

# Math 49 (3)

## Midterm

Write all of your work in your bluebooks. You may write the problems in any order you like, but do not put work for more than one problem on the same page of your bluebook. When you are done, number the pages of your bluebook(s) and make a table of contents on the cover of the first one indicating which problems you worked and which pages I can find them on.

**Problem 1.** In this problem, all variables refer to elements of  $\mathbb{Z}$ .

a) Find the greatest common divisor,  $d = (78, 36)$ .

*Solution.* We use the Euclidean algorithm, although other methods are also acceptable. Successive divisions give the results:

$$78 = (36)(2) + 6 \quad (1)$$

$$36 = (6)(6) + 0 \quad (2)$$

The last nonzero remainder is 6, so  $d = 6$ . □

b) For the  $d$  you found in part a) of this problem, find integers  $s$  and  $t$  so that  $78s + 36t = d$ .

*Solution.* Using the results of the calculation in equation (1), we get

$$6 = (78)(1) + (36)(-2).$$

□

c) Is 36 a unit in  $\mathbb{Z}_{78}$ ? If so, find  $36^{-1}$ . If not, say why not.

*Solution.* No. I'll give two complete arguments:

6 divides 36 and 6 divides 78 but if  $36 \cdot a \equiv 1 \pmod{78}$  we would have  $36a - 1 = n78$  for some  $n \in \mathbb{Z}$  which would imply  $(36, 78) = 1$  which contradicts our previous work.

Working modulo 78, we have  $36 \cdot 13 \equiv -6 \cdot 13 \equiv 0$ , so if  $36a \equiv 1$  we would have  $13 \equiv a \cdot 36 \cdot 13 \equiv 0$  which is a contradiction.  $\square$

d) Is  $\mathbb{Z}_{78}$  a field? If so, give a one sentence justification. If not, say why not.

*Solution.* No,  $35 \neq 0$  in  $\mathbb{Z}_{78}$ , but 36 is not a unit. In a field, all nonzero elements are units.  $\square$

**Problem 2.** In this problem, all variable polynomials refer to elements of  $\mathbb{Z}_3[x]$ . (Note carefully: I used  $\mathbb{Z}_3$  here instead of  $\mathbb{Z}$ . If you overlook that fact, the following computations become much more ugly.)

a) Find the greatest common divisor  $d(x) = (x^4 + 2x^3 + 2x^2 + 2x + 1, x^3 + 2)$

*Solution.* In this solution, to simplify the typing and the calculations, we represent  $\mathbb{Z}_3$  as  $\{0, 1, -1\}$ . We proceed according to the Euclidean algorithm. The successive divisions yield the following equations.

$$x^4 - x^3 - x^2 - x + 1 = (x - 1)(x^3 - 1) - (x^2) \quad (3)$$

$$x^3 - 1 = (x)(x^2) - (1) \quad (4)$$

The next remainder is clearly going to be zero, so  $d(x) = 1$ .  $\square$

b) For the  $d(x)$  you found in part a) of this problem, find  $s(x), t(x) \in \mathbb{Z}_3[x]$  so that

$$s(x)(x^4 + 2x^3 + 2x^2 + 2x + 1) + t(x)(x^3 + 2) = d(x).$$

*Solution.* Using equations (3) and (4), we get

$$\begin{aligned} 1 &= (x)(x^2) - (x^3 - 1) \\ &= x((x - 1)(x^3 - 1) - (x^4 - x^3 - x^2 - x + 1)) - (x^3 - 1) \\ &= (x^2 - x - 1)(x^3 - 1) - (x)(x^4 - x^3 - x^2 - x + 1) \end{aligned}$$

$\square$

- c) Is  $x^3 + 2$  a unit in  $\mathbb{Z}_3[x]/(x^4 + 2x^3 + 2x^2 + 2x + 1)$ ? If so, find  $(x^3 + 2)^{-1}$ . If not, say why not.

*Solution.* Yes, because we can find an inverse,  $x^2 - x - 1 = (x^3 + 2)^{-1}$  by the above calculation.  $\square$

- d) Is  $\mathbb{Z}_3[x]/(x^4 + 2x^3 + 2x^2 + 2x + 1)$  a field? If so, give a one sentence justification, if not, say why not.

*Solution.* No.  $(-1)^4 - (-1)^3 - (-1)^2 - (-1) + 1 = 1 + 1 - 1 + 1 + 1 = 0$ , so  $x + 1$  divides  $x^4 - x^3 - x^2 - x + 1$ , so  $x + 1$  is not a unit in  $\mathbb{Z}_3/(x^4 - x^3 - x^2 - x + 1)$ . (See previous problem for a more detailed justification.)  $\square$

### Problem 3.

- a) Let  $R, S$  be rings. Give the definition of homomorphism. That is to say, state exactly what it means for  $f : R \rightarrow S$  to be a homomorphism.

*Solution.*  $f$  is a homomorphism if the following two equalities hold for every pair of elements  $a, b \in R$ :

$$f(a + b) = f(a) + f(b)$$

$$f(ab) = f(a)f(b).$$

$\square$

- b) Prove that if  $f : R \rightarrow S$  is a homomorphism, then  $f(a - b) = f(a) - f(b)$ .

*Solution.* Here we will use only the definition of ring, the definition of homomorphism and the definition of “ $-$ .” Recall that  $-$  is defined by  $a - b := a + (-b)$  where  $-b$  is the unique element such that  $b - b = 0$ . We then have

$$\begin{aligned} f(a - b) &= f(a - b) + 0 \\ &= f(a - b) + (f(b) - f(b)) = (f(a - b) + f(b)) - f(b) \\ &= f((a + (-b)) + b) - f(b) = f(a + (b - b)) - f(b) \\ &= f(a + 0) - f(b) = f(a) - f(b). \end{aligned}$$

$\square$

**Problem 4.** In this problem,  $R$  is a commutative ring with identity element and  $I$  and  $J$  are ideals in  $R$ . We define a set  $K \subseteq R$  by the equation

$$K := \{r \in R \mid rj \in I \text{ for all } j \in J.\}.$$

Prove that  $K$  is an ideal in  $R$  and that it contains  $I$ .

*Solution.* To show that  $K$  is an ideal we need to show that for every  $k_1, k_2 \in K$  and every  $r \in R$  we have

i)  $k_1 + k_2 \in K$ .

ii)  $-k_1 \in K$ .

iii)  $k_1 r \in K$ .

We address these individually using the notation already established.

i) The definition of  $K$  gives us that for every  $j \in J$  we have  $jk_1$  and  $jk_2$  are elements of  $I$ . Since  $I$  is an ideal we then have  $j(k_1 + k_2) = jk_1 + jk_2 \in I$  for all  $j \in J$ . But this is exactly the definition of the membership  $(k_1 + k_2) \in K$ .

ii) The definition of  $K$  gives us that for every  $j \in J$  we have  $jk_1 \in I$ . So  $j(-k_1) = (-j)k_1 \in I$  by the properties of  $-$  and because  $I$  is an ideal. This is exactly the definition of the membership  $-k_1 \in K$ .

iii) The definition of  $K$  gives us that for every  $j \in J$  we have  $jk_1 \in I$ . So  $j(rk_1) = (rj)k_1 \in I$  for every  $j \in J$ . This is exactly the definition of membership  $rk_1 \in K$ .

Hence,  $K$  is an ideal. To see that  $K \supseteq I$  let  $i \in I$  then  $ij \in I$  for every  $j \in J$  (in fact  $ir \in I$  for every  $r \in R$ ) because  $I$  is an ideal. This is exactly the definition of membership  $i \in K$ .  $\square$