Homework 18 Solutions

Problems

1. **The goal of this problem is to find $5/17 \pmod{31}$. Note that 31 is prime, and thus we know that a solution exists.**

   (a) Use the Euclidean Algorithm to find integers x and y such that $17x + 31y = 1$.

   (b) Using part (a), what is $1/17 \pmod{31}$?

   (c) Using part (b), find $5/17 \pmod{31}$.

   Let's apply the Euclidean algorithm:

$$\begin{aligned} 31 &= 17 + 14 \\ 17 &= 14 + 3 \\ 14 &= 4 \times 3 + 2 \\ 3 &= 2 + 1 \end{aligned}$$

   And now backwards:

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (14 - 4 \times 3) = -14 + 5 \times 3 \\ &= -14 + 5(17 - 14) = 5 \times 17 - 6 \times 14 \\ &= 5 \times 17 - 6(31 - 17) = \boxed{-6 \times 31 + 11 \times 17} \end{aligned}$$

   So we see that $11 \times 17 = 1$ up to adding on a multiple of 31. In other words $1/17 \equiv \boxed{11} \pmod{31}$.

   For the last part, then, $5/17 \equiv 5 \times 11 \equiv 55 \equiv \boxed{24} \pmod{31}$

2. **Use the Euclidean algorithm to compute the following.**

   (a) $1/13 \pmod{97}$.

   (b) $1/73 \pmod{17}$.

   We must solve for x in $1 = 13x + 97y$. Using the Euclidean algorithm, we find

$$\begin{aligned} 97 &= 7 \times 13 + 6 \\ 13 &= 2 \times 6 + 1 \end{aligned}$$

   and running it backwards,

$$\begin{aligned} 1 &= 13 - 2 \times 6 \\ &= 13 - 2 \times (97 - 7 \times 13) = 15 \times 13 - 2 \times 97 \end{aligned}$$

   so $1/13 \equiv \boxed{15} \pmod{97}$.

   Note that $73 \equiv 5 \pmod{17}$. Hence, we solve for x in $1 = 5x + 17y$. Using the Euclidean algorithm, we find

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

and so

$$
\begin{aligned}
1 &= 5 - 2 \times 2 \\
&= 5 - 2 \times (17 - 3 \times 5) = 7 \times 5 - 2 \times 17
\end{aligned}
$$

so $1/73 \equiv \boxed{7} \pmod{17}$.

3. **Compute the following divisions:**

   (a) $7/10 \pmod{41}$.

   (b) $10/2 \pmod{31}$.

   (c) $5/16 \pmod{17}$.

   Euclid for part (a) is short:

$$
41 = 4 \times 10 + 1
$$

   and backwards:

$$
1 = 41 - 4 \times 10
$$

   so $1/10 \equiv -4 \equiv 37 \pmod{41}$.

   Then $7/10 \equiv -4 \times 7 \equiv -28 \equiv \boxed{13} \pmod{41}$.

   No need for any Euclidean messing here, because we know how to divide 10 by 2: $10/2 \equiv \boxed{5} \pmod{31}$.

   $16 \equiv -1 \pmod{17}$. So $5/16 \equiv 5/-1 \equiv -5 = \boxed{12} \pmod{17}$.