Math 328K. Fall 2025

Some solutions to Homework # 4

Prof. Hector E. Lomeli

1. §3.3. Exercise 32. Let $n \in \mathbb{N}$. We define $d_0 = (n^2 + 2, n^3 + 1)$. We notice that

$$n^3 + 1 = n(n^2 + 2) - 2n + 1.$$

This implies that d_0 can be written as $d_0 = (n^2 + 2, -2n + 1)$. We have the following linear combination

$$4(n^2 + 2) + (2n + 1)(-2n + 1) = 9.$$

Given that d_0 divides both $n^2 + 2$ and $-2n + 1$, we conclude that $d_0 \mid 9$. We know that $d_0 > 0$ and therefore $d_0 = 1, 3$ or 9.

2. a) We will use the PMI to prove that the following predicate is true for all $n \in \mathbb{N}$.

$$P(n) \Longleftrightarrow a^y - 1 \mid (a^y)^n - 1.$$

- **Base case.** If $n = 1$, then $P(1)$ is trivially true.
- **Induction step.** Let $n \in \mathbb{N}$ be arbitrarily chosen. We assume that $P(n)$ is true. We will show that $P(n + 1)$ is also true. We have that

  $$(a^y)^{n+1} - 1 = (a^y)^n (a^y - 1) + \left((a^y)^n - 1\right).$$

  Given that $a^y - 1 \mid (a^y)^n - 1$ and $a^y - 1 \mid a^y - 1$, we conclude that $a^y - 1 \mid (a^y)^{n+1} - 1$, and therefore $P(n + 1)$ is true.

Using the PMI, we conclude that $P(n)$ is true for all $n \in \mathbb{N}$.

2. b) If $x > y > 0$ and $y \mid x$, then there exists $n \in \mathbb{N}$ such that $x = ny$. Using the result above, this implies that

$$a^y - 1 \mid (a^y)^n - 1 = a^x - 1.$$

3. a) Given that $(m, n) \mid m$ and $(m, n) \mid n$, the previous problem implies that d_0 divides both $a^m - 1$, and $a^n - 1$. From this, we conclude that $d_0 | d_1$.

3. b) Using Bezout's theorem, we know that there exists $x, y \in \mathbb{Z}$ such that

$$(m, n) = m\,x + n\,y.$$

We notice that, if $t \in \mathbb{N}$, we also have

$$(m, n) = m\,(t\,n + x) + n\,(y - t\,m) = m\,(t\,n + x) - n\,(t\,m - y).$$

Taking t sufficiently large, we get that $t\,n + x > 0$ and $t\,m - y > 0$. In this case, we can choose $t \in \mathbb{N}$ to satisfy $t > [-x/n] + 1$ and $t > [y/m] + 1$. We define $p = t\,n + x$ and $q = t\,m - y$.

3. c) We have $a^{(m,n)}\,v = a^{mp} - a^{(m,n)}$. This implies that $d_0 = a^{(m,n)} - 1 = a^{mp} - 1 - a^{(m,n)}\,v = u - a^{(m,n)}\,v$.

3. d) The previous problem implies that d_1 divides both u and v. Therefore, d_1 divides d_0, because d_0 is a linear combination of u and v. Given that both d_0, d_1 are positive, $d_0 | d_1$ and $d_1 | d_0$, we conclude $d_0 = d_1$.

---

4. $(190, 25) = 5$. One possible Bezout linear combination is $(2) \cdot 190 + (-15) \cdot 25 = 5$.

5. $(800, 255) = 5$. One possible Bezout linear combination is $(22) \cdot 800 + (-69) \cdot 255 = 5$.

6. $(2000, 1001) = 1$. One possible Bezout linear combination is $(500) \cdot 2000 + (-999) \cdot 1001 = 1$.

---

§3.3. Exercise 25. Solution 1. If a is an integer then clearly both numbers $8a+3$ and $5a+2$ are non-zero. Then we can simplify their greatest common denominator in the following way.

$$(8a+3, 5a+2) = ((8a+3)-(5a+2), 5a+2) = (3a+1, 5a+2) =$$
$$(3a+1, (5a+2)-(3a+1)) = (3a+1, 2a+1) = (a, 2a+1).$$

If $a = 0$ then $(a, 2a+1) = (0, 1) = 1$. If $a \neq 0$, then $(a, 2a+1) = (a, 1) = 1$. In this way, we conclude that $(8a+3, 5a+2) = 1$.

§3.3. Exercise 25. Solution 2. Another solution is possible. We will find integers m, n such that

$$m(8a+3) + n(5a+2) = 1,$$

for all $a \in \mathbb{Z}$. We notice that

$$m(8a+3) + n(5a+2) = (8m+5n)a + (3m+2n).$$

So, it is enough to solve the system of equations

$$8m + 5n = 0,$$
$$3m + 2n = 1.$$

Solving, we find that $m = -5$ and $n = 8$. This implies that $(-5)(8a+3) + 8(5a+2) = 1$, for all $a \in \mathbb{Z}$. We conclude that $8a+3$ and $5a+2$ are relatively prime, for any choice of $a \in \mathbb{Z}$.

§3.3. Exercise 30. Let $n \in \mathbb{N}$ and $d = (n+1, n^2-n+1)$. We noticed that $n^2-n+1 = (n+1)(n-2)+3$. This implies that

$$d = (n+1, n^2-n+1) = \big(n+1, (n+1)(n-2)+3\big) = (n+1, 3).$$

Then $d \mid n+1$ and $d \mid 3$. Given that $d > 0$, $d = 1$ or $d = 3$ because 3 is prime.