Solutions to Homework 3

Tim Smits

January 27, 2022

1. Recall from worksheet 3 the *least common multiple* of a and b, denoted $\text{lcm}(a, b)$. It is defined as the smallest positive integer ℓ such that:

i. It's a common multiple of a and b, i.e. $a \mid \ell$ and $b \mid \ell$.

ii. It's the smallest such common multiple, i.e. if $a \mid c$ and $b \mid c$, then $\ell \leq c$.

Prove that if $\gcd(a, b) = 1$, then $\text{lcm}(a, b) = ab$.

Solution: Let $\ell = \text{lcm}(a, b)$. Since $a \mid ab$ and $b \mid ab$ then by definition, we have $\ell \leq ab$. By Bezout's lemma, there exist integers x, y such that $ax + by = 1$. Multiplying by ℓ, we have $a\ell x + b\ell y = \ell$. As $a \mid \ell$ and $b \mid \ell$, we can write $\ell = ak = bm$ for some integers k, m. Plugging in yields $abmx + abky = \ell$. Since the left hand side is divisible by ab, this means $ab \mid \ell$, so $ab \leq \ell$. Combining the two inequalities yields $ab = \ell$.

2. Define a sequence of numbers F_n as follows:

$$F_0 = 1, \quad F_1 = 1$$
$$F_{n+1} = F_n + F_{n-1}, \quad n \geq 1$$

This sequence starts $1, 1, 2, 3, 5, 8, 13, 21, \ldots$. This sequence is called the *Fibonacci sequence*, and the number F_n is called the n^{th} Fibonacci number. Prove by induction that for all $n \geq 1$, the number of steps required for the Euclidean algorithm on the pair (F_{n+1}, F_n) to terminate is exactly n.

Solution: First, we start with the base case. We have $F_2 = 2$ and $F_1 = 1$, and the division algorithm says $2 = 1 \cdot 2 + 0$, so the Euclidean algorithm finishes after the first step. Now suppose that for some k, the Euclidean algorithm on (F_{k+1}, F_k) takes k steps to stop. We now want to run the Euclidean algorithm on F_{k+2} and F_{k+1}. By definition, we have $F_{k+2} = F_{k+1} \cdot 1 + F_k$. It's clear that $F_{k+1} > F_k$ because each Fibonacci number is obtained by adding a positive integer to the previous Fibonacci number, so this equation is then the form given by the division algorithm, i.e. the first step in the Euclidean algorithm. The Euclidean algorithm then continues on by running it on the pair (F_{k+1}, F_k) which by induction hypothesis, terminates in k steps, so the Euclidean algorithm on (F_{k+2}, F_{k+1}) terminates in $k + 1$ steps as desired. Therefore by induction, we're done.

Remark: Fibonacci numbers represent the "worst case scenario" for the Euclidean algorithm, in the sense that if you have positive integers a, b such that the Euclidean algorithm takes n steps, one can show that $a \geq F_{n+1}$ and $b \geq F_n$.

3. In this problem, you will give a proof that $\sqrt{2}$ is irrational using the Euclidean algorithm. Suppose that $\sqrt{2}$ was rational, so it can be written as $\sqrt{2} = \frac{a}{b}$ for some positive integers a, b with $b \neq 0$.

(a) Show that $a = b \cdot 1 + (a-b)$ with $0 \leq a-b < b$, so that this is the first step in the Euclidean algorithm on the pair (a,b) with $q_1 = 1$ and $r_1 = a-b$.

(b) Write down the next step in the Euclidean algorithm by performing the division algorithm on the pair $(b, a-b)$. What is q_2? What is the ratio r_1/r_2? (Your answers should be *numbers*, not involving the letters a, b).

(c) Prove that $q_n = q_2$ and $\frac{r_{n-1}}{r_n} = \frac{r_1}{r_2}$ for all $n \geq 2$. (*Hint: prove these both simultaneously via induction.*)

(d) Explain why the truth of the statement in (c) yields a contradiction, therefore proving that $\sqrt{2}$ must not be rational.

Solution:

(a) Note that $\sqrt{2} > 1$ because $2 > 1$. In particular, this says $a > b$ so $a - b > 0$. We have $a - b < b$ because $b > 0$, the equation $a = b \cdot 1 + (a-b)$ satisfies the conditions for q, r in the division algorithm. By uniqueness, we must have $q_1 = 1$ and $r_1 = a - b$.

(b) We have $\frac{b}{a-b} = \frac{1}{\frac{a-b}{b}}$. Note that $\frac{a-b}{b} = \frac{a}{b} - 1 = \sqrt{2} - 1$, so $\frac{b}{a-b} = \frac{1}{\sqrt{2}-1} = \sqrt{2}+1$. To figure out what q_2 and r_2 must be, suppose we have $b = (a-b) \cdot q_2 + r_2$ with $0 \leq r_2 < a - b$. Then $\frac{b}{a-b} = q_2 + \frac{r_2}{a-b}$. In particular, this says q_2 must be the integer part of $\frac{b}{a-b}$ because $\frac{r_2}{a-b} < 1$. Note that $2 < \sqrt{2}+1 < 3$, so $q_2 = 2$. This then says $\sqrt{2}+1 = 2 + \frac{r_2}{a-b} = 2 + \frac{r_2}{r_1}$, so $\frac{r_2}{r_1} = \sqrt{2} - 1$ gives $\frac{r_1}{r_2} = \sqrt{2}+1$. To figure out what r_2 actually is, we have $b = (a-b) \cdot 2 + (3b - 2a)$, and note that $\frac{3b-2a}{a-b} = \frac{3(b-a)+a}{a-b} = -3 + \frac{a}{a-b} = -3 + \frac{1}{\frac{a-b}{a}} = -3 + \frac{1}{1-\frac{b}{a}} = -3 + \frac{1}{1-\frac{1}{\sqrt{2}}} = \sqrt{2} - 1 < 1$. We also see that $0 \leq 3b - 2a$ because $\sqrt{2} < 3/2$ as $2 < 9/4$, so this says that $3b - 2a$ satisfies the remainder bound, yielding $r_2 = 3b - 2a$.

(c) We wish to prove that $q_n = 2$ and $\frac{r_{n-1}}{r_n} = \sqrt{2}+1$ for all $n \geq 2$. The base case was proven above in part (b), so assume it holds for all $1, 2, \ldots, k$ that $q_k = 2$ and $\frac{r_{k-1}}{r_k} = \sqrt{2}+1$. We wish to show it holds for $k+1$ as well. One of the steps in the Euclidean algorthim tells us that $r_{k-1} = r_k q_{k+1} + r_{k+1}$ with $0 \leq r_{k+1} < r_k$, so dividing says $\frac{r_{k-1}}{r_k} = q_{k+1} + \frac{r_{k+1}}{r_k}$. By assumption, $\frac{r_{k-1}}{r_k} = \sqrt{2}+1$, so $q_{k+1} = 2$ because similarly as above, it must be the integer part of $\sqrt{2}+1$. We then have $\sqrt{2}+1 = 2 + \frac{r_{k+1}}{r_k}$, so $\sqrt{2} - 1 = \frac{r_{k+1}}{r_k}$ then yields $\frac{r_k}{r_{k+1}} = \sqrt{2}+1$ as desired. Therefore by induction, we are done.

(d) Since $\frac{r_{n-1}}{r_n} = 1 + \sqrt{2}$ for all $n \geq 2$, we can never have $r_n = 0$ for any n. This means the Euclidean algorithm on a, b cannot ever terminate, which is a contradiction, because we proved that for any pair of integers it must stop. Therefore, $\sqrt{2}$ cannot be rational.

4. For each of the pairs of integers (a,b) below, do the following:

(i) Run the Euclidean algorithm to compute $\gcd(a,b)$.

(ii) Use back substitution to find integers x, y such that $ax + by = \gcd(a,b)$.

(a) $(504, 94)$

(b) $(-1260, 816)$

Solution: Details omitted since everyone knew what they were doing!

(a) $504 \cdot (-11) + 94 \cdot (59) = 2$, so we may take $x = -11$ and $y = 59$.

(b) $-1260 \cdot (11) + 816 \cdot (17) = 12$, so we may take $x = 11$ and $y = 17$.

5. Let $c \in \mathbb{Z}$. Prove that $ax + by = c$ has integer solutions if and only if $\gcd(a, b) \mid c$.

Solution: Suppose that $ax+by = c$ has integer solutions, so that there actually are integers x, y with $ax+by = c$. Since $\gcd(a, b)$ divides a and b, it therefore must divide the linear combination $ax + by$, which equals c. On the other hand, suppose that $\gcd(a, b) \mid c$, so $c = \gcd(a, b)k$ for some integer k. By Bezout's lemma, there are integers x, y such that $ax + by = \gcd(a, b)$, so multiplying by k yields $a(xk) + b(yk) = c$, which says the equation has the integer solution (xk, yk).

6. Let $d = \gcd(a, b)$ and suppose that $d \mid c$, so that by the previous problem, the equation $ax+by = c$ has integer solutions. Suppose you are given $x_0, y_0 \in \mathbb{Z}$ such that $ax_0 + by_0 = c$. Let $a = da'$ and $b = db'$ for some integers a', b'. Define, for any $k \in \mathbb{Z}$,

$$x_k = x_0 + b'k \qquad \text{and} \qquad y_k = y_0 - a'k.$$

Note: Try to avoid the use of fractions throughout this problem! You don't actually need them anywhere!

(a) Prove that for all $k \in \mathbb{Z}$, (x_k, y_k) is a solution to the equation $ax + by = c$.

(b) Now assume that (x, y) is another solution to the equation $ax + by = c$. Prove that there is some $k \in \mathbb{Z}$ for which $x = x_k$ and $y = y_k$.

(c) Find all integer solutions to the equation $37x + 47y = 103$.

Solution:

(a) Plugging in, we have $a(x_0 + b'k) + b(y_0 - a'k) = ax_0 + by_0 = c$.

(b) Suppose we have two solutions, (x_0, y_0) and (x, y). This says $ax_0+by_0 = c$ and $ax+by = c$, so equating yields $ax_0+by_0 = ax+by$. Combining like terms, we find $a(x-x_0) = b(y_0-y)$. Since $a = a'd$ and $b = b'd$, plugging in then gives $a'(x-x_0) = b'(y_0-y)$. Since $a' \mid b'(y_0-y)$ and a', b' are relatively prime, we must have $a' \mid (y_0 - y)$ so there is some k such that $y_0 - y = a'k$. Similarly, there is some ℓ such that $x - x_0 = b'\ell$. Plugging these in says $a'b'\ell = b'a'k$, so $k = \ell$. This says that $x = x_0+b'k = x_k$ and $y = y_0-a'k = y_k$ as desired.

(c) First, we need to find one solution. Running the Euclidean algorithm and performing back substitution tells us that $37 \cdot 14 + 47 \cdot (-11) = 1$, so multiplying by 103 says $37 \cdot (14 \cdot 103) + 37 \cdot (-11 \cdot 103) = 103$. Therefore, we have $x_0 = 14 \cdot 103 = 1442$ and $y_0 = -11 \cdot 103 = -1133$. Since $\gcd(37, 47) = 1$, we have $a' = 37$ and $b' = 47$. The previous parts say the solutions are given by (x_k, y_k) for integers k, so the solution set is $\{(x_k, y_k) : k \in \mathbb{Z}\} = \{(1442 + 47k, -1133 - 37k) : k \in \mathbb{Z}\}$.