

### 4400/6400 PROBLEM SET 3

A sufficient number of problems: 4 for 4400 students, 6 for 6400 students.

3.1) Let  $c$  and  $N > 1$  be integers, and let  $\bar{c}$  be the class of  $c$  modulo  $N$ .

- a) Show that  $\bar{c}$  is a unit in  $\mathbb{Z}/N\mathbb{Z}$  if and only if  $\gcd(c, N) = 1$ .
- b) Show that  $\#(\mathbb{Z}/N\mathbb{Z})^\times \leq N - 1$ , with equality holding if and only if  $N$  is prime.

3.2) Let  $m$  and  $b$  be real numbers, and consider the line

$$\ell : y = mx + b.$$

- a) Show that the only possibilities for the number of  $\mathbb{Q}$ -rational points  $(x, y)$  on  $\ell$  are: none, exactly one, infinitely many.
- b) Suppose  $m$  and  $b$  are both rational. Show  $\ell$  has infinitely many rational points.
- c) Suppose  $m$  is rational and  $b$  is irrational. Show  $\ell$  has no rational points.
- d) Suppose  $m$  is irrational and  $b$  is rational. Show  $\ell$  has exactly one rational point.
- e) What can be said when  $m$  and  $b$  are both irrational?

3.3) (Converse of Wilson's Theorem) Let  $N > 1$  be such that

$$(N - 1)! \equiv -1 \pmod{N}.$$

Show that  $N$  is prime.

3.4)\* Let  $D$  be a squarefree integer which is not 0 or 1, and put

$$R_D := \mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\} \cong \mathbb{Z}[t]/(t^2 - D).$$

Thus  $R_D$  is the subring of the complex numbers obtained by adjoining  $\sqrt{D}$  to  $\mathbb{Z}$ .

a) Show that  $R_D$  is an integral domain, with fraction field

$$\mathbb{Q}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}.$$

b) Suppose  $D > 1$ , so that  $\mathbb{Z}[\sqrt{D}]$  is a subring of  $\mathbb{R}$ . Show that  $\mathbb{Z}[\sqrt{D}]$  is dense in  $\mathbb{R}$ : for any real numbers  $x < y$ , there exist  $a, b \in \mathbb{Z}$  such that  $x < a + b\sqrt{D} < y$ .

3.5) We maintain the notation of the previous problem. Define the **norm map**  $N : \mathbb{Q}[\sqrt{D}] \rightarrow \mathbb{Q}$  by  $N(a + b\sqrt{D}) = |(a + b\sqrt{D})(a - b\sqrt{D})| = |a^2 - Db^2|$ . Note that the absolute value is superfluous if  $D < 0$ .

- a) Show that  $N$  is multiplicative: for all  $\alpha, \beta \in \mathbb{Q}[\sqrt{D}]$ ,  $N(\alpha\beta) = N(\alpha)N(\beta)$ .
- b) Show that, for  $\alpha \in \mathbb{Q}[\sqrt{D}]$ ,  $N(\alpha) = 0 \iff \alpha = 0$ .
- c) Show that, for  $\alpha \in R_D$ ,  $N(\alpha) = 1 \iff \alpha \in R_D^\times$  (that is, the norm 1 elements of  $R_D$  are precisely the units of  $R_D$ ).
- d) Suppose  $D = -1$ . Show that  $R_D$  has exactly 4 units and find them explicitly.
- e) Suppose  $D < -1$ . Show that the units in  $R_D$  are  $\pm 1$ .
- f) Suppose that  $\alpha \in R_D$  is such that  $N(\alpha)$  is a prime number. Show that  $\alpha$  is an irreducible element of  $R_D$ . Does the converse hold?

3.6) Let  $R$  be a commutative ring which is not the zero ring. We say that a function  $N : R \rightarrow \mathbb{N}$  is a **weak norm** if it satisfies

(WN1)  $N(0) = 0, 0 \neq x \in R \implies N(x) \neq 0$ , and

(WN2) For all  $x, y \in R, N(xy) = N(x)N(y)$ .

a) Suppose  $N$  is a weak norm on  $R$ . Show that for all  $x \in R^\times, N(x) = 1$ .

b) Suppose that  $R$  admits a weak norm  $N$ . Show that  $R$  is an integral domain.

c) For any ring  $R$ , define a function  $N_0 : R \rightarrow \mathbb{N}$  by  $N_0(0) = 0, N_0(R \setminus \{0\}) = \{1\}$ . Show that if  $R$  is an integral domain, then  $N_0$  is a weak norm.

d) Conclude: a commutative ring is a domain if and only if it admits a weak norm.

e) Let  $N$  be a weak norm on  $R$ , and let  $K$  be the fraction field of  $R$ . Show that  $N(\frac{x}{y}) := \frac{N(x)}{N(y)}$  extends  $N$  to a well-defined function from  $R$  to  $\mathbb{Q}^{\geq 0}$  which satisfies the analogous property: for  $\alpha, \beta \in K, N(\alpha\beta) = N(\alpha)N(\beta)$ .

3.7) By a **norm** on a nonzero commutative ring  $R$ , we mean a weak norm  $N : R \rightarrow \mathbb{N}$  such that for all  $x \in R, N(x) = 1 \implies x \in R^\times$ .

a) Show that the function  $z \mapsto |z|$  is a norm function on  $\mathbb{Z}$ .

b) Show that the function  $N$  defined on the ring  $R_D$  in 3.5) is a norm function.

c) Suppose that  $R$  admits a norm function  $N$ . Show that every nonzero nonunit element  $a \in R$  admits a factorization  $a = x_1 \cdots x_r$ , where each  $x_i$  is irreducible.<sup>1</sup>

d)\* Show that any unique factorization domain admits a norm function.

3.8) a)\*\* We saw above that any integral domain admits a weak norm, namely  $N_0$ . Find an example of an integral domain which does not admit any norm.

b)(U) Find a characterization of the class of integral domains which admit a norm.

3.9) Let  $R$  be an integral domain which satisfies the following two properties:

(i) Every ideal of  $R$  is principal ( $R$  is a PID).

(ii) Every nonzero nonunit of  $R$  admits at least one factorization into irreducibles. Show that  $R$  is a unique factorization domain.<sup>2</sup>

3.10) A norm function  $N$  on a ring  $R$  is **Euclidean** if for all  $a \in R, b \in R \setminus \{0\}$ , there exist  $q, r \in R$  such that  $a = qb + r$  and  $N(r) < N(b)$ .

a) Convince yourself that the absolute value function on  $\mathbb{Z}$  is a Euclidean norm.

b) Recall any weak norm function  $N$  on  $R$  extends naturally to a  $\mathbb{Q}^{\geq 0}$ -valued function on the fraction field  $K$ . Show that  $N$  is a Euclidean norm on  $R$  iff the extended function  $N$  satisfies: for all  $x \in K \setminus R$  there exists  $y \in R$  such that  $N(x - y) < 1$ .

c) Suppose that  $R$  is a ring endowed with a Euclidean norm function  $N$ , and let  $I$  be an ideal of  $R$ . Show that  $I$  is principal: indeed, show that  $I = (a)$  for any element  $a$  of  $I$  of minimal norm. Therefore, finding a Euclidean norm on a ring  $R$  shows that  $R$  is a principal ideal domain.

d) Let  $k$  be a field and  $R = k[t]$ , the polynomial ring in one variable over  $k$ . For an element  $P(t) \in R$ , we denote its degree by  $\deg(P)$ ; by convention the degree of the zero polynomial is  $-\infty$ . Show that the function  $N : P(t) \mapsto 2^{\deg(P(t))}$  (with the convention that  $2^{-\infty} = 0$ ) is a Euclidean norm on  $R$ , hence  $R$  is a PID.

<sup>1</sup>Hint: adapt the proof we give for  $R = \mathbb{Z}$ .

<sup>2</sup>Hint: the argument we gave for  $\mathbb{Z}$  carries over *mutatis mutandis*.