Assignment 1 Solutions

by Pinar Colak

(1) Let $d = (110257, 110385)$. We know that d has to divide the difference of the numbers: $d|(110385 - 110257) = 128$. We note that $128 = 2^7$, which means that d is either 1 or is a power of 2. However, both 110257 and 110385 are odd, hence d cannot be even. It follows that $d = 1$ and that $\frac{110257}{110385}$ is reduced.

(2) Suppose $b = (a, d)$. Note that

$$a = qd + r \Rightarrow r = a - qd.$$

Since $b|d$ and $b|a$, we get $b|r$. Then b is a common divisor of both d and r, implying that $b|(r, d)$. Since (r, d) is the greatest common divisor, we get

$$b = (a, d) \leqslant (r, d).$$

Similarly, let $c = (r, d)$. Then $c|a$ as $a = qd + r$. We get that c is a common divisor of both a and d, implying that $c|(a, d)$. Then we get

$$c = (r, d) \leqslant (a, d).$$

As a result, we get

$$(a, d) = (r, d).$$

(3) (i) $a = 37$, $b = 50$. By Euclidean Algorithm

$$50 = 37 + 13$$

$$37 = 2(13) + 11$$

$$13 = 11 + 2$$

$$11 = 5(2) + \mathbf{1}$$

$$2 = 2 + 0.$$

Therefore, $(37, 50) = 1$.

(ii) $a = 2709$, $b = 5518$. By Euclidean Algorithm

$$5518 = 2(2709) + 100$$

$$2709 = 27(100) + 9$$

$$100 = 11(9) + \mathbf{1}$$

$$9 = 9(1) + 0.$$

Therefore, $(5518, 2709) = 1$.

(4) By using 1.3 (i)

$$1 = 11 - 5(2) = 11 - 5(13 - 11) = 6(11) - 5(13) = 6(37 - 2(13)) - 5(13)$$

$$= 6(37) - 17(13) = 6(37) - 17(50 - 37) = 23(37) - 17(50).$$

Hence $x = 23$ and $y = -17$.

(5) Since $(a, b) = d$, there exists x and y in $\mathbb{Z}$ such that

$$ax + by = d.$$

Moreover, $d \mid a$ and $d \mid b$. Divide both sides by d:

$$\frac{a}{d}x + \frac{b}{d}y = a'x + b'y = 1.$$

Note that if $c = (a', b')$, then c divides left hand side of the equation. Then it divides the right hand side as well, hence $c|1$. But this implies that $c = 1$. Thus, $(a', b') = 1$.

(6) ($\Longleftarrow$) If $a' \mid c$, then $a = a'd \mid cd$, whence $a \mid b'cd$ as well. But $b'd = b$, so $a \mid bc$.
($\Longrightarrow$) We first prove a lemma.

Lemma 1. *If A, B, C are positive integers such that $(A, B) = 1$ and $A \mid BC$, then $A \mid C$.*

Proof. Since $(A, B) = 1$, there exist $x, y \in \mathbb{Z}$ such that $Ax + By = 1$. It follows that $ACx + BCy = C$. The left hand side is divisible by A (since both terms are), hence the right hand side is also divisible. Hence, $A \mid C$ as claimed. $\square$

Assume that $a \mid bc$. Rewrite it as $a'd \mid b'dc$, which implies $a' \mid b'c$. From (1.5) we know that $(a', b') = 1$, so the Lemma implies that $a' \mid c$.

(7) (i) We will substitute $x = x_0 + b'k$ and $y = y_0 - a'k$ to show that they satisfy the equation. Let $d = (a, b)$, and observe that $ab' = (a'd)b' = a'(db') = a'b$. Thus,

$$\begin{aligned} ax + by &= a(x_0 + b'k) + b(y_0 - a'k) = ax_0 + ab'k + by_0 - ba'k \\ &= ax_0 + a'bk + by_0 - a'bk = ax_0 + by_0 = c. \end{aligned}$$

(ii) Let $d = (a, b)$. Assume x and y are both integral solution to the given equation, hence $ax + by = c$. We also know that $ax_0 + by_0 = c$. This means that

$$\begin{aligned} ax + by &= ax_0 + by_0 \\ ax - ax_0 &= by_0 - by \\ a(x - x_0) &= b(y_0 - y) \\ a'd(x - x_0) &= b'd(y_0 - y) \\ a'(x - x_0) &= b'(y_0 - y) \end{aligned}$$

.

Since we know from question (1.5) that $(a', b') = 1$, the Lemma above implies that $b' \mid (x_0 - x)$. Hence there exists an integer k such that $x - x_0 = b'k$. This means $x = x_0 + b'k$. Now substitute this back into the last equation we got, then

$$\begin{aligned} a'(x_0 + b'k - x_0) &= b'(y_0 - y) \\ a'b'k &= b'(y_0 - y) \\ a'k &= y_0 - y \\ y &= y_0 - a'k \end{aligned}$$

as desired.

(8) Let $d = (a, a+k)$, that means $d|a$ and $d|a+k$. Then d divides their difference as well: $d|a+k-a=k$.

(9) (i) Suppose $a|n$ and $b|n$. Hence we can find integeres c and d such that $n = ac$ and $n = bd$. If $(a, b) = 1$, then we can find integers x and y such that

$$ax + by = 1.$$

Multiply both sides by n:

$$\begin{aligned} anx + bny &= n \\ a(bd)x + b(ac)y &= n \\ (ab)dx + (ab)cy &= n. \end{aligned}$$

Note that ab divides both of the terms on the left hand side, so it divides right hand side as well. We get that $ab|n$.

(ii) No, it doesn't hold: let $a = 2$, $b = 4$ and $n = 4$. It is clear that $2|4$ and $4|4$, however, $2(4) = 8$ does not divide 4.

(10) (i) We have

$$\begin{aligned} n_j &= q_{j+1}n_{j+1} + n_{j+2} \\ n_{j+1} &= q_{j+2}n_{j+2} + n_{j+3} \end{aligned}$$

Then we have

$$\begin{aligned} n_j &= q_{j+1}(q_{j+2}n_{j+2} + n_{j+3}) + n_{j+2} \\ &= n_{j+2}(q_{j+1}q_{j+2} + 1) + q_{j+1}n_{j+3}. \\ &\geqslant 2n_{j+2} + n_{j+3}. \end{aligned}$$

We know that $n_{j+3} \geqslant 0$, hence

$$n_j \geqslant 2n_{j+2}.$$

Moreover, with the exception of the last step of the algorithm, $n_{j+3} > 0$, so

$$n_j > 2n_{j+2}$$

for all such j. We conclude that

$$n_{j+2} < \frac{1}{2}n_j$$

for all $j \geqslant 1$, with the exception of at most one value of j (in which case $n_{j+2} \leqslant \frac{1}{2}n_j$).

(ii) According to the Euclidean Algorithm, we have the following equations:

$$\begin{aligned} a &= bq_1 + n_2 \\ b &= n_2q_2 + n_3 \\ n_2 &= n_3q_3 + n_4 \\ &\dots \\ n_{k-3} &= n_{k-2}q_{k-2} + n_{k-1} \\ n_{k-2} &= n_{k-1}q_{k-1} + 0. \end{aligned}$$

This means that we have $k-2$ steps to get the gcd. We will use the first part of the question to prove the statement.

If $k-2$ is even, then $k-1$ is odd, and $n_{k-1} \geqslant 1$. Then

$$\begin{aligned} b = n_1 > 2n_3 > 4n_5 > 8n_7 > \cdots \geqslant 2^{\frac{k-2}{2}} n_{k-1} \geqslant 2^{\frac{k-2}{2}}. \\ b \geqslant 2^{\frac{k-2}{2}} \\ \log_2 b \geqslant \frac{k-2}{2} \\ 2\log_2 b \geqslant k-2 \end{aligned}$$

as desired.

If $k-2$ is odd, then $n_{k-2} \geqslant 2$ (note that it cannot be 1, as then the process would have ended in the previous step). Then

$$\begin{aligned} b = n_1 > 2n_3 > 4n_5 > 8n_7 > \cdots \geqslant 2^{\frac{k-3}{2}} n_{k-2} \geqslant 2^{\frac{k-1}{2}} > 2^{\frac{k-2}{2}}. \\ b > 2^{\frac{k-2}{2}} \\ \log_2 b > \frac{k-2}{2} \\ 2\log_2 b > k-2 \end{aligned}$$

as desired.

Hence, in either case, the algorithm terminates after at most $2\log_2 b$ steps.