OLGA RADKO MATH CIRCLE: ADVANCED 3

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

Worksheet 2:

For a prime number p, we define $\mathbb{F}_p$ (read as 'the field of p elements) to'be the set of integers $\{0, 1, 2, \dots, p-1\}$. In $\mathbb{F}_p$ we define the sum of two numbers $a+b$, to be the only integer c in the set $\{0, 1, 2, \dots, p-1\}$, such that $c \equiv a+b \pmod{p}$. In the same way $a \cdot b$ is the only integer d in the set $\{0, 1, 2, \dots, p-1\}$, such that $d \equiv a \cdot b \pmod{p}$.

Problem 2.0: Simplify the following expressions

- $(2+3) \cdot 4$ in $\mathbb{F}_5$
- $5 - (2+3) \cdot 4$ in $\mathbb{F}_7$
- $10 + (3+2)^2$ in $\mathbb{F}_{11}$
- $2 + (1 + 2 \cdot 2)^4$ in $\mathbb{F}_3$

Solution 2.0:

For the field $\mathbb{F}_p$, 0 is called the "additive identity", because $a + 0 = a = 0 + a$. 1 is called the "multiplicative identity", because $a \cdot 1 = a = 1 \cdot a$.

We say that c has an additive inverse d, if $c + d = 0$.

Problem 2.1: Show that in $\mathbb{F}_2$ and $\mathbb{F}_3$, every element has an additive inverse. Does this hold true for any $\mathbb{F}_p$?

Solution 2.1:

We say that a non-zero element a is a zero-divisor if there exists some non-zero element b, such that $a \cdot b = 0$.

Problem 2.2: Is any non-zero element in $\mathbb{F}_p$ a zero-divisor?

Solution 2.2:

More generally, we can define $\mathbb{Z}/m\mathbb{Z}$ to be the set $\{0, 1, 2, \ldots, m-1\}$ with addition and multiplication defined using congruence mod m, for any positive integer m. Hence $\mathbb{F}_p$ is the same as $\mathbb{Z}/p\mathbb{Z}$.

Problem 2.3: Do all elements have an additive inverse in $\mathbb{Z}/m\mathbb{Z}$?

Solution 2.3:

We say that b has a multiplicative inverse a if $b \cdot a = 1$.

Problem 2.4: Find the multiplicative inverses for all non-zero elements in $\mathbb{Z}/5\mathbb{Z}$.

Solution 2.4:

Problem 2.5: Which numbers in $\mathbb{Z}/4\mathbb{Z}$ have a multiplicative inverse? Which elements in $\mathbb{Z}/4\mathbb{Z}$ are zero-divisors.
Solution 2.5:

Prove that if an element has a multiplicative inverse, then it cannot be a zero-divisor.

Problem 2.6:

Solution 2.6:

A "field" is defined as a set F, with two operations "addition" and "multiplication" that satisfy the following properties:

- Associativity of addition and multiplication: $a + (b + c) = (a + b) + c$, and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- Commutativity of addition and multiplication: $a + b = b + a$, and $a \cdot b = b \cdot a$.
- Additive and multiplicative identity: there exist two distinct elements 0 and 1 in F such that $a + 0 = a$ and $a \cdot 1 = a$.
- Additive inverses: for every a in F, there exists an element in F, denoted $-a$, called the additive inverse of a, such that $a + (-a) = 0$.
- Multiplicative inverses: for every non-zero a in F, there exists an element in F, denoted by a^{-1}, called the multiplicative inverse of a, such that $a \cdot a^{-1} = 1$.
- Distributivity of multiplication over addition: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Problem 2.7:

- Show that $\mathbb{F}_p$ are fields for any prime number p.
- Show that $\mathbb{Z}/m\mathbb{Z}$ is not a field whenever m is not prime.

Solution 2.7:

The goal of the next problems is to create the field of 4 elements.

We will define $\mathbb{F}_4$ to be the set of degree 0 or 1 polynomials, with coefficients in $\mathbb{F}_2$, define the addition of two polynomials $(ax + b) + (dx + e) = (a + d)x + (b + e)$, i.e. add them as you would do with integer coefficients, and then reduce mod p.

Problem 2.8: Prove that every element has an additive inverse in $\mathbb{F}_4$

Solution 2.8:

We define the multiplication in the following way. To multiply polynomials $f(x)$ and $g(x)$, first multiply them as if the coefficients where integers. Then we take the residue (also known as remainder) after dividing by $x^2 + x + 1$ and we finally reduce the coefficients modulo 2

Problem 2.9: Prove that this set is a field. If we took the residue after dividing by $x^2 + 1$. Would this still be a field?

Solution 2.9:

Problem 2.10:

Can you create the field of 9 elements, by using degree 0 or 1 polynomials with coefficients in $\mathbb{F}_3$?

Hint: You need to take the residue after dividing by a degree two polynomial that cannot be written as the product of two degree one polynomials.

Can you extend this construction to create fields of p^2 elements?

Solution 2.10:

We have created fields of 2, 3, 4, 5, 7, 9 elements.

Problem 2.11: Can there be a field of 6 elements? Can there be a field of 8 elements?

Solution 2.11:

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