

## Problem Session 2

Manuel de Lecha

6) Prove that  $\mathbb{Z}[x]$  is not an Euclidean domain.

Let  $R$  be an integral domain. A Euclidean function  $f: R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$  is one such that satisfies the following property:

EF) If  $a, b$  are in  $R$  and  $b$  is nonzero, then there exist  $q$  and  $r$  in  $R$  such that  $a = bq + r$  and either  $r = 0$  or  $f(r) < f(b)$ .

Then, an Euclidean domain is an integral domain which can be endowed with at least one Euclidean function.

Lemma: Every Euclidean domain is a PID.

Let  $I$  be a nonzero proper ideal of  $D$ . Let  $a \in I$  such that  $d(a) := \min_{0 \neq x \in I} d(x)$

We claim that  $I$  is generated by  $a$ .

Suppose not,  $\exists b \in I$  such that it is not a multiple of  $a$ . Hence, by the properties of a ED,  $\exists r \in D$  such that  $b = aq + r$  with  $d(r) < d(a)$ .

Therefore,  $r = b - aq \in I$  and  $d(r) = \min_{0 \neq x \in I} d(x)$  is contradicted.

□ QED

3)  $\mathbb{Z}[x]$  is not a PID, since  $\mathbb{Z}$  is not a field.

2)  $\langle x, 2 \rangle$  is a proper ideal, but not principal.

5)  $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$  which is not a field

↑  
irreducible so it should be maximal & PID but  $\mathbb{Z}$  is not a field.

6) What is the least non-negative integer  $f$  with  $f \equiv 2 \pmod{3}$ ,  $f \equiv 3 \pmod{5}$ ,  $f \equiv 2 \pmod{7}$ .

First of all, we can notice that  $3, 5, 7$  are pairwise coprime

Let  $M = 105$

Chinese Remainder

$$M_1 = 105/3 = 35 \quad 35 \cdot 2 \equiv 1 \pmod{3}$$

Algorithm.

$$M_2 = 105/5 = 21 \quad 21 \equiv 1 \pmod{5}$$

$$M_3 = 105/7 = 15 \quad 15 \equiv 1 \pmod{7}$$

$$x = 2 \cdot M_1 \cdot 2 + 3 \cdot M_2 \cdot 1 + 2 \cdot M_3 \cdot 1 = 233 \equiv 23 \pmod{105}$$

3) Let  $R$  be an Euclidean Domain  $f, g \in R$ . Show that  $\langle f, g \rangle$  and  $\langle \gcd(f, g) \rangle$  coincide.

$R \text{ ED} \Rightarrow \text{PID} \Rightarrow \text{it must exist } a \in R \text{ s.t. } \langle f, g \rangle = \langle a \rangle$

$$d = \gcd(f, g) \Leftrightarrow d \mid f, d \mid g \text{ and } d = sf + tg \text{ for } s, t \in R \Leftrightarrow \langle d \rangle \subseteq \langle f, g \rangle \quad \text{②}$$

$$\langle d \rangle \supseteq \langle f, g \rangle \quad \text{①}$$