OLGA RADKO MATH CIRCLE: ADVANCED 3

FERNANDO FIGUEROA, ROHAN JOSHI, JOAQUÍN MORAGA, AND CALEB PARTIN

Worksheet 4: Polynomials over finite fields

In general we can have polynomials over more variables, and when we add and multiply them we have to consider the degrees of all the variables. $F[x, y]$ will be the set of polynomials over F with two variables.

Problem 4.0: Expand the following polynomials, each of them over $\mathbb{Z}[x, y]$, $\mathbb{F}_3[x, y]$ and $\mathbb{F}_5[x, y]$

- $(x + y + 1)(x + y + 2)$
- $(xy + x)(y + 2)$
- $(x + y + 1)^3$

Solution 4.0:

For a polynomial $p(x, y)$ in $F[x, y]$ a *solution* is a pair (a, b) with a and b both in F, such that $p(a, b) = 0$.

Problem 4.1: Determine the solutions of these polynomials.

- $x^3 + x^2 - 2x - y$ in $\mathbb{F}_3[x, y]$
- $-x + y^2 - y + 1$ in $\mathbb{F}_3[x, y]$
- $x^2 - 1$ in $\mathbb{F}_5[x, y]$

Solution 4.1:

We can graph the solutions of polynomials in a grid $F \times F$

Problem 4.2: Graph the solutions of the polynomials from the previous problem. Graph them also in $\mathbb{Z}[x, y]$ and $\mathbb{R}[x, y]$. Compare these graphs.

Solution 4.2:

The degree of a monomial in $F[x,y]$ is the sum of its degree in x and its degree in y. A polynomial is called *homogeneous* if all of its monomials have the same degree. Finding the solutions of a homogeneous polynomial in $F[x,y]$ can be done by using an auxiliary variable $t = x/y$. For example, for the following polynomial in $\mathbb{F}_2$:

$$x^3 + x^2y + xy^2 + y^3 = y^3((\frac{x}{y})^3 + (\frac{x}{y})^2 + (\frac{x}{y}) + 1) = y^3(t^3 + t^2 + t + 1)$$

Because we used the auxiliary variable $t = x/y$, which is divided by y, we will only find the solutions where y isn't zero using this auxiliary variable. Therefore the only solutions with $y \neq 0$ make $t^3 + t^2 + t + t = 0$, so $t = 1$ and so $x = y = 1$.We can see that if $y = 0$, then $x = 0$.Therefore the solutions are $(0,0)$ and $(1,1)$.

Problem 4.3: Determine the solutions of the following polynomials and graph them.

- $x^3 + x^2y - 2xy^2 - y^3$ in $\mathbb{F}_3[x,y]$
- $x^3y + y^4$ in $\mathbb{F}_3[x,y]$
- $x^4 + x^3 + x^3y + x^2y - 2x - 2$ in $\mathbb{F}_5[x,y]$

Solution 4.3:

We say that a polynomial $p(x)$ is identically zero if $p(a) = 0$ for any element a. Similarly, $p(x, y)$ is identically zero if $p(a, b) = 0$ for any pair of elements (a, b).

Problem 4.4: Let F be finite field.

- Show that a non-zero polynomial in $\mathbb{Z}[x]$ is never identically zero.
- Show that a non-zero polynomial in $\mathbb{Z}[x, y]$ is never identically zero.
- Can a non-zero polynomial in $F[x]$ be identically zero, what can you say of the degree of this polynomial?
- Can a non-zero polynomial in $F[x, y]$ be identically zero, what can you say of the degree of this polynomial?

Solution 4.4:

Problem 4.5: Let F be a finite field. Show that in $F[x, y]$, there are irreducible polynomials of degree at least d for any positive number d.

Hint: Show that there are infinitely many distinct irreducible polynomials.

Solution 4.5:

Problem 4.6: Determine if the following polynomials are irreducible or factor them:

- $x^4 + x^3 + x^2 + x - 1$ in $\mathbb{F}_3[x, y]$
- $x^4 + x^3y + x^2y^2 + xy^3 - y^4$ in $\mathbb{F}_3[x, y]$
- $x^4 + x^2y^2 + xy^3 + y^4$ in $\mathbb{F}_5[x, y]$

Solution 4.6:

Any irreducible polynomial $p(x)$ of degree d in $\mathbb{F}_p[x]$ divides the polynomial $x^{p^d} - 1$

Problem 4.7: Show that $x^{10} + x^3 + 1$ is irreducible in $\mathbb{F}_2[x]$.

Hint: Euclid's algorithm for greatest common divisors, also works for polynomials over a field.

Solution 4.7:

Problem 4.8: Find all irreducible polynomials of degree 5 in $\mathbb{F}_2[x]$
Solution 4.8:

UCLA Mathematics Department, Los Angeles, CA 90095-1555, USA.
Email address: fzamora@math.princeton.edu

UCLA Mathematics Department, Los Angeles, CA 90095-1555, USA.
Email address: rohansjoshi@math.ucla.edu

UCLA Mathematics Department, Box 951555, Los Angeles, CA 90095-1555, USA.
Email address: jmoraga@math.ucla.edu

UCLA Mathematics Department, Los Angeles, CA 90095-1555, USA.
Email address: ctpartin@math.ucla.edu