

Problem 1. Let $\tau(n)$ be equal to the number of divisors of n . Show that $\tau(m.n) = \tau(m).\tau(n)$ if m and n are coprime.

Problem 2. Is the ring $\mathbb{Z}[X]$ a euclidian ring? Is it a Principal Ideal Domain?

Problem 3. Show that $\mathbb{Q}[\sqrt{-5}]$ (which is by definition $\{a + b(i\sqrt{5}) \mid a, b \in \mathbb{Q}\}$) is isomorphic to $\mathbb{Q}[X]/(X^2 + 5)$.

Problem 4. Show that if p is prime and a is an integer not divisible by p , then there exists integers x and y such that $a.x \equiv y \pmod{p}$, with $0 < |x| < \sqrt{p}$ and $0 < |y| < \sqrt{p}$.

(**Hint:** consider all the integers of the form $au - v$ with $0 \leq u \leq [\sqrt{p}]$, $0 \leq v \leq [\sqrt{p}]$ where $[\cdot]$ denotes the integer part, and show that there must be two of them that are congruent modulo p , then form the difference of these two integers).

Problem 5. In order to do this problem you need the results of the previous exercise. One would like to know whether a prime integer like 3, stays a prime when we pass from \mathbb{Z} to the Gaussian integers $\mathbb{Z}[i]$. In other words, can we have a non trivial factorization $3 = (a + bi).(c + di)$? By taking the square of the modulus, one finds $3 = (a^2 + b^2).(c^2 + d^2)$. Therefore one is reduced to the problem of determining when a prime integer is the sum of two squares.

1. Show that if a prime number $p \neq 2$ can be written as a sum $a^2 + b^2$ then necessarily one has $p \equiv 1 \pmod{4}$.
2. Explain why (-1) has a square root in $\mathbb{Z}/p\mathbb{Z}$, when p is a prime of the form $4n + 1$.
3. Use the previous question together with the previous problem to show that if p prime is congruent to 1 modulo 4, then p can be written as the sum of two squares.
4. If $p \equiv 1 \pmod{4}$ then show that p can be written as a product of two elements in $\mathbb{Z}[i]$ that are not invertible. (Hence we proved that such a prime p is not anymore a prime in $\mathbb{Z}[i]$...)