

MATH 513: LINEAR ALGEBRA

ASSIGNMENT 1

HARM DERKSEN

The **Challenging Problems** are due on Friday, September 14 at noon in class. You do **not** have to hand in the routine problems. On a quiz on Monday, September 17, similar problems may appear. It is optional to hand in the **Very Challenging Problems** (but the same deadline applies). These problems will be very hard. You can earn extra credit with the very challenging problems (but they will be graded more strictly).

READING

Read Chapter 1 of Curtis and the section “Modular Arithmetic” below. For Monday, September 10, read Section 3. For Wednesday, September 12, read Section 4.

MODULAR ARITHMETIC

Let \mathbb{Z} be the integers. If a and b are integers we write

$$a + b\mathbb{Z} = \{\dots, a - 2b, a - b, a, a + b, a + 2b, \dots\}$$

which is called a *congruence class modulo b* . Remark that we have for example

$$2 + 3\mathbb{Z} = 11 + 3\mathbb{Z}$$

because $11 - 2$ is divisible by 3. In general $a_1 + b\mathbb{Z}$ and $a_2 + b\mathbb{Z}$ are the same if and only if $a_1 - a_2$ is divisible by b . In such case we say that a_1 and a_2 are *congruent modulo b* , and we sometimes write

$$a_1 \equiv a_2 \pmod{b}.$$

We define $\mathbb{Z}/b\mathbb{Z}$ as the set of all congruence classes modulo b :

$$\mathbb{Z}/b\mathbb{Z} = \{a + b\mathbb{Z} \mid a \in \mathbb{Z}\} = \{b\mathbb{Z}, 1 + b\mathbb{Z}, 2 + b\mathbb{Z}, \dots, (b - 1) + b\mathbb{Z}\}$$

Note that if a is any integer, we can always find an element in $\{0, 1, 2, \dots, b - 1\}$ which is congruent to a modulo b . The set $\mathbb{Z}/b\mathbb{Z}$ consists of exactly b congruence classes. We can also define addition and multiplication on $\mathbb{Z}/b\mathbb{Z}$ as follows:

$$(1) \quad (a_1 + b\mathbb{Z}) + (a_2 + b\mathbb{Z}) = (a_1 + a_2) + b\mathbb{Z}$$

$$(2) \quad (a_1 + b\mathbb{Z}) \cdot (a_2 + b\mathbb{Z}) = (a_1 \cdot a_2) + b\mathbb{Z}.$$

The first question we should ask here is: *Is this well defined?* Since $a_1 + b\mathbb{Z}$ represents the same congruence class for different choices of a_1 , we must show that the definition in (1) does not depend on the choice of the a_1 . Suppose a'_1 is congruent to a_1 and a'_2 is congruent to a_2 . Then we must show that

$$(a_1 + a_2) + b\mathbb{Z} = (a_1 + b\mathbb{Z}) + (a_2 + b\mathbb{Z}) = (a'_1 + b\mathbb{Z}) + (a'_2 + b\mathbb{Z}) = (a'_1 + a'_2) + b\mathbb{Z}.$$

Now this is clearly true: b divides $(a'_1 + a'_2) - (a_1 + a_2) = (a'_1 - a_1) + (a'_2 - a_2)$ because b divides both $a'_1 - a_1$ and $a'_2 - a_2$.

In a similar fashion we can show that the multiplication in (2) is well-defined. Again, suppose that a'_1 is congruent to a_1 and a'_2 is congruent to a_2 modulo b . We have to show that $a_1 a_2$ and $a'_1 a'_2$ are congruent modulo b . Indeed, b divides

$$a'_1 a'_2 - a_1 a_2 = a'_1 (a'_2 - a_2) + a_2 (a'_1 - a_1)$$

because b divides $a'_2 - a_2$ and $a'_1 - a_1$.

We have created the number system $\mathbb{Z}/b\mathbb{Z}$.

ROUTINE PROBLEMS

1. Do Curtis, Section 2, page 14, Exercise 1 (both parts).
2. Show that $\mathbb{Z}/b\mathbb{Z}$ as defined above satisfies the field axioms 1-5 (Definition 2.1, Section 2, page 8). Note that

$$\mathbf{0} = b\mathbb{Z}$$

is the zero element of $\mathbb{Z}/b\mathbb{Z}$ and

$$\mathbf{1} = 1 + b\mathbb{Z}$$

is the one element of $\mathbb{Z}/b\mathbb{Z}$. Also show that if $b \geq 2$, then $\mathbb{Z}/b\mathbb{Z}$ satisfies axiom 6 as well.

CHALLENGING PROBLEMS

1. Do Curtis, Section 2, Exercise 3 on page 15. (There is a typo in this exercise. It should say $\binom{n}{0} = \binom{n}{n} = 1$ instead of $\binom{n}{0} = \binom{n}{1} = 1$.)
2. Prove (2.12) in Chapter 1, Section 2 on page 13. Use **only** the definition of a field. Show exactly where you use which axiom. Also, be careful to put parenthesis in the right places everywhere. You can mimmick the proof of (2.8).
3. Prove that if p is a prime number, then $\mathbb{Z}/p\mathbb{Z}$ satisfies field axiom 7 as well. Since we already have shown that the other axioms are true, we conclude that $\mathbb{Z}/p\mathbb{Z}$ is a field!
4. Suppose that F_0 is a subfield of \mathbb{R} (for example \mathbb{Q}). Define

$$F = \{a + b\sqrt{2} \mid a, b \in F_0\}.$$

Show that F is also a field.

Remark: The field $\mathbb{Z}/p\mathbb{Z}$ is often denoted by \mathbb{F}_p . It is known (but we will not prove this now) that for every prime power $q = p^r$ there exists (a unique) field \mathbb{F}_q with q elements.

VERY CHALLENGING PROBLEMS

1. Prove *Fermat's Little Theorem*: If p is a prime, and a is not divisible by p then

$$a^{p-1} \equiv 1 \pmod{p}.$$

(*Hint:* First show that

$$\{1 + p\mathbb{Z}, 2 + p\mathbb{Z}, \dots, (p-1) + p\mathbb{Z}\} = \{a + p\mathbb{Z}, 2a + p\mathbb{Z}, \dots, (p-1)a + p\mathbb{Z}\}$$

Then take products over the set on the left hand side and the product over the set on the right hand side and compare.)