Homework 2 solutions

Problem 1. Show that $3 \mid a^3 - a$ for every $a \in \mathbb{Z}$.

Solution 1. We can write $a^3 - a = a(a-1)(a+1)$. One of these factors is always divisible by 3.

Problem 2. The *greatest integer function* or *floor function* $\lfloor \cdot \rfloor \colon \mathbb{R} \to \mathbb{Z}$ is defined as follows: for every real number $x \in \mathbb{R}$, $\lfloor x \rfloor$ is the greatest integer which is less or equal to x.

Using the floor function and the basic arithmetic operations, find an explicit formula for the quotient and remainder of two integers. Prove your result.

Solution 2. Let $a, b \in \mathbb{Z}$ with $b > 0$. Then the quotient of a divided by b is $q = \lfloor a/b \rfloor$ and the remainder is $r = a - b\lfloor a/b \rfloor$. To prove this, we just have to check that $a = bq + r$ and $0 \leq r < b$. The first is clear and the second is equivalent to the inequalities $a/b \geq \lfloor a/b \rfloor$ as well as $a/b < \lfloor a/b \rfloor + 1$. The first is clear from the definition of the floor function, and if $x \geq \lfloor x \rfloor + 1$ for any $x \in \mathbb{R}$ then $\lfloor x \rfloor + 1$ would be an integer less or equal to x but greater than $\lfloor x \rfloor$, which is impossible.

Problem 3. Suppose that $a, b \in \mathbb{Z}$ and $a \mid b$. Show that $a^n \mid b^n$ for every $n \in \mathbb{N}$.

Solution 3. $a \mid b$ means that $b = ka$ for some $k \in \mathbb{Z}$. But then $b^n = k^n a^n$, so $a^n \mid b^n$.

Problem 4. The following are meant to help you avoid common mistakes.

(a) Find integers a, b and c such that $a \mid bc$ but $a \nmid b$ and $a \nmid c$.

(b) Find integers a, b and c such that each pair of them has a common divisor greater than 1, but that all three of them together do not have a common divisor greater than 1.

Solution 4.

a) For example $a = 6$, $b = 2$, $c = 3$.

b) For example $a = 6$, $b = 10$, $c = 15$. Then $(6, 10) = 2$, $(10, 15) = 5$, $(6, 15) = 3$, but there is no common divisor of all three except ± 1.

Problem 5. Let a and b be integers. Recall that a *pair of Bezout coefficients* for a and b is a pair of integers $m, n \in \mathbb{Z}$ such that

$$ma + nb = (a, b).$$

Prove that, for any fixed pair of integers a and b, there are infinitely many pairs of Bezout coefficients.

Solution 5. Let a, b, m, n be as in the statement of the problem. Let $k \in \mathbb{Z}$ be another integer and define $m' = m + kb$ and $n' = n - ka$. Then

$$m'a + n'b = (m + kb)a + (n - ka)b = ma + kab + nb - kab = ma + nb = (a, b),$$

so (m', n') is another pair of Bezout coefficients for a and b. The set

$$\{(m + kb, n - ka) \mid k \in \mathbb{Z}\}$$

is infinite. That was the expected solution.

Alternatively, we can invest some more effort and try to find *all* possible pairs of Bezout coefficents. The answer would be: if (m, n) is one pair of Bezout coeffients, and $d = (a, b)$, then the set of all pairs of Bezout coefficients for a and b is

$$X = \left\{ \left(m + \frac{be}{d}, n - \frac{ae}{d} \right) \mid e \in \mathbb{Z} \right\} \subset \mathbb{Z} \times \mathbb{Z}.$$

To show that, assume that (m', n') is another pair of Bezout coefficients and define $M = m' - m$ and $N = n' - n$. Then

$$Ma + Nb = m'a + n'b - ma - nb = d - d = 0,$$

so $Ma = -Nb$. If we define $p = a/d$ and $q = b/d$ then $Mp = -Nq$ $(\star)$. Also, we showed in class that p and q defined like this are coprime. It follows from $(\star)$ that $q \mid Mp$ and, because p and q are coprime, $q \mid M$. Analogously, we have $p \mid Nq$ and therefore $p \mid N$. So we can write $M = qe$ and $N = pf$ for some integers e and f. Using $(\star)$ again, we get

$$qep = Mp = -Nq = -pfq,$$

so $f = -e$. Putting everything together, we showed that

$$m' = m + M = m + qe = m + \frac{be}{d}, \qquad n' = n + N = n - pe = n - \frac{ae}{d},$$

so $(m', n') \in X$.

Conversely, if $(m', n') \in X$, then $m' = m + be/d$ and $n' = n - ae/d$ for some integer e, so

$$\left(m + \frac{be}{d} \right) a + \left(n - \frac{ae}{d} \right) b = ma + nb + \frac{abe}{d} - \frac{abe}{d} = (a, b).$$

Hence (m', n') is a pair of Bezout coefficients.