Solutions - Quiz 1

SECTION 005, M. BILU

Question 1.(4 points.) Give a proof of the Gauss lemma, stated below:
Let a, b, c be integers. If $a \mid bc$ and $gcd(a, b) = 1$ then $a \mid c$.

From Bézout's theorem, there exist some integers u and v such that $au + bv = 1$.
Multiplying this relation by c, we get $acu + bcv = c$.
Because $a \mid bc$, there exists q an integer such that $bc = aq$.
Substituting in the first relation, we get $a(cu + qv) = c$.
Because $cu + qv \in \mathbb{Z}$, $a \mid c$.

Question 2.(4 points.) Give the definition of an equivalence relation on a set A.

An binary relation $\mathcal{R}$ on the set A is a subset of $A \times A$.
For $x, y \in A$, we write $x\mathcal{R}y$ if the couple (x, y) (in this order!) belongs to $\mathcal{R}$.
We say that $\mathcal{R}$ is an equivalence relation if:

1. $\mathcal{R}$ is reflexive: for $x \in A$, $x\mathcal{R}x$.
2. $\mathcal{R}$ is symmetric: for $x, y \in A$, $x\mathcal{R}y \Rightarrow y\mathcal{R}x$.
3. $\mathcal{R}$ is transitive: for $x, y, z \in A$, $x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow x\mathcal{R}z$.

Problem 1.(6 points.) These questions are independent.

1. Find the inverse of 49 modulo 53.

   We can use the Euclidean algorithm to get an inverse of 49 modulo 53, that is an integer n such that $49n \equiv 1 \pmod{53}$, that is an integer n such that there exists an integer q such that $49n - 53q = 1$. We obtain:

$$53 = 49 \times 1 + 4$$
$$49 = 4 \times 12 + 1$$
$$4 = 4 \times 1 + 0$$

   Therefore $\gcd(49, 53) = 1$ (that was assumed by the question, otherwise n wouldn't exist). And if you compute the reversed algorithm, you reach the following relation (if necessary, after simplification):

$$49 \times 13 - 53 \times 12 = 1$$

   Therefore, the inverse of 49 modulo 53 is 13.

2. Give the list of all the units of $\mathbb{Z}/15\mathbb{Z}$.

   You have seen in class that it is exactly the set of classes of integers relatively prime to 15. You should obtain:

$$(\mathbb{Z}/15\mathbb{Z})^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

Problem 2.(6 points.) For any integer n, show that $\gcd(2n + 4, 3n + 3)$ can only be 1,2,3 or 6.

It is sufficient to find a Bézout relation whose divisors of the right-hand side are 1, 2, 3 and 6.
You can observe that: $3 \times (2n + 3) - 2 \times (3n + 3) = 6$.
Therefore, $gcd(2n + 4, 3n + 3) \mid 6$ (that comes from the equality of sets: $a\mathbb{Z} + b\mathbb{Z} = gcd(a, b)\mathbb{Z}$).
As a divisor of 6, $\gcd(a, b) \in \{1, 2, 3, 6\}$.

Bonus. For non-zero integers x, y, $\operatorname{lcm}(x, y)$ is defined as the smallest positive common multiple of x and y.
Find all integers x, y such that: $gcd(x, y) + \operatorname{lcm}(x, y) = x + y$.

Note that, $\gcd(x, y)$ and $\operatorname{lcm}(x, y)$ being positive by definition, we need to have $x+y$ positive, so at least one of the integers x, y is positive. Up to exchanging x and y, we may assume $x \leq y$ (so that in particular y is positive). Since $\operatorname{lcm}(x, y)$ is in particular a multiple of y, there is an integer $k \geq 1$ such that $\operatorname{lcm}(x, y) = ky$. Then we have

$$\gcd(x, y) + ky \leq 2y,$$

so that $0 < \gcd(x, y) \leq (2-k)y$. In particular, y being positive, we have $2-k > 0$, that is, $k < 2$, so $k = 1$. We therefore have $y = \operatorname{lcm}(x, y)$, that is, y itself is a common multiple of x and y, so x must divide y. From the equation, we moreover get that $x = \gcd(x, y)$, that is, x is positive. Recalling that we assumed $x \leq y$ up to exchanging x and y, the solutions are pairs of positive integers (x, y) such that $x|y$ or $y|x$.