

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 $I = b.R$).

Answer. Pick any $r \in I$ different from the origin. If it is at minimal distance from the origin, then we are done. Otherwise, find one that is at strictly smaller distance from the origin. By continuing this process you get a sequence of decreasing positive real numbers. It has a limit l which is > 0 (because there is a small disk around the origin that contains only the element 0 in the ring). I claim that there is indeed an element $b \in I$ that is exactly at distance $|b| = l$ from the origin. If not I could find an infinite number of $a_i \in I$ with distance from the origin between l and $l + \epsilon$ (for an arbitrary ϵ). Among these a_i , two of them at least, say a_1, a_2 would be at distance less than 2ϵ . If you shift them to the origin (by subtracting a_1 , you would contradict the first condition. Now pick any $c \in I$. By the second condition, there exists $\lambda \in I$ such that $|\frac{c}{b} - \lambda| < 1$. But this implies $|c - \lambda.b| < |b|$. By the definition of b this implies that necessarily $c = \lambda.b$, and we are done: the ideal I is the set of multiples of the element b .

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 $p = 2$?

Answer. Here I should have said: "assume that a is not zero", otherwise the question is not correct. We have $y^2 - d \equiv 4a^2.x^2 + 4a.b.x + b^2 - b^2 + 4.a.c \equiv 4a.(a.x^2 + b.x + c) \equiv 0$. Therefore $a.x^2 + b.x + c \equiv 0$ implies $y^2 - d \equiv 0$. Conversely: if $y^2 - d \equiv 0$ then $4a.(a.x^2 + b.x + c) \equiv 0$. Since p is odd and a is not zero, this implies the first condition. Now if $d \equiv 0$, then necessarily $y \equiv 0$ and there is only one solution $x = (-b).(2a)^{-1}$. If d has a square root y , then $-y$ is the only other solution to $y^2 \equiv d$, and we get two solutions $x = (2a)^{-1}(\pm y - b)$. If d has no square root then the initial equation has no solution. For $p = 2$: the equation is equivalent to $(a + b).x \equiv -c$ and this has a unique solution if and only if $(a + b)$ is not zero.

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).

Answer. Consider the ideal I made of all the polynomials that can be written as $2k + X \cdot Q(X)$. Assume $I = P(X) \cdot \mathbb{Z}[X]$. Since $2 \in I$ we see that P must be of degree 0, so it is a constant a . Now $X \in I$ so we must have $X = a \cdot bX$ for some $b \in \mathbb{Z}$. Therefore we must have $a = \pm 1$ and then $I = \mathbb{Z}[X]$. But clearly 3 is not in I so there is a contradiction.

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.

Answer. See for example this article: <http://en.wikipedia.org/wiki/Elgamal>

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

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

Show that 2 has no square root in $\mathbb{Z}/p\mathbb{Z}$.

Answer. Since ζ is of order exactly 4, we know that $\zeta^2 \equiv -1$. This implies $(\zeta + 1)^2 \equiv 2\zeta$. If 2 had a square root x (meaning $x^2 \equiv 2$, then you would have $\zeta \equiv (\zeta + 1)^2 \cdot (x^{-1})^2$ (a square), but this is a contradiction.