Irreducibility of Polynomials over the Integers

Claudiu Raicu

April 27, 2010

1 Let's warm up!

1. Is $X^2 + 4X + 3$ reducible? What about $X^2 + 3X + 4$?
2. Show that $X^3 - 5X + 14$ is irreducible. What about $X^3 - 51X + 14$?
3. Show that $X^4 + 1$ is irreducible. Is $X^4 + 4$ reducible?
4. Show that $X^5 + 6X^4 + 6X^3 + 24X + 72$ is irreducible.

2 Take a look at the roots!

1. Is the polynomial $X^{18} - 18$ irreducible? What about $X^{18} - 36$? And $X^{18} - 72$?
2. Let a, n be integer numbers, $n \geq 1$, and let p be a prime number, $p > |a| + 1$. Show that the polynomial
$$X^n + aX + p$$
is irreducible.
3. Let $n \geq 2$ be an odd integer, and let p be a prime number. Assume that all the roots of the polynomial
$$X^n + a_{n-1}X^{n-1} + \cdots + a_1X + p^2$$
have the same absolute value. Show that the polynomial $g(X) = f(X^2)$ is irreducible.

Theorem 2.1. *(Perron's criterion) Let $f = X^n + a_1X^{n-1} + \cdots + a_n$ be a polynomial with integer coefficients. If $|a_1| > 1 + |a_2| + \cdots + |a_n|$, then f is irreducible.*

Quick question: is the polynomial $X^n + 5X^{n-1} + 3$ reducible?

3 What if our polynomials take lots of small values?

1. Show that if $a_1, \cdots, a_n$ are distinct integers, then the polynomial
$$(X - a_1) \cdots (X - a_n) - 1$$
is irreducible.

2. Show that if $a_1, \cdots, a_n$ are distinct integers, then the polynomial

$$(X - a_1)^2 \cdots (X - a_n)^2 + 1$$

is irreducible.

3. Let g be a polynomial of degree k with integer coefficients, and let $d_1, \cdots, d_k$ be distinct integers. Show that

$$|g(d_i)| \geq \frac{k!}{2^k}$$

for at least one value of $i \in \{1, \cdots, k\}$. (You'll need this result for the next problem)

4. (Polya) Let f be a polynomial of degree n with integer coefficients, and set $m = \lfloor (n+1)/2 \rfloor$. Suppose there exist n distinct integer numbers $a_1, \cdots, a_n$ which are not roots of f, for which

$$f(a_i) < \frac{m!}{2^m}.$$

Prove that f is irreducible.

4 Reducing mod p...starting to feel the heat?

Theorem 4.1. *(Eisenstein's criterion) Let p be a prime number, and $f = a_n X^n + \cdots + a_1 X + a_0$ a polynomial with integer coefficients. Assume that*

- $p \nmid a_n$
- $p | a_{n-1}$, $p | a_{n-2}$, $\cdots$, $p | a_1$, $p | a_0$.
- $p^2 \nmid a_0$.

Then f is irreducible.

1. Show that if p is a prime number and q is not divisible by p, then $X^n - pq$ is irreducible. (Can you do this without Eisentein's criterion?)

2. Let p be a prime number. Show that

$$X^{p-1} + X^{p-2} + \cdots + X + 1$$

is irreducible.

3. Show that the polynomial

$$(X^2 + X)^{2^n} + 1$$

is irreducible.

4. Let p be a prime number, and a an integer not divisible by p. Show that the polynomial

$$X^p - X + a$$

is irreducible over the integers (by showing the stronger statement that it is irreducible over $\mathbb{Z}/(p)[X]$.

5. Show that $X^4 + 1$ is irreducible in $\mathbb{Z}[X]$, but reducible in $\mathbb{Z}/(p)[X]$ for every prime number p.

6. Is the polynomial $X^n + 5X^{n-1} + 3$ reducible? (have you seen this before?)

5 Enter the Heroes: Newton Polygons

Theorem 5.1. *(Dumas) The Newton polygon of a product of polynomials is the union of the Newton polygons of the factors.*

1. Let's try this again: show that $X^5 + 6X^4 + 6X^3 + 24X + 72$ is irreducible. Maybe try something easier before: is $X^5 + 2X^3 + 2X + 4$ irreducible?
2. Is the polynomial $X^n + 5X^{n-1} + 3$ reducible? (I thought we've answered this already...)
3. Let $n \geq 2$ be an odd integer, and let p be a prime number. Assume that all the roots of the polynomial
$$X^n + a_{n-1}X^{n-1} + \cdots + a_1X + p^2$$
have the same absolute value. Show that the polynomial $g(X) = f(X^2)$ is irreducible. (am I repeating myself?)
4. Show that the polynomial
$$\frac{X^n}{n!} + \frac{X^{n-1}}{(n-1)!} + \cdots + \frac{X}{1!} + 1$$
is irreducible. (For those of you who know about power series, the above polynomials form, as n ranges over the natural numbers, the truncations of the power series expansion of e^X.)

6 The Masterpiece

We'll try to put together (some of) the techniques we've learnt so far to prove the irreducibility of an interesting collection of polynomials. Consider the polynomials

$$f_n = \frac{(X+1)^n - X^n - 1}{X},$$

for $n \geq 1$. We will show that f_{2p} is irreducible whenever p is a prime number. Note that the problem of establishing the irreducibility of f_n is NOT solved for arbitrary n, so if you wanna get rich...spiritually...you should give it a try!

Here are the steps for the irreducibility of f_{2p}:

(a) Explain why if α is a root of f_n, then so is $1/\alpha$.

(b) From here on, we assume that $n = 2p$ with p a prime number. Consider the Newton polygon of f_n with respect to the prime number p. Show that f_n is either irreducible, or it can be written as a product of two irreducible polynomials of degree $(p-1)$, $f_n = g \cdot h$.

(c) Without loss of generality, assume that g and h have positive leading coefficients. If we let $\gcd(g)$ and $\gcd(h)$ be the greatest common divisors of the coefficients of the two polynomials (also known as *the contents* of the polynomials), show that $\gcd(g) = \gcd(h) = 1$. Show that, under our assumption, the constant terms in g, h are positive.

(d) Show that if α is a root of g, then $1/\alpha$ is NOT a root of g.

(e) Prove that g is the reciprocal of h, i.e.

$$g(X) = X^{n-1}h(1/X).$$

(f) Show that the situation in (e) cannot occur, and conclude that f_n is irreducible (when $n = 2p$).