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. **Compute the following divisions:**

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

   (b) $9/23 \pmod{41}$.

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

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

   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 shortcuts for part (b). Let's hit this with Euclid, once frontways, and once backaways:

$$\begin{aligned} 41 &= 23 + 18 \\ 23 &= 18 + 5 \\ 18 &= 3 \times 5 + 3 \\ 5 &= 3 + 2 \\ 3 &= 2 + 1 \end{aligned}$$

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5 - 3) = 2 \times 3 - 5 \\ &= 2 \times (18 - 3 \times 5) - 5 = 2 \times 18 - 7 \times 5 \\ &= 2 \times 18 - 7 \times (23 - 18) = 9 \times 18 - 7 \times 23 \\ &= 9 \times (41 - 23) - 7 \times 23 = 9 \times 41 - 16 \times 23 \end{aligned}$$

Hence $1/23 \equiv -16 \pmod{41}$, so $9/23 \equiv 9 \times -16 \equiv -144 \equiv \boxed{20} \pmod{41}$.

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