OLGA RADKO MATH CIRCLE: ADVANCED 3

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

Worksheet 3: Introduction to polynomials over finite fields

The set of polynomials with one variable x over a field F is denoted by $F[x]$. Addition is performed by adding up the coefficients of monomials of the same degree, while multiplication is performed by multiplying the coefficients in the field and adding up the degrees of the monomials x^i, respecting the distributive property.

Problem 3.1: Expand the following polynomials, each of them over $\mathbb{F}_3[x]$, $\mathbb{F}_5[x]$ and $\mathbb{R}[x]$

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

Solution 3.1:

For a polynomial $p(x)$ in $F[x]$, a solution α is an element of F that satisfies $p(\alpha) = 0$. A polynomial with integer coefficients can be seen as a polynomial with coefficients over a finite field $\mathbb{F}_p$ by taking the coefficients $\pmod{p}$.

Problem 3.2:

What are the solutions of $p(x) = x^2 - 1$ in $\mathbb{F}_2[x]$? What about $\mathbb{F}_3[x]$? What about any $\mathbb{F}_p[x]$?

Can you find a polynomial $p(x)$ with integer coefficients that does not have any common solutions when you see it as a polynomial over two different finite fields?

Solution 3.2:

Problem 3.3: Does $x^2 + 1$ have any solutions as a polynomial in $\mathbb{Q}[x]$? What about as a polynomial in $\mathbb{F}_2[x]$ or $\mathbb{F}_3[x]$?

Solution 3.3:

Problem 3.4: Expand the following polynomials:

- $(x+1)^2$ in $\mathbb{F}_2[x]$
- $(x+2)^5$ in $\mathbb{F}_5[x]$
- $(x+a)^p$ in $\mathbb{F}_p[x]$, where a is an element in $\mathbb{F}_p$

Solution 3.4:

We can factor (some) polynomials by using similar techniques as the ones used for polynomials over the integers, rationals, or real numbers. Factorizations for polynomials over a field are unique (up to multiplication by constants).

Problem 3.5: Factor the following polynomials

- $x^2 + 3$ in $\mathbb{F}_7[x]$
- $x^3 + 2$ in in $\mathbb{F}_5[x]$

Solution 3.5:

Problem 3.6: Let F be a field. Show that a degree d polynomial $p(x)$ in $F[x]$ has at most d solutions.
Solution 3.6:

The integers $\mathbb{Z}$ are not a field, but we still have polynomials over $\mathbb{Z}$. Polynomials can be defined over a set with well-behaved product and addition, such as $\mathbb{Z}/m\mathbb{Z}$.

Problem 3.7: Can you find a degree d polynomial with more than d solutions in some $\mathbb{Z}/m\mathbb{Z}[x]$?

Solution 3.7:

We say that a polynomial $p(x)$ of positive degree is irreducible, if whenever you have $p(x) = q(x)r(x)$, then either $q(x)$ or $r(x)$ is a constant (degree zero).

Problem 3.8: Prove that $x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$

Can you find a degree 3 irreducible polynomial in $\mathbb{F}_2[x]$.

Solution 3.8:

Problem 3.9: Find an example of a polynomial $p(x)$ that is irreducible in $\mathbb{Z}[x]$, but can be factored in some $\mathbb{F}_2[x]$.

Can such an example be found for any $\mathbb{F}_p[x]$?

Are there polynomials that are irreducible in some $\mathbb{F}_p[x]$ but can be factored in $\mathbb{Z}[x]$?

Solution 3.9:

Problem 3.10: Can you find a polynomial in some $\mathbb{Z}/m\mathbb{Z}[x]$ that can be factored in more than one way? Does such a polynomial exist for any m that is not a prime number?

Solution 3.10:

Problem 3.11: Show that the polynomial $x^p - x$ in $\mathbb{F}_p[x]$ has every element of $\mathbb{F}_p$ as a solution.
Solution 3.11:

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