Chapter 8

Ethan Mahintorabi

April 17, 2018

8.B

(i)

Consider $a = 87$ and $b = 8$. We have $S = \{x \in \mathbb{Z} | 0 \leq 8x \leq 87\} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. So $maxS = 10 = q$ and $r = 87 - 8 \cdot 10 = 7 = r$

Consider $a = 138$ and $b = 17$. We have $S = \{x \in \mathbb{Z} | 0 \leq 17x \leq 87\} = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$. So $maxS = 10 = q$ and $r = 138 - 17 \cdot 8 = 2 = r$

Consider $a = 192$ and $b = 12$. We have $S = \{x \in \mathbb{Z} | 0 \leq 12x \leq 87\} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$. So $maxS = 16 = q$ and $r = 192 - 12 \cdot 16 = 0 = r$

(ii)

Example 1 We will find the inverse [3] in $\mathbb{Z}/7\mathbb{Z}$ starting with the division algorithm and the expression

$$7 = 3 \cdot 2 + 1.$$

Now by solving for the remainder we have

$$1 = 7 \cdot 1 + 3 \cdot -2.$$

Lastly substituting our expressions in reverse we see that the multiplicative inverse is equal to $[-2]$ or [5].

Example 2 We will find the inverse [5] in $\mathbb{Z}/19\mathbb{Z}$ starting with the division algorithm and the expression

$$19 = 5 \cdot 3 + 4$$
$$5 = 4 \cdot 1 + 1.$$

Now by solving for the remainder we have

$$\begin{aligned}1 &= 5 - 4 \cdot 1 \\ 4 &= 19 - 5 \cdot 3.\end{aligned}$$

Lastly we will apply the definitions in reverse to solve bezot's identity for

$$\begin{aligned}1 &= 5 - (19 - 5 \cdot 3) \cdot 1 \\ &= 5 \cdot 4 - 19 \\ &= 5 \cdot (19 - 5 \cdot 3) - 19 \\ &= 19 \cdot 4 + 5 \cdot -15.\end{aligned}$$

As we can see the multiplicative inverse of [5] in $\mathbb{Z}/19\mathbb{Z}$ is $[-15] = [4]$.

Example 3 We will find the inverse [17] in $\mathbb{Z}/37\mathbb{Z}$ starting with the division algorithm and the expression

$$\begin{aligned}37 &= 17 \cdot 2 + 3 \\ 17 &= 3 \cdot 5 + 2 \\ 3 &= 2 \cdot 1 + 1\end{aligned}$$

Now by solving for the remainder we have

$$\begin{aligned}1 &= 3 - 2 \cdot 1 \\ 2 &= 17 - 3 \cdot 5 \\ 3 &= 37 - 17 \cdot 2\end{aligned}$$

Lastly we will apply the definitions in reverse to solve bezot's identity for

$$\begin{aligned}1 &= 3 - (17 - 3 \cdot 5) \cdot 1 \\ &= 3 \cdot 6 - 17 \\ &= 6 \cdot (37 - 17 \cdot 2) - 17 \\ &= 6 \cdot 37 - 12 \cdot 17 - 17 \\ &= 6 \cdot 37 + -13 \cdot 17\end{aligned}$$

As we can see the multiplicative inverse of [17] in $\mathbb{Z}/37\mathbb{Z}$ is $[-13] = [24]$.