TW314 Lecture 20 (We 15 Mar. 2017)

FINITE FIELDS

Definition 2.3 A field $(F, +, \cdot)$ is a set F together with two binary operations $+$ and $\cdot$ such that

1. $(F, +)$ is an abelian group.
2. $(F - \{0\}, \cdot)$ is an abelian group, where 0 denote the identity element of $(F, +)$.
3. For any $a, b, c \in F$, $a \cdot (b+c) = a \cdot b + a \cdot c$ — this is known as the distributive law.

We usually let 0 denote the identity element of the group $(F, +)$ and call it the additive identity or zero — by 1 we denote the identity element of the group $(F - \{0\}, \cdot)$ and call it the multiplicative identity or unity. The inverse of a in $(F, +)$ is denoted by $-a$ and is called the additive inverse of a. The inverse of a in $(F - \{0\}, \cdot)$ is denoted by a^{-1} and is called the multiplicative inverse of a. Also, we agree to write ab instead of $a \cdot b$.

• Example $(\mathbb{R}, +, \cdot)$ is a field, but $(\mathbb{Z}, +, \cdot)$ is not a field. Why?

Theorem 2.1

If $a, b \in \mathbb{Z}$ with $b > 0$, then there exists $q, r \in \mathbb{Z}$ with $0 \leq r < b$ such that $a = qb + r$.

Furthermore, the quotient q and the remainder r are unique.

Definition 2.4 Let $m \in \mathbb{Z}$ with $m > 0$.

For $a, b \in \mathbb{Z}$, a is congruent to b modulo m if $a - b$ is divisible by m.

If a is congruent to b, we write $a \equiv b \pmod{m}$.

Note that congruence modulo m is an equivalence relation on the set $\mathbb{Z}$, that is

1. For all $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$ ← reflexivity

2. $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$ ← symmetry

3. $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m} = a \equiv c \pmod{m}$

↑ transitivity.

• Since congruence modulo m is an equivalence relation, we have a natural partition of $\mathbb{Z}$ into equivalence classes. Denote the equivalence class of $a \in \mathbb{Z}$ by $[a]_m$, that is

$$[a]_m = \{ a' \in \mathbb{Z} : a' - a \text{ is divisible by } m \}.$$

• Example The equivalence classes with respect to congruence modulo 3 is

$$[0]_3 = \{ \ldots, -3, 0, 3, 6, \ldots \}$$

$$[1]_3 = \{ \ldots, -2, 1, 4, 7, \ldots \}$$

$$[2]_3 = \{ \ldots, -1, 2, 5, 8, \ldots \}$$

Of course $[0]_3 = [3]_3 = [6]_3$ et cetera and $[1]_3 = [4]_3 = [7]_3$ et cetera, but we choose 0, 1 and 2 as the representatives of the equivalence classes, since these are the unique remainders when we divide by 3.

In general, the equivalence classes with respect to congruence modulo m is

$$[0]_m, [1]_m, \ldots, [m-1]_m.$$