MATH 9
ASSIGNMENT 10: IRREDUCIBLE POLYNOMIALS

DEC 12, 2021

Divisibility of integers: reminder

When studying integer numbers, we had discussed a number of results.

Recall that a number $p > 1$ is called prime if it can't be written in the form $p = ab$, with $a < p$, $b < p$.

Theorem 1. *Any integer $n > 1$ can be written as product of primes. This factorization is unique up to reordering the factors.*

We also talked about greatest common divisor and least common multiple.

Theorem 2. *Let $d = \gcd(a, b)$. Then a number k is a common divisor of a, b if and only if it is a divisor of d.*

Let $m = \operatorname{lcm}(a, b)$. Then a number k is a common multiple of a, b if and only if it is a multiple of m.

The greatest common divisor can be found using Euclid algorithm: given a pair (a, b), with $a \geq b$, replace it by a new pair (b, r), where r is the remainder upon division of a by b. Repeat it until you get the pair $(d, 0)$. So obtained d is the greatest common divisor of (a, b). To find the least common multiple, we can use the identity $\operatorname{lcm}(a, b) \cdot \gcd(a, b) = ab$.

Finally, the following result is commonly useful:

Theorem 3. *Let k, a be relatively prime: $\gcd(a, k) = 1$. Then kx is divisible by a if and only if x is divisible by a.*

For example, if $5x$ is divisible by 12, then x is divisible by 12.

Divisibility of polynomials

All of the above can be repeated for polynomials, with minor changes.

Definition. A polynomial $p(x)$ of degree n is called **irreducible** if it can not be written in the form $p(x) = a(x)b(x)$ where $a(x)$, $b(x)$ are polynomials of degree $< n$.

Note that we require that both factors have strictly lower degree than $p(x)$, so factorization like $2x^2 + 4 = 2 \cdot (x^2 + 2)$ doesn't count: here one of the factors has the same degree as the original polynomial.

Note also that if $p(x)$ is irreducible, then so is $2p(x)$, or, more generally, $cp(x)$, where c is a constant.

Theorem 4. *Any polynomial of degree ≥ 1 can be written as product of irreducible polynomials. Such factorization is unique up to changing the order of factors and* **multiplying irreducible factors by constants***.*

Note that even if the original polynomial has integer coefficients, the irreducible factors might have fractional or irrational coefficients. E.g., here is the factorization of polynomial $p(x) = x^2 - 2$:

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}).$$

Definition. A polynomial $d(x)$ is called a greatest common divisor of polynomials $a(x)$, $b(x)$ if

1. It is a common divisor of $a(x)$, $b(x)$
2. It has maximal possible degree of all common divisors of $a(x)$, $b(x)$.

From this definition, it is not clear if the greatest common divisor is unique — one could imagine there are several different common divisors of the same degree. However, it doesn't happen, as the theorem below shows.

Theorem 5. *The greatest common divisor of $a(x)$, $b(x)$ is unique (up to multiplying by a constant). Moreover, a polynomial $f(x)$ is a common divisor of $a(x)$, $b(x)$ if and only if $f(x)$ is a divisor of $\gcd(a(x), b(x))$.*

The greatest common divisor can be found using Euclid algorithm — in exactly the same way as it is for integers.

Problems

1. (a) Show that any polynomial of degree 1 is irreducible.
(b) Show that a polynomial of degree 2 is irreducible if and only if it has no roots.

In fact, it is known that these are the only irreducible polynomials (with real coefficients): any polynomial of degree 3 and higher must factor. However, it is a very difficult result; more importantly, there is no easy way to factor a polynomial, even if we know that it is not irreducible.

2. Compute the following greatest common divisors of polynomials:
(a) $(x-1)^2(x+2)^3(x^2+1)$ and $(x^2-1)(x^2+1)$
(b) x^5+5x^2-6 and x^3-1

3. Use Theorem 3 to show that if k, a are relatively prime, then common divisors of a, b are the same as common divisors of a, kb. In particular, $\gcd(a,b) = \gcd(a, kb)$

4. (a) Use Euclid algorithm and previous problem to compute $\gcd(2^{28}-1, 2^{18}-1)$.
[Hint: $2^{28}-1 = 2^{10}(2^{18}-1) + 2^{10} - 1$.]
(b) More generally, show that $\gcd(2^m-1, 2^n-1) = 2^{\gcd(m,n)} - 1$

5. (a) Use Euclid algorithm to compute the following greatest common divisor of polynomials: $\gcd(x^{28}-1, x^{18}-1)$
(b) Can you guess the general formula for $\gcd(x^m-1, x^n-1)$?

6. Solve the following system of equations:

$$\begin{aligned} x+y+z &= 6 \\ \tfrac{1}{x}+\tfrac{1}{y}+\tfrac{1}{z} &= \tfrac{11}{6} \\ xy+xz+yz &= 6 \end{aligned}$$