

**Problem 1.** Let  $R$  be a subring of the complex numbers  $\mathbb{C}$  having the following two properties:

1. There is a disk  $D$  around the origin  $0 \in \mathbb{C}$ , such that  $D \cap R = \{0\}$ ;
2. For any  $z \in \mathbb{C}$  there exists an element  $\lambda \in R$  such that  $|z - \lambda| < 1$ .

Show that any ideal  $I$  of  $R$  is the set of the multiples of an element  $a \in R$ .

**Hint:** Show that, in any ideal  $I$  of  $R$ , there exists one element  $b \in I$  that is different from 0, and that is at minimal distance from the origin. Show that the ideal  $I$  coincides actually with the set of multiples of  $b$  (namely show that  $I = b.R$ ).

**Problem 2.** Let  $p$  be an odd prime and let  $d = b^2 - 4ac$ . Show that the congruence

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

is equivalent to the congruence  $y^2 \equiv d \pmod{p}$ , where  $y = 2ax + b$ . Conclude that if  $d \equiv 0 \pmod{p}$ , then there is exactly one solution modulo  $p$ ; if  $d$  has a square root in  $\mathbb{Z}/p\mathbb{Z}$ , then there are two (non congruent) solutions; and if  $d$  has no square root in  $\mathbb{Z}/p\mathbb{Z}$ , then there are no solutions. What about the case  $p = 2$ ?

**Problem 3.** Consider  $\mathbb{Z}[X]$ , the set of polynomials with coefficients in  $\mathbb{Z}$ . Show that there are ideals in  $\mathbb{Z}[X]$  that cannot be written as the set of multiples of a single polynomial.

**Hint:** consider the ideal generated by 2 and  $X$  (meaning: the ideal made of all the possible sums of one multiple of 2 and one multiple of  $X$ ).

**Problem 4.** Go on the web and find a short description of the "ElGamal cryptosystem". Write a short (< 10 lines) description of this algorithm used for encryption.

**Problem 5.** Let  $p$  be an odd prime. Assume that in  $\mathbb{Z}/p\mathbb{Z}$  there exists a nonzero element  $\zeta$  such that

- $\zeta$  has no square root in  $\mathbb{Z}/p\mathbb{Z}$ ;
  - the order of  $\zeta$  in the multiplicative group of  $\mathbb{Z}/p\mathbb{Z}$  is exactly 4.
- Show that 2 has no square root in  $\mathbb{Z}/p\mathbb{Z}$ .