QUIZ 1 VERSION B SOLUTIONS
MATH 103A, SUMMER 2021

(1) Suppose $a, b, c \in \mathbf{Z} \setminus \{0\}$ and $\gcd(a, b) = 1$. If $a|bc$ then $a|c$.

(2) *Solution 1.* Notice that $[11]_{36}[x]_{36} = [1]_{36}$ if and only if $11x \equiv 1 \pmod{36}$. The latter means that $11x - 1 = 36y$ for some integer y. Hence we are looking for an integer solution for $11x - 36y = 1$. We know that we can use Euclid's algorithm to do this.

$$\begin{aligned} 36 &= 11 \cdot 3 + 3 \\ 11 &= 3 \cdot 3 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0. \end{aligned}$$

Hence as it is discussed in the lectures, we have

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 36 \\ 11 \end{pmatrix}.$$

We have

$$\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} = \begin{pmatrix} 1 & -3 \\ -3 & 10 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & -3 \\ -3 & 10 \end{pmatrix} = \begin{pmatrix} -3 & 10 \\ 4 & -13 \end{pmatrix}.$$

Hence

$$\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} -3 & 10 \\ 4 & -13 \end{pmatrix} = \begin{pmatrix} 4 & -13 \\ * & * \end{pmatrix},$$

and so $1 = 4 \cdot 36 + (-13) * 11$. Therefore $[-13]_{36} = [23]_{36}$ is a desired solution.

Solution 2. Similar to the beginning of the first solution, we have to find an integer solution for $11x - 36y = 1$. Hence we have to find a solution for the following congruence relation

$$36y \equiv -1 \pmod{11}.$$

Since $36 \equiv 3 \pmod{11}$, we have to solve $3y \equiv -1 \pmod{11}$. Notice that $3 \cdot 4 = 12 \equiv 1 \pmod{11}$. Hence -4 is a solution of the above congruence relation. Hence $y = -4$ should correspond to an integer solution of $11x - 36y = 1$. From this we obtain the same answer as in the first solution.

(3) Using Euclid's division algorithm, we get

$$\begin{aligned} 703 &= 629 \cdot 1 + 74 \\ 629 &= 74 \cdot 8 + 37 \\ 74 &= 37 \cdot 2 + 0 \end{aligned}$$

Therefore $\gcd(703, 629) = 37$. Now, as we have seen in the lectures,

$$\begin{pmatrix} 37 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -8 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 703 \\ 629 \end{pmatrix}.$$

Since $\begin{pmatrix} 0 & 1 \\ 1 & -8 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -8 & 9 \end{pmatrix}$, we obtain

$$\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -8 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} -8 & 9 \\ * & * \end{pmatrix}.$$

Thus $37 = (703) \cdot (-8) + (629) \cdot (9)$.

(4) Suppose $[x]_n = [y]_n$ then $n|(y-x)$. Since $m|n$, we have $m|(y-x)$ and therefore $[x]_m = [y]_m$. In other words,

$$f([x]_n) = [x]_m = [y]_m = f([y]_n)$$

and f is well defined.

(5) *solution 1.* We observe that for every integer n,

$$1 = 11 \cdot (5n+1) - 5 \cdot (11n+2).$$

Therefore $\gcd(11n+2, 5n+1) = 1$.

Solution 2. We try to follow Euclid's idea and make use of the equation $\gcd(a,b) = \gcd(a-qb, b)$ for every integer q. Choosing an appropriate q, we reduce the coefficient of n. Hence we have

$$\gcd(11n+2, 5n+1) = \gcd(11n+2-(2)(5n+1), 5n+1) = \gcd(n, 5n+1),$$

and

$$\gcd(5n+1, n) = \gcd((5n+1)-5n, n) = \gcd(1, n) = 1.$$

This completes the solution.