

**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.

**Answer.** See the correction of the midterm, where we proved that all the products  $a.b$  where  $a$  divides  $m$  and  $b$  divides  $n$  coincide exactly with the set of divisors of  $m.n$  when  $m, n$  are coprime.

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

**Answer.** In some previous HW, we proved that the ideal generated by 2 and  $X$  is not principal, therefore our ring is not a principal ideal domain, and therefore it isn't a euclidian ring either.

**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  $\mathbb{Q}[X]/(X^2 + 5)$ .

**Answer.** Consider the surjective map  $\phi : \mathbb{Q}[X] \longrightarrow \mathbb{Q}[\sqrt{-5}]$  given by  $P(X) \mapsto P(i.\sqrt{5})$ . We know that  $\mathbb{Q}[X]/\ker\phi$  is isomorphic to  $\text{im}\phi = \mathbb{Q}[\sqrt{-5}]$ , so we have to prove that  $\ker\phi = (X^2 + 5).\mathbb{Q}[X]$ . One inclusion is easy: if a polynomial  $R(X)$  is a multiple of  $X^2 + 5$ , then  $P(i.\sqrt{5}) = 0$ . Conversely, take  $S(X)$  in  $\ker\phi$ , then write the euclidian division of this polynomial by  $X^2 + 5$ :  $S(X) = (X^2 + 5).R(X) + bX + a$ . Since  $S(X)$  is in  $\ker\phi$ , one must have  $b(i\sqrt{5}) + a = 0$ , but this implies  $b = a = 0$  and therefore  $S(X)$  must be a multiple of  $X^2 + 5$ .

**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).

**Answer.** Since each of  $u, v$  can take  $[\sqrt{p}] + 1 > \sqrt{p}$  values, there exist at least  $p = \sqrt{p}.\sqrt{p}$  integers of the form  $au - v$ . But there are only  $p$  possible values modulo  $p$ , therefore two at least of these integers must be congruent modulo  $p$ , say  $au - v \equiv au' - v' \pmod{p}$ . But then  $ax \equiv y \pmod{p}$  if one writes  $x = u - u', y = v - v'$ . Now  $x, y$  satisfy  $0 \leq |x| < \sqrt{p}$  and  $0 \leq |y| < \sqrt{p}$ . If one of them is zero, then the other one must be zero modulo  $p$ , and therefore must be zero in  $\mathbb{Z}$  (because 0 is the only multiple of zero in this range of possible values for  $x, y$ ).

**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  $\mathbb{Z}[i]$ ...)

- Answer.**
1. The only possible values taken by squares modulo 4 are 0 and 1. So sums of two squares can only take the values 0, 1, 2, and never 3. (Remember that an odd prime is congruent to 1 or 3 modulo 4).
  2. When we studied quadratic reciprocity we proved that  $-1$  is a square modulo  $p$  if and only if  $\frac{p-1}{2}$  is even.
  3. From the previous question, we know the existence of an integer  $a$  with square  $\equiv -1$  modulo  $p$ . From the previous exercise we know the existence of  $x, y$  such that  $a \cdot x \equiv y$  and  $0 < |x| < \sqrt{p}$  and  $0 < |y| < \sqrt{p}$ . But this implies  $-x^2 \equiv a^2 x^2 \equiv y^2$ , so  $p$  divides  $0 < x^2 + y^2 < 2p$ , therefore  $x^2 + y^2$  must be  $p$  and we are done.
  4. Just notice that  $p = x^2 + y^2 = (x + iy)(x - iy)$ , and that none of  $x + iy, x - iy$  is invertible because  $|x \pm iy| = \sqrt{p}$ , and we know that invertible elements must have a norm equal to 1.