

## CORRECTION OF FINAL EXAM

Name:

Student I.D:

**Problem 1. (30 points)**

1. How many solutions  $(x, y) \in \mathbb{Z} \times \mathbb{Z}$  does have the equation:  $4x^2 + 3y^2 = 1$  ?
2. How many solutions  $(x, y) \in \mathbb{Z} \times \mathbb{Z}$  does have the equation:  $2x^2 - 3y^2 = 1$  ?
3. How many solutions  $(x, y, z) \in \mathbb{Z}^3$  does have the equation:  $x^2 + y^2 = 4z + 3$  ?

**Correction:**

1. No solution: Because  $(x, y) \neq (0, 0)$  implies  $4x^2 + 3y^2 \geq 3 > 1$ .
2. No solution: in  $\mathbb{Z}/3\mathbb{Z}$ , the only possible values for  $2x^2$  are 0, 2 so  $2x^2 - 3y^2$  which is congruent to  $2x^2$  modulo 3 cannot be congruent to 1.
3. No solution: by working modulo 4, one realizes that the only possible values for  $x^2 + y^2$  modulo 4 are 0,1,2, and not 3.

**Problem 2. (35 points) An elliptic curve with no integer points**

In this problem we want to show that the curve  $E: y^2 = x^3 + 7$  has no points  $(x, y)$  with coordinates in  $\mathbb{Z}^2$ .

1. Suppose that  $(x, y)$  is a solution in integers. Show that  $x$  must be odd.
2. Show that  $y^2 + 1 = (x + 2)(x^2 - 2x + 4)$ .
3. Show that  $x^2 - 2x + 4$  must be congruent to 3 modulo 4. Explain why  $x^2 - 2x + 4$  must be divisible by some prime  $q$  satisfying  $q \equiv 3 \pmod{4}$ .
4. Reduce the original equation modulo  $q$  and deduce from it that  $(-1)$  must have a square root in  $\mathbb{Z}/q\mathbb{Z}$ . Show that this is impossible, thus proving that the equation has no solutions in integers.

**Correction:**

1. If  $x$  is even then  $y^2$  would be of the form  $8k + 7$ , but by writing them down, one sees that squares of integers can only be congruent to 0,1,4 modulo 8. Thus  $x$  is odd.
2. Just expand the product.
3. We proved that  $x$  is odd  $= 2k + 1$ , thus  $x^2 - 2x + 4 = (2k + 1)(2k - 1) + 4 \equiv 4k^2 + 3$  must be congruent to 3 mod 4. Now the prime numbers dividing  $x^2 - 2x + 4$  cannot be all of type  $4k + 1$  (because the product of their powers would be of same type, which is not the case).
4. Since  $q$  divides  $x^2 - 2x + 4$ , it must divide  $y^2 + 1$ , which means that  $y$  would be a square root of  $-1 \pmod{q}$ . Since  $(-1)^{\frac{q-1}{2}} = -1$ , this is a contradiction.

**Problem 3. (20 points)** Let  $p$  be an odd prime such that  $p = 8n + 1$  for some integer  $n$ . We have seen in class that the non-zero elements of  $\mathbb{Z}/p\mathbb{Z}$  form a group for the multiplication law, and that this group is cyclic of order  $p - 1 = 8n$ . We consider one generator, called  $r$ , of this multiplicative group  $(\mathbb{Z}/p\mathbb{Z} - \{0\}, \times)$ .

Show that the solutions of the congruence  $x^2 \equiv 2 \pmod{p}$  are given by

$$x \equiv \pm (r^{7n} + r^n) \pmod{p}$$

**Correction:**

Since  $\mathbb{Z}/p\mathbb{Z}$  is a field, there are at most 2 solutions for the polynomial equations, so if the proposed numbers are solutions, they will constitute the complete set of solutions.

Let's set  $x = (r^{7n} + r^n)$ . Then  $x^2 = (r^{7n} + r^n)^2 = r^{14n} + 2r^{8n} + r^{2n} = r^{6n} + 2 + r^{2n} = 2 + r^{2n}(1 + r^{4n})$ , because  $r^{8n} = 1$ . For the same reason, one must have  $r^{4n} = -1$ , which implies the conclusion.

**Problem 4. (45 points)**

Let  $p$  be an odd prime. We want to show the following:  $p \equiv 1, 3 \pmod{8}$  if and only if  $p$  can be written as  $p = x^2 + 2y^2$  for some choice of integers  $x$  and  $y$ . For the rest of the problem, you can use (without proving it) the following result coming from quadratic reciprocity: if  $p \equiv 1, 3 \pmod{8}$  then there exists an integer  $r$  such that  $r^2 \equiv -2 \pmod{p}$ .

1. Show that if  $p = x^2 + 2y^2$  for some integers  $x$  and  $y$ , then  $p$  is not congruent to 5, nor 7 modulo 8. (Hint: what are the possible values modulo 8 taken by squares of integers?) Conclude that necessarily  $p$  must be congruent to 1 or 3 in this case.

2. Show the following lemma (independent of the rest of the problem):

**Lemma.** If  $x \in \mathbb{R}$ ,  $n \in \mathbb{N}$ , then there exists a fraction  $\frac{a}{b}$  in lowest terms such that  $0 < b \leq n$  and

$$\left| x - \frac{a}{b} \right| \leq \frac{1}{b(n+1)}.$$

(Hint: approximation by continued fractions...)

3. Apply the lemma to  $x = \frac{-r}{p}$  (where  $r$  is a square root of  $(-2)$  in  $\mathbb{Z}/p\mathbb{Z}$ ), and  $n = \lfloor \sqrt{p} \rfloor$  (this means the integer part of  $\sqrt{p}$ ). Letting  $c = r \cdot b + p \cdot a$ , show the following:
  - a)  $c^2 + 2b^2 \equiv 0 \pmod{p}$ .
  - b)  $0 < c^2 + 2b^2 < 3p$ .
  - c) Both cases  $c^2 + 2b^2 = 2 \cdot p$  and  $c^2 + 2b^2 = p$  give a solution to the initial problem.
4. Conclude.

**Correction:**

1. Squares of integers modulo 8 can only take the values 0,1,4, therefore  $2y^2$  can only take the values 0,2 modulo 8, and the sum  $x^2 + 2y^2$  can only take the values 0,1,2,3,4,6, but not 5,7. Thus the odd prime  $p$  must be congruent to 1 or 3 modulo 8.
2. From the theory of continued fractions, we know the existence of approximations

$$\left| x - \frac{p_i}{q_i} \right| \leq \frac{1}{q_i \cdot q_{i+1}},$$

where the  $q_i$  form an unbounded increasing sequence of integers. Thus for any integer  $n + 1$ , there exists an integer  $i$  such that  $q_i < n + 1 \leq q_{i+1}$ , and this implies the result because  $1/q_{i+1} \leq 1/(n + 1)$  and at the same time  $0 < q_i \leq n$ .

3.

a) First one has  $c^2 \equiv r^2 \cdot b^2 \equiv -2b^2 \pmod{p}$ , hence the result.

b) Now one has  $\left| \frac{a \cdot p + b \cdot r}{p \cdot b} \right| = \left| \frac{-r}{p} - \frac{a}{b} \right| \leq \frac{1}{b(n+1)}$ , so  $c^2 \leq \frac{p^2}{(n+1)^2} < p$ .

Moreover one has  $b \leq n \leq \sqrt{p}$ , so  $2b^2 \leq 2p$ . Putting everything together, one gets the desired inequality.

c) The quantity  $c^2 + 2b^2$  must be a multiple of  $p$ , strictly between 0 and  $3p$ , so it can be  $p$  or  $2p$ . If it is  $p$  then we are done.

Suppose it is now equal to  $2p$ , then this would imply that  $c^2$  is even, so  $c$  itself would be even equal to  $2d$ , but then our equation would become  $4d^2 + 2b^2 = 2 \cdot p$  which implies  $2d^2 + b^2 = p$ , a solution to our problem.

4. If  $p$  is congruent to 1 or 3 modulo 8, then we can find a solution in integers to the equation  $p = x^2 + 2y^2$ , and these two conditions are equivalent.

### Problem 5. (40 points)

1. Show that the ring of Gaussian integers  $\mathbb{Z}[i]$  is isomorphic to  $\mathbb{Z}[X]/I$ , where  $I$  is the ideal generated by  $X^2 + 1$ .
2. Find an explicit isomorphism between  $\mathbb{Z}[X]/(X - 3)$  and  $\mathbb{Z}$ .
3. Is the ring  $\mathbb{Z}[X]/(3X - 1)$  isomorphic to  $\mathbb{Z}$ ?
4. Show that if  $\varepsilon \in \mathbb{Z}[i]$  has an inverse in  $\mathbb{Z}[i]$  (we call such an element a *unit* of  $\mathbb{Z}[i]$ ) then necessarily  $\varepsilon^5 = \varepsilon$ . (Hint: use the norm  $N(a + b \cdot i) = a^2 + b^2$  and its properties).
5. Show that  $\mathbb{Q}[X]/(X^2 + X + 1)$  is a field and find the inverse of the element  $X + 2 \pmod{X^2 + X + 1}$ .

### Correction:

1. Consider the ring morphism

$$\begin{aligned} \varphi: \mathbb{Z}[X] &\longrightarrow \mathbb{Z}[i] \\ P(X) &\longmapsto P(i) \end{aligned}$$

This is clearly surjective ( $a + b \cdot i$  can be obtained as  $\varphi(a + b \cdot X)$ ). The kernel contains  $(X^2 + 1)$ . Moreover, if one writes the euclidean division of  $P(X)$  by  $X^2 + 1$ , one obtains a remainder of degree 1,  $a + b \cdot X$ , which is zero if and only if  $a + b \cdot i = \varphi(P(X))$  is zero, so the kernel is the ideal  $(X^2 + 1)$ . One concludes with the isomorphism theorem.

2. Just consider

$$\begin{aligned} \varphi: \mathbb{Z}[X] &\longrightarrow \mathbb{Z} \\ P(X) &\longmapsto P(3) \end{aligned}$$

This is surjective of kernel  $(X - 3)$ , hence the result.

3. Let's consider  $\bar{X}$  (or if you prefer  $X \pmod{3X - 1}$ ) in  $\mathbb{Z}[X]/(3X - 1)$ . It's an element that has the property that  $3 \cdot \bar{X} = 1$ , so 3 is invertible in that ring. Now in  $\mathbb{Z}$ , we know that 3 is not invertible, therefore the two rings cannot be isomorphic.
4. Invertible elements in  $\mathbb{Z}[i]$  are the elements with norm=1. It's easy to check that only the 4th roots of unity are invertible, and they satisfy the required equation.
5. The polynomial is irreducible (roots are  $j, j^2$ ), so we get a field. Now  $(X + 2)(X - 1) \equiv -3$  so the inverse of  $X + 2$  is  $(-1/3)(X - 1)$ .

**Problem 6. (30 points)**

1. Find the solutions  $(x, y) \in \mathbb{Z}^2$  to the equation  $7x - 12y = 4$ .
2. Find the continued fraction expansion of  $\frac{41}{15}$ .

**Correction:**

1. You'll find  $x = 4 + 12k$ ,  $y = 2 + 7k$ , where  $k$  is an arbitrary integer.
2. You get  $41/15 = [2; 1, 2, 1, 3]$