CS5610 Assignment 1

Gautam Singh
CS21BTECH11018

1) The given equation is
$$6x + 10y = 2. \tag{1}$$
Computing the GCD of 6 and 10 using Euclid's extended algorithm, we get
$$\begin{pmatrix} 6 \\ 10 \end{pmatrix} \xrightarrow{q=1} \begin{pmatrix} 4 \\ 6 \end{pmatrix} \xrightarrow{q=1} \begin{pmatrix} 2 \\ 4 \end{pmatrix} \xrightarrow{q=2} \begin{pmatrix} 0 \\ 2 \end{pmatrix}. \tag{2}$$
where q is the quotient on dividing the larger number by the smaller number. Since $2 \mid 2$, (1) equation has a solution over integers. The transition matrix is given by
$$M = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} -5 & 3 \\ 2 & -1 \end{pmatrix}. \tag{3}$$
Thus, the required integer solution is $(x, y) = (2, -1)$.
2) Using Bezout's Lemma, we know that the equation $6x + 10y = c$ has an integer solution if $\gcd(6, 10) \mid c$. Hence, we may write
$$6x + 10y = 2t \tag{4}$$
for some integer t. The new equation is
$$2t + 15z = 1. \tag{5}$$
Using Euclid's extended algorithm, we get
$$\begin{pmatrix} 2 \\ 15 \end{pmatrix} \xrightarrow{q=7} \begin{pmatrix} 1 \\ 2 \end{pmatrix} \xrightarrow{q=2} \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{6}$$
Since $1 \mid 1$, (5) has a solution over integers. The transition matrix is given by
$$M = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -7 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 15 & -2 \\ -7 & 1 \end{pmatrix}. \tag{7}$$
Hence, $(t, z) = (-7, 1)$. Suppose that (x_0, y_0) is an integer solution to (1). Then, an integer solution to (4) is (tx_0, ty_0). From the previous question, $(x_0, y_0) = (2, -1)$. Hence, an integer solution to (5) is $(x, y, z) = (-14, 7, 1)$.
3) Denote $(a, b) \triangleq \gcd(a, b)$. If $m = n$, then we have
$$\left(a^m - 1, a^n - 1\right) = a^m - 1 = a^{\gcd(m,n)} - 1 \tag{8}$$
and the claim holds. Suppose without loss of generality that $m > n$. Then, the proof proceeds by induction on $m + n$. The base case is when $m = 2$ and $n = 1$, whence
$$\begin{aligned} \left(a^2 - 1, a - 1\right) &= \left((a - 1)(a + 1), a - 1\right) \qquad (9) \\ &= a - 1 = a^{(2,1)} - 1. \qquad (10) \end{aligned}$$
For the induction step, we make use of the following lemma.
Lemma 1. *If integers a, b satisfy $(a, b) = 1$, then for any integer c, $(ab, c) = (a, c)(b, c)$.*

Proof. Using Bezout's Lemma, there exist integers x and y such that

$$ax + by = 1. \tag{11}$$

Multiplying (11) by c, we see that $acx + bcy = c$, which can be recast as

$$(a, c)(b, c)\left[\frac{a}{(a, c)}\frac{c}{(b, c)}x + \frac{b}{(b, c)}\frac{c}{(a, c)}y\right] = c \tag{12}$$

where $\frac{a}{(a,c)}$ etc. are integers. Thus, $(a, c)(b, c) \mid c$. Since $(a, c) \mid a$ and $(b, c) \mid b$, we obtain $(a, c)(b, c) \mid ab$. Hence, $(a, c)(b, c) \mid (ab, c)$. To prove the other direction, applying Bezout's lemma twice gives us integers p, q, r, s such that

$$ap + cq = (a, c) \tag{13}$$
$$br + cs = (b, c). \tag{14}$$

Thus,

$$(a, c)(b, c) = (ap + cq)(br + cs) \tag{15}$$
$$= abpr + c(aps + bqr + cqs). \tag{16}$$

Hence, $(ab, c) \mid (a, c)(b, c)$. Putting both directions together, we have $(ab, c) = (a, c)(b, c)$. $\square$

In the original question, suppose that the claim holds for all $k < m + n$. Then, using Euclid's algorithm,

$$(a^m - 1, a^n - 1) = (a^m - a^n, a^n - 1) \tag{17}$$
$$= \left(a^n\left(a^{m-n} - 1\right), a^n - 1\right) \tag{18}$$
$$= (a^n, a^n - 1)\left(a^{m-n} - 1, a^n - 1\right) \tag{19}$$
$$= \left(a^{m-n} - 1, a^n - 1\right) \tag{20}$$
$$= a^{(m-n,n)} - 1 = a^{(m,n)} - 1. \tag{21}$$

where (19) follows from Lemma 1 since

$$a^n\left(a^{m-n}\right) + (-1)(a^m - 1) = 1 \implies (a^n, a^m - 1) = 1 \tag{22}$$

and (21) follows from the induction hypothesis since $m - n + n = m < m + n$.

4) The given equation is

$$2x + 3y + 5z = 0. \tag{23}$$

We recast this as

$$2x + 3y = -5z. \tag{24}$$

Now, using Euclid's algorithm, we obtain

$$\begin{pmatrix} 2 \\ 3 \end{pmatrix} \xrightarrow{q=1} \begin{pmatrix} 1 \\ 2 \end{pmatrix} \xrightarrow{q=2} \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{25}$$

and since $1 \mid -5z$ for all integers z, there exists a solution to (23). We find the solution for

$$2x + 3y = 1 \tag{26}$$

as follows.

$$M = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & -2 \\ -1 & 1 \end{pmatrix}. \tag{27}$$

whence a particular solution for (26) is $(x, y) = (-1, 1)$. Multiplying (26) by $-5z$, a particular solution of (24) is $(x, y, z) = (5z, -5z, z)$. The entire family of solutions is then given by $(x, y, z) = (5z - 3t, 2t - 5z, z)$ for all integers t, z.