Basic Number Theory and Modulo Joy
Chapter 3

1. (a) Find integers x and y such that $17x + 101y = 1$
The way that you start this problem is using the Extended Euclidean Algorithim. You can go about that as follows. You can use the Extended Eucleadean algorithm to find s and t of the following equation

$$as + nt = gcd(a, n)$$

. So in our case $a = 17, n = 101, gcd(a, n) = 1$. The first step is to do the Euclidean algorithm in order to find the quotients.

$$\begin{aligned} 101 &= 17 \cdot 5 + 16 \\ 17 &= 16 \cdot 1 + 1 \\ 16 &= 1 \cdot 16 \end{aligned}$$

Our quotients are $5, 1, 16$. The extended Euclidean algorithm gives us a recursion in terms of the quotients q and s, t to find s_n and t_n. That is of the following form

$$\begin{aligned} x_0 = 0, x_1 = 1, x_j &= -q_{j-1}x_{j-1} + x_{j+2} \\ y_0 = 1, y_1 = 0, y_j &= -q_{j-1}y_{j-1} + y_{j+2} \end{aligned}$$

Now knowing this equation we can solve for x_n where n is the last step in the Euclidean Algorithim.

$$\begin{aligned} x_0 &= 0 x_1 = 1 \\ x_2 &= -5 \cdot 1 + 0 \\ x_3 &= -1 \cdot -5 + 1 \end{aligned}$$

Going through these same steps for solving y_n we get $x_n = 6$ and $y_n = -1$. Checking our answer we see that this indeed true.

(b) Find $17^{-1} \pmod{101}$
To find the inverse of $17 \pmod{101}$. We need to find a number x that holds the following condition $17x \equiv 1 \pmod{101}$. If we look close at the equation from part (a). We can write it as the following

$$\begin{aligned} 17x + 101y &= 1 \\ 17x &= 1 - 101y \\ 17 - 1 &= -101y \\ 17 - 1 &= 101 \cdot (-y) \\ 17x &\equiv 1 \pmod{101} \end{aligned}$$

So x is 6 in other words $17^{-1} \pmod{101}$ is 6

2. (a) Solve $7d \equiv 1 \pmod{30}$
Similar to our solution to question 1. We need to use the Euclidean Algorithim to find the quotients then solve for the equation $as + nt = 1$ where $a = 7, n = 30$. Then d will be s.

$$\begin{aligned} 30 &= 7 \cdot 4 + 2 \\ 7 &= 4 \cdot 1 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 \end{aligned}$$

Now knowing this equation we can solve for x_n where n is the last step in the Euclidean Algorithim.

$$\begin{aligned} x_0 &= 0, x_1 = 1 \\ x_2 &= -4 \cdot 1 + 0 \\ x_3 &= -1 \cdot -4 + 1 \\ x_3 &= -1 \cdot -4 + 1 \end{aligned}$$

Going through these same steps for solving y_n we get $x_n = 6$ and $y_n = -1$.