Fall 2021 – Math 328K – 55385

Homework 3 Solutions

Problem 1. How many integer solutions $x, y \in \mathbb{Z}$ do the following equations have? If there is at least one solution, find an example.

a) $60x + 18y = 97$

b) $37x + 1000010000100001y = 0$

c) $14541x + 1367631y = 13566531$

Solution 1.

a) $(60, 18) = 6$, and $6 \nmid 97$, so there are no solutions.

b) Whatever the gcd of 37 and 1000010000100001 is, it divides 0. So there are (infinitely many) solutions. A simple example is $x = 1000010000100001, y = -37$.

c) We use the extended Euclidean algorithm

r_k	q_k	s_k	t_k
1367631		1	0
14541	94	0	1
777	18	1	-94
555	1	-18	1693
222	2	19	-1787
111	2	-56	5267
0			

This tells us that

$$5267 \cdot 14541 - 56 \cdot 1367631 = 111.$$

Furtheremore, we see that the greatest common divisor 111 divides 13566531, with quotient 122221. Multiplying the previous equation with 122221 gives the pair of solutions

$$x = 5267 \cdot 122221, \quad y = -56 \cdot 122221.$$

Problem 2. Let a, b be positive integers such that $a^2 \mid b^2$. Show that $a \mid b$.

Solution 2. We can use the prime decomposition, or alternatively an argument like this:

Let $d = (a, b)$, and $a' = a/d$ as well as $b' = b/d$. Then a' and b' are coprime and so are a'^2 and b'^2: if they had a common divisor greater than 1, they would have a common prime divisor, which would also divide a and b. But by assumption $d^2b'^2 = b^2 = ka^2 = kd^2a'^2$ for some integer k. So $b'^2 = ka'^2$. But a'^2 and b'^2 are coprime, which is only possible if $a'^2 = 1$, and therefore $a' = 1$. But then $a = d$ divides b.

Problem 3. Denote by p_n be the n–th prime ($p_1 = 2, p_2 = 3, p_3 = 5, \dots$). Show that $p_n \leq 2^{2^{n-1}}$ for every $n \in \mathbb{N}$. Conclude that there are at least $n + 1$ primes less than 2^{2^n} for every $n \in \mathbb{N}$.

Hint: Look at Euclid's proof of the infinitude of primes.

Solution 3. We prove this by (strong) induction on n. If $n = 1$, then $p_1 = 2$ and $2^{2^{1-1}} = 2$. So now assume that $p_k \leq 2^{2^{k-1}}$ for all $k \in \{1, \dots, n\}$. We want to prove that $p_{n+1} \leq 2^{2^n}$. Consider the integer $Q = p_1 \cdots p_n + 1$. It is greater than 1, but $p_i \nmid Q$ for all $i \in \{1, \dots, n\}$. So Q must have a prime factor P which is not one of the first n primes, that is $P \geq p_{n+1}$. Hence

$$p_{n+1} \leq P \leq Q = \prod_{i=1}^{n} p_n + 1 \leq \prod_{k=1}^{n} 2^{2^{k-1}} + 1 = \prod_{k=0}^{n-1} 2^{2^k} + 1 = 2^{\sum_{k=0}^{n-1} 2^k} + 1 = 2^{2^n-1} + 1 \leq 2^{2^n},$$

where we used the geometric sum and that $1 \leq 2^{2^n-1}$ in the last two steps.

Problem 4. Let $p \neq q$ be prime numbers and a be an integer such that $p \mid a$ and $q \mid a$. Show that $pq \mid a$. Find a counterexample if either p or q is not prime.

Solution 4. This is easy once we know the Fundamental Theorem. If we don't want to use it, it follows from the following fact, which was the essential ingredient of the Fundamental Theorem: for three integers $a, b, c \in \mathbb{Z}$, if $(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

As a reminder, we proved this using Bezout's Theorem: since $(a, b) = 1$ there are Bezout coefficients $s, t \in \mathbb{Z}$ with $as + bt = 1$. Multiplying by c, we get $asc + bct = c$. Since a divides the left hand side, $a \mid c$.

Assuming this fact, we can solve the problem as follows: assume that $p \neq q$ are prime, $p \mid a$ and $q \mid a$. Then $a = kq$ for an integer k. So $p \mid kq$ and $(p, q) = 1$, hence $p \mid k$, that is $k = pm$ for some $m \in \mathbb{Z}$. So $a = pqm$.

Problem 5. Let $a, b, c \in \mathbb{Z}$ and write $d = (a, b)$. We proved in class that the equation $ax + by = c$ has an integer solution if and only if $d \mid c$.

Now assume that $d \mid c$, and let s, t be a pair of Bezout coefficients for a and b, so that $as + bt = d$. Show that the set of all solutions (x, y) of $ax + by = c$ is

$$\left\{ \left(\frac{cs - nb}{d}, \frac{ct + na}{d} \right) \mid n \in \mathbb{Z} \right\}.$$

Solution 5. First let

$$(x, y) = \left(\frac{cs - nb}{d}, \frac{ct + na}{d} \right).$$

We need to show that this is a solution. Indeed,

$$a\frac{cs - nb}{d} + b\frac{ct + na}{d} = \frac{acs - nab + bct + nab}{d} = \frac{c}{d}(as + bt) = c.$$

Conversely, let (x, y) be a solution, that is $ax + by = c$. Then

$$ax + by = c = \frac{c}{d}(as + bt).$$

Let $m_1 = x - cs/d$ and $m_2 = y - ct/d$. Then $am_1 + bm_2 = 0$. If we also set $a' = a/d$ and $b' = b/d$, we have $(a', b') = 1$ and $a'm_1 = -b'm_2$. This implies $a' \mid m_2$ and $b' \mid m_1$. So $m_1 = b'n_1$ and $m_2 = a'n_2$ for integers n_1, n_2 with $a'b'n_1 = -a'b'n_2$. So $m_1 = -b'n_2$ and $m_2 = a'n_2$. Note this is still true if $a' = 0$ or $b' = 0$.

We therefore have

$$x = m_1 + \frac{cs}{d} = -\frac{bn_2}{d} + \frac{cs}{d}, \quad y = m_2 + \frac{ct}{d} = \frac{an_2}{d} + \frac{ct}{d},$$

which is what we wanted to show.