

Algebra

Math 294A: Problem Solving Seminar

1 Polynomials

One of the most important things to know when solving a problem involving polynomials is how to factor. There are a large number of identities which can be useful when factoring, but the most basic ones are

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}),$$
$$a^n + b^n = (a + b)(a^{n-1} - a^{n-2}b + \cdots - ab^{n-2} + b^{n-1}), \quad n \text{ odd.}$$

Similar to division and factoring in the integers, we may apply the Division algorithm to polynomials.

Division Algorithm. Let $f(x)$ and $g(x)$ be either polynomials with coefficients in \mathbb{R} , \mathbb{C} , or \mathbb{Q} , or monic polynomials over \mathbb{Z} . Then there exist unique polynomials (of the same type) $q(x)$ and $r(x)$, such that

$$f(x) = q(x)g(x) + r(x),$$

where $\deg(r(x)) < \deg(g(x))$, and $g(x)$ divides $f(x)$ precisely when $r(x)$ is the zero polynomial.

Like in the integers, the division algorithm can be used to find the greatest common divisor of two polynomials.

Example 1. Let x_1 and x_2 be the roots of the equation

$$x^2 - (a + d)x + (ad - bc) = 0.$$

Show that x_1^3 and x_2^3 are the roots of the equation

$$y^2 - (a^3 + d^3 + 3abc + 3bcd)y + (ad - bc)^3 = 0.$$

Example 2. Prove that the fraction $(n^3 + 2n)/(n^4 + 3n^2 + 1)$ is irreducible for every natural number n .

Example 3. Let N be the number which consists of 91 consecutive 1's in base ten expansion. Prove that N is composite.

Problem 1. Show that $n^4 - 20n^2 + 4$ is composite for any integer n .

Problem 2. Determine all solutions in the real numbers x, y, z, w of the system

$$x + y + z = w, \quad 1/x + 1/y + 1/z = 1/w.$$

Problem 3. For what n is the polynomial $1+x^2+x^4+\dots+x^{2n-2}$ divisible by the polynomial $1+x+x^2+\dots+x^{n-1}$?

Problem 4. Consider all lines which meet the graph of

$$y = 2x^4 + 7x^3 + 3x - 5$$

in four distinct points, say (x_i, y_i) , $i = 1, 2, 3, 4$. Show that

$$\frac{x_1 + x_2 + x_3 + x_4}{4}$$

is independent of the line, and find its value.

Problem 5. Prove that there are no prime numbers in the infinite sequence of integers

$$10001, 100010001, 1000100010001, \dots$$

Problem 6. Given numbers x, y, z such that

$$x + y + z = 3, \quad x^2 + y^2 + z^2 = 5, \quad x^3 + y^3 + z^3 = 7,$$

find the value of $x^4 + y^4 + z^4$.

Problem 7. If $n > 1$, show that $(x + 1)^n - x^n - 1 = 0$ has a multiple root if and only if $n - 1$ is divisible by 6.

Problem 8. Let $P(x)$ be the following polynomial, with real coefficients:

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_3 x^3 + x^2 + x + 1,$$

where $n \geq 2$. Show that the equation $P(x) = 0$ cannot have all real roots.

2 Groups

Let S be a set. A *binary operation* on S is a function from $S \times S$ to S . For example, addition is a binary operation on \mathbb{Z} . A binary operation $*$ on S is *associative* if $r * (s * t) = (r * s) * t$ for all $r, s, t \in S$. A *group* is a nonempty set G with an associative binary operation $*$ such that

- (i) G contains an *identity element*, $e \in G$, which has the property $e * g = g * e = g$ for every $g \in G$.
- (ii) G contains *inverses* of elements. That is, for every $g \in G$, there is an element $h \in G$ such that

$$g * h = h * g = e,$$

where e is the identity element of G .

So, for example, \mathbb{Z} with addition is a group. Note that the operation is not required to be commutative. An example of a group with a non-commutative operation is the group of two-by-two matrices over \mathbb{R} with multiplication.

In an arbitrary group, the binary operation is often denoted by juxtaposing two elements (as in multiplication), so that ab means the operation performed on a and b .

The theory of groups is a huge subject, so we restrict ourselves to only a few facts and notions. Firstly, the identity element and inverses in groups are unique (prove this as an exercise). Secondly, groups have the left and right *cancellation* property. That is, for all $a, b, c \in G$, $ab = ac$ implies $b = c$, and $ab = cb$ implies $a = c$. A *subgroup* of a group G is a subset of G which forms a group under the same operations as H . For example, the set of even integers is a subgroup of \mathbb{Z} under addition.

Example 4. Let a and b be two elements in a group such that $aba = ba^2b$, $a^3 = e$, and $b^{2n-1} = e$ for some positive integer n . Prove that $b = e$, where e is the identity element.

Problem 9. Let G be a set with an associative binary operation such that for all $a, b \in G$, $a^2b = b = ba^2$. Show that G is a group and the operation is commutative.

Problem 10. Let A be a subset of a finite group G such that A contains more than half of the elements of G . Prove that each element of G is the product of two elements of A .

Problem 11. Prove that no group is a union of two proper subgroups (that is, subgroups which are not the group itself).

Problem 12. Let S be a nonempty set with an associative binary operation with the left and right cancellation properties. Assume that for every $a \in S$, the set $\{a^n \mid n = 1, 2, 3, \dots\}$ is finite. Must S be a group?