Math 328K. Fall 2025
Some solutions to Homework # 3

Prof. Hector E. Lomeli

Problem 1. a) Let $k \in \mathbb{Z}$. We notice that the term $b_k - 1$ can be written as

$$b_k - 1 = 3k^2 - 3k = 3(k^2 - k).$$

We know that $k^2 - k$ is divisible by 2. Then, there exists ℓ such that $k^2 - k = 2\ell$. This implies that $b_k = 3 \cdot 2\ell = 6\ell$. We conclude that $6 \mid b_k - 1$.

Problem 1. b) We notice that

$$\sum_{k=1}^{n} b_k = \sum_{k=1}^{n} ((b_k - 1) + 1) = \sum_{k=1}^{n} (b_k - 1) + \sum_{k=1}^{n} 1$$

Each term in the sum $\sum_{k=1}^{n} (b_k - 1)$ is divisible by 6. Therefore, the sum is divisible by 6 and there exists an integer q such that

$$\sum_{k=1}^{n} (b_k - 1) = 6q.$$

We also have that $\sum_{k=1}^{n} 1 = n$. We conclude that there exists an integer q such that $\sum_{k=1}^{n} b_k = 6q + n$.

Problem 1. c) We notice that the term b_k is of the form $b_k = a_k - a_{k-1}$, where $a_k = k^3$. Therefore, the sum is telescoping. We get that

$$\sum_{k=1}^{n} b_k = a_n - a_0 = n^3.$$

Using part b), we get that $n^3 = 6q + n$ and therefore 6 divides $n^3 - n$.

---

§1.5. Exercise 23. Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Using the division algorithm (also known as Quotient-Remainder Theorem or QRT), we know that there exists two integers q, r such that

$$a = qb + r, \qquad 0 \le r < b.$$

We will consider two cases: $b \nmid a$ and $b \mid a$.

- If $b \nmid a$, we have $r > 0$. Then

  $$-a = -qb - r = -(q+1)b + (b-r).$$

  Given that $0 < r < b$, we conclude that $0 < b - r < b$. Then the numbers $q' = -(q+1)$ and $r' = b - r$ satisfy the conditions of the QRT, when we divide $-a$ by b. We conclude that they are the quotient and remainder of dividing $-a$ by b.

- If $b \mid a$, we have $r = 0$. Then

  $$-a = -qb - r = (-q)b + 0.$$

  The numbers $q' = -q$ and $r' = 0$ satisfy the conditions of the QRT, when we divide $-a$ by b. We conclude that they are the quotient and remainder of dividing $-a$ by b.

§1.5. Exercise 38. Let n be an odd integer. It is of the form $n = 2\ell + 1$, for some $\ell \in \mathbb{Z}$. This implies that

$$n^2 = 4\ell^2 + 4\ell + 1 = 4(\ell^2 + \ell) + 1.$$

In class, we saw that we always have $2 \mid \ell^2 + \ell$. Then, there exists $k \in \mathbb{Z}$ such that $\ell^2 + \ell = 2k$. After substitution, we conclude that $n^2 = 8k + 1$.

§3.1. Exercise 6. Solution 1. We can write the statement using quantifiers. We need to prove the following universal conditional.

$$(\forall n \in \mathbb{Z})\big(n^3 + 1 \text{ is prime } \rightarrow n = 1\big).$$

Let $n \in \mathbb{Z}$ be an arbitrarily chosen integer. We assume that $n^3 + 1$ is prime. We will show that $n = 1$.

Given that $n^3 + 1$ is prime, we get that $n^3 + 1 > 1$. This implies that $n^3 > 0$ and therefore $n > 0$. We notice that $n^3 + 1$ can be factored in the following way

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

We know that $n > 0$, so we have that $n + 1 > 1$. Then $n + 1$ is a positive divisor of $n^3 + 1$, that is different from 1. Given that $n^3 + 1$ is prime, the only possibility is that $n + 1 = n^3 + 1$. From this, we conclude that $n^3 - n = 0$.

There are only three solutions to the equation $n^3 - n = 0$, namely $n = -1, 0, 1$. Given that $n > 0$ we conclude that $n = 1$.

§3.1. Exercise 6. Solution 2. We can write the statement using quantifiers. We need to prove the following universal conditional.

$$(\forall n \in \mathbb{Z})\big(n \neq 1 \rightarrow n^3 + 1 \text{ is not prime }\big).$$

Let $n \in \mathbb{Z}$ be an arbitrarily chosen integer. We assume that $n \neq 1$. We will show that $n^3 + 1$ is not prime.

Given that $n \neq 1$, we have two cases: $n \leq 0, n > 1$.

- If $n \leq 0$, then $n^3 \leq 0$ and therefore $n^3 + 1 \leq 1$. We know that any prime is at least 2, so the number $n^3 + 1$ is not a prime.

- In the second case, we assume that $n > 1$. We notice that $n^3 + 1$ can be factored in the following way

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

  We know that $n > 0$, so we have that $n + 1 > 1$. Then $n + 1$ is a divisor of $n^3 + 1$, that satisfies $n + 1 > 1$. We also have that $n(n-1) > 0$ and this implies that $(n^2 - n + 1) > 1$. This implies that $n^3 + 1$ is composite, and not a prime.

§3.1. Exercise 14. The assumption is that there exists an integer n_0 such that the prime p is of the form $p = 3n_0 + 1$. We will show that there exists an integer n_1 such that $p = 6n_1 + 1$.

We claim that $2 \mid n_0$. By way of contradiction, suppose that $2 \nmid n_0$. Then there exists an integer k such that $n_0 = 2k + 1$. This implies that

$$p = 3n_0 + 1 = 6k + 4 = 2(3k + 2).$$

This implies that $2|p$. Given that p is prime, $p = 2$ and $3k + 2 = 1$. We conclude that $1 = -3k$ and hence $3 \mid 1$. This is a contradiction. We conclude that $2 \mid n_0$.

Then there exists an integer n_1 such that $n_0 = 2n_1$. After substitution, $p = 3n_0+1 = 3(2n_1)+1 = 6n_1+1$.

§3.3. Exercise 9. We define $d = (a, b)$ and $e = |c|d$. We will show that $e = (ca, cb)$. In order to prove this, we will show that e is the greatest common divisor of ca and cb. This is, e satisfies:

a) $e \mid ca$ and $e \mid cb$.

b) If x is a positive integer such that $x \mid a$ and $x \mid b$, then $x \leq e$.

Let $p, q \in \mathbb{Z}$ be two integers such that $a = p\,d$ and $b = q\,d$. Then $ca = p\,cd$ and $cb = q\,cd$. Now the only potential difference between c and $|c|$ is a sign. Therefore, we can find integers $p', q' \in \mathbb{Z}$ such that $ca = p'\,|c|d = p'\,e$ and $cb = q'\,|c|d = q'\,e$. This shows that $e \mid ca$ and $e \mid cb$.

Let x be a positive integer that divides both ca and cb. From Bezout's theorem, we know that there exist integers m, n such that

$$m\,a + n\,b = d.$$

This implies that

$$m\,(ca) + n\,(cb) = cd.$$

As before, we notice that the only potential difference between c and $|c|$ is a sign. Therefore, we can find integers $m', n' \in \mathbb{Z}$ such that

$$m'\,(ca) + n'\,(cb) = |c|d = e.$$

Given that x divides ca and cb, we conclude that $x|e$. By assumption, both x and e are positive and this implies that $x \leq e$. This shows that e is the greatest common divisor of ca and cb.

§3.3. Exercise 10. We know that $(a, b) = 1$. This implies that $(a, a + b) = 1$. Let $d_0 = (a - b, a + b)$. We will show that $d_0 = 1$ or $d_0 = 2$. By Bezout's theorem, we can find integers m, n such that

$$m\,a + n\,(a + b) = 1.$$

We also have that $d_0 > 0$ and

$$d_0 = (a - b, a + b) = ((a - b) + (a + b), a + b) = (2a, a + b).$$

Using the linear combination above, we find that

$$m\,(2a) + 2n\,(a + b) = 2.$$

We know that $d_0 \mid 2a$ and $d_0 \mid (a + b)$. Therefore, $d_0 \mid 2$ and this implies that either $d_0 = 1$ or $d_0 = 2$.

§3.3. Exercise 11. We know that $(a, b) = 1$. This implies that $(a, a + b) = 1$. Let $d_1 = (a^2 + b^2, a + b)$. We will show that $d_1 = 1$ or $d_1 = 2$.

As is the previous problem, we can find integers m, n such that

$$m\,a + n\,(a + b) = 1.$$

Define, also as in the previous problem, $d_0 = (2a, a + b)$. We simplify the expression for d_1 and get that

$$d_1 = (a^2 + b^2, a + b) = (a^2 + b^2 + (a - b)(a + b), a + b) = (2a^2, a + b).$$

Using the linear combination above, we find that

$$m\,(2a^2) + 2an\,(a + b) = 2a.$$

We know that $d_1 \mid 2a^2$ and $d_1 \mid (a + b)$. Therefore, $d_1 \mid 2a$ and this implies that $1 \le d_1 \le d_0$ because d_0 is the greatest common divisor of $2a$ and $a + b$. But $d_0 \le 2$ and this implies that either $d_1 = 1$ or $d_1 = 2$.

§3.3. Exercise 14. Solution 1. Given that $(a, b) = 1$, we can find integers m, n such that

$$m\,a + n\,b = 1.$$

The condition $c \mid a + b$ implies that there exists an integer q such that $a + b = qc$. From this, we get

$$(m - n)a + (nq)c = 1, \qquad (mq)c + (n - m)b = 1.$$

This implies that $(a, c) = 1$, and $(b, c) = 1$.

§3.3. Exercise 14. Solution 2. The condition $c \mid a + b$ implies that there exists an integer q such that $a + b = qc$. Let $d_0 = (a, c)$ and $d_1 = (b, c)$.

We have that d_0 is a positive integer such that $d_0 \mid a$, $d_0 \mid c$. Therefore, d_0 divides any linear combination of a and c. In particular, this implies that $d_0 \mid (-a + qc) = b$.

We conclude that d_0 is a positive common divisor of a and b. However, a and b are relatively prime, so the only possibility is that $d_0 = 1$. In the same way, we prove that $d_1 = 1$.

§3.3. Exercise 14. Solution 3. Let $d_0 = (a, c)$ and $d_1 = (b, c)$.

We know that $d_0 \ge 1$. By way of contradiction, suppose that $d_0 > 1$. Then $d_0 \mid a$ and $d_0 \mid c$. We know that $c \mid a + b$, so $d_0 \mid a + b$. This also implies that $d_0 \mid (a + b) - a = b$.

The statements above imply that there exists a common divisor d_0 of a and b that satisfies $d_0 > 1$. This contradicts that a and b are relatively prime. We conclude that $d_0 = 1$.

In the same way, we prove that $d_1 = 1$.

§3.3. Exercise 16. a) Given that $(a, b) = 1$, we can find integers m_1, n_1 such that

$$m_1\, a + n_1\, b = 1.$$

In the same way, using that $(a, c) = 1$, we can find integers m_2, n_2 such that

$$m_2\, a + n_2\, c = 1.$$

From this, we find that

$$n_1\, b = 1 - m_1\, a, \qquad n_2\, c = 1 - m_2\, a.$$

Multiplying, $(n_1\, b)(n_2\, c) = (1 - m_1\, a)(1 - m_2\, a) = 1 + (m_1 m_2\, a - m_1 - m_2)\, a.$ This implies that

$$m_0\, a + n_0\, bc = 1.$$

where $m_0 = m_1 + m_2 - m_1 m_2\, a$, and $n_0 = n_1\, n_2$. We conclude that $(a, bc) = 1$.

Problem 10. a) It is clear that $(a + 2b, b) = (a, b) = 1$.

Problem 10. b) Using part a), we can find integers m, n such that

$$m\,(a + 2b) + n\, b = 1.$$

We simplify the expression for d_0 and get that

$$d_0 = (a + 2b, 4a + 3b) = (a + 2b, (4a + 3b) - 4(a + 2b)) = (a + 2b, -5b).$$

Using the linear combination above, we find that

$$5m\,(a + 2b) + (-n)\,(-5b) = 5.$$

By definition, we know that $d_0 \mid a + 2b$ and $d_0 \mid -5b$. Therefore, $d_0 \mid 5$. Given that $d_0 > 0$, we conclude that $d_0 = 1$ or $d_0 = 5$.