)| &= |\alpha^{n-1} + b_{n-2}\alpha^{n-2} + b_{n-3}\alpha^{n-3} + \cdots + b_1\alpha + b_0| \\ &\geq |\alpha^{n-1}| - |b_{n-2}\alpha^{n-2}| - |b_{n-3}\alpha^{n-3}| - \cdots - |b_1\alpha| - |b_0| \\ &\geq |\alpha|^{n-1} - |\alpha|^{n-1}\left(|b_{n-2}| + |b_{n-3}| + \cdots + |b_1| + |b_0|\right) \\ &= |\alpha|^{n-1}\left(1 - |b_{n-2}| - |b_{n-3}| - \cdots - |b_1| - |b_0|\right) \\ &> 0\end{aligned}$$

And so α cannot be a root. It follows that all the zeros of Q lie strictly inside the unit circle. This completes the proof of the lemma. □

In the polynomial P, the second term x^{n-1} is "dominating," in the sense that the absolute value of its coefficient is greater than the sum of the absolute values of all the other coefficients. In the above proof, we managed to construct a new polynomial Q, whose leading term is dominating. While exactly one zero of P is outside the unit circle, none of the zeros of Q is outside the unit circle. This observation generalizes to the following result.

Proposition 6. Let $P(z) = a_n z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$ be a polynomial with complex coefficients, and such that

$$|a_k| > |a_0| + |a_1| + \cdots + |a_{k-1}| + |a_{k+1}| + \cdots + |a_n|$$

for some $0 \leq k \leq n$. Then exactly k zeros of P lie strictly inside the unit circle, and the other $n-k$ zeros of P lie strictly outside the unit circle.

This is indeed true. The easiest way to prove this result is to invoke a well-known theorem in complex analysis, known as **Rouché's theorem**.

Theorem 7 (Rouché)**.** Let f and g be analytic functions on and inside a simple closed curve $\mathcal{C}$. Suppose that $|f(z)| > |g(z)|$ for all points z on $\mathcal{C}$. Then f and $f+g$ have the same number of zeros (counting multiplicities) interior to $\mathcal{C}$.

The proof of Rouché's theorem uses the argument principle. It can be found in any standard complex analysis textbook.

In practice, for polynomials, Rouché's theorem is generally applied to some circle, and is useful when one term is very big compared to the other terms.

Proposition 6 becomes very easy to prove with the aid of Rouché's theorem. Indeed, let us apply Rouché's theorem to the functions $a_k z^k$ and $P(z) - a_k z^k$ with the curve being the unit circle. The given inequality implies that $|a_k z^k| > |P(z) - a_k z^k|$ for all $|z| = 1$. It follows that P has the same number of zeros as $a_k z^k$ inside the unit circle. It follows that P has exactly k zeros inside the unit circle. Also, it is not hard to show that P has no zeros on the unit circle (c.f. first proof of Lemma 1). Thus we have proved Proposition 6.

Second proof of Lemma 1. Apply Proposition 6 to $k = n-1$. □

While we're at it, let's look at couple of neat applications of Rouché's theorem, just for fun. These are not integer polynomial problems, but they contain useful ideas.

Problem 3. (Romania ??) Let $f \in \mathbb{C}[x]$ be a monic polynomial. Prove that we can find a $z \in \mathbb{C}$ such that $|z| = 1$ and $|f(z)| \geq 1$.

Solution. Let $\deg P = n$. Suppose that $|f(z)| < 1$ for all z on the unit circle. Then $|f(z)| < |z^n|$ for all z on the unit circle. So, by Rouché's theorem, $f(z) - z^n$ has n roots inside the unit circle, which is impossible, since $f(z) - z^n$ has degree $n-1$. □

The Fundamental Theorem of Algebra is also an easy consequence of Rouché's theorem.

Theorem 8 (Fundamental Theorem of Algebra)**.** Any polynomial $P(x) \in \mathbb{C}[x]$ of degree n has exactly n complex zeros.

Bibliography

1. **The Fundamental Theorem of Algebra, by Benjamin Fine and Gerhard Rosenberger (Springer-Verlag, 1997)**
2. **Stillwells' "Mahtematics and its history"**
3. **Stillwell's Elements of Algebra**
4. **Polynomials by Titu Andreescu**
5. **Polynomials by E.Barbeau**
6. **Polynomials by V.V. Prasolov**
7. **J. V. Uspensky, Theory of Equations**
8. **McKee and Smyth, Number Theory and Polynomials**
9. **Langevin and Waldschmidt, Cinquante Ans de Polynomes - Fifty Years of Polynomials, proceedings of a conference held in Paris, 26-27 May 1988,**