Homework 5 Solutions

Math 55, DIS 101-102

4.4.6 [2 points]

A number of people made arithmetic mistakes on this one. . . to minimize the chance of that happening, be sure to simplify your equations at every step so that you aren't dealing with too many terms.

1. (a = 2, m = 17)

$$17 - 2 \cdot 8 = 1$$

   Therefore, $(-8) \equiv 9$ is a multiplicative inverse of 2 mod 17.

2. (a = 34, m = 89)

$$\begin{aligned}
89 - 2 \cdot 34 &= 21 \\
34 - 21 &= 13 \\
21 - 13 &= 8 \\
13 - 8 &= 5 \\
8 - 5 &= 3 \\
5 - 3 &= 2 \\
3 - 2 &= 1 \\
3 - (5 - 3) &= 1 \\
2 \cdot 3 - 5 &= 1 \\
2 \cdot (8 - 5) - 5 &= 1 \\
2 \cdot 8 - 3 \cdot 5 &= 1 \\
2 \cdot 8 - 3 \cdot (13 - 8) &= 1 \\
5 \cdot 8 - 3 \cdot 13 &= 1 \\
5 \cdot (21 - 13) - 3 \cdot 13 &= 1 \\
5 \cdot 21 - 8 \cdot 13 &= 1 \\
5 \cdot 21 - 8 \cdot (34 - 21) &= 1 \\
13 \cdot 21 - 8 \cdot 34 &= 1 \\
13 \cdot (89 - 2 \cdot 34) - 8 \cdot 34 &= 1 \\
13 \cdot 89 - 34 \cdot 34 &= 1
\end{aligned}$$

   Therefore $(-34) \equiv 55$ is a multiplicative inverse of 34 mod 89. This particular choice of a and m was rather annoying because Fibonacci numbers make the Euclidean algorithm take as long as it possibly can.

3. (a = 144, m = 233)

   More Fibonacci numbers. . . the gcd will be 1, and we'll use the previous problem to get to a solution faster:

$$\begin{aligned}
233 - 144 &= 89 \\
144 - 89 &= 55 \\
89 - 55 &= 34 \\
13 \cdot 89 - 34 \cdot 34 &= 1 \\
13 \cdot 89 - 34 \cdot (89 - 55) &= 1 \\
-21 \cdot 89 + 34 \cdot 55 &= 1 \\
-21 \cdot 89 + 34 \cdot (144 - 89) &= 1 \\
34 \cdot 144 - 55 \cdot 89 &= 1 \\
34 \cdot 144 - 55 \cdot (233 - 144) &= 1 \\
89 \cdot 144 - 55 \cdot 233 &= 1
\end{aligned}$$

Therefore 89 is a multiplicative inverse of 144 mod 233. Note that the answers in these last 2 problems were both Fibonacci numbers as well. . . there is a relationship here that we'll show on Monday using induction.

4. (a = 200, m = 1001)

$$1001 - 5 \cdot 200 = 1$$

Therefore, $(-5) \equiv 996$ is a multiplicative inverse of 200 mod 1001. Several people made the mistake of saying 5 was the multiplicative inverse, missing the minus sign.

4.4.7 [0 points]

Good answer: If $ab \equiv 1 \pmod{m}$ and $ac \equiv 1 \pmod{m}$ then $ab \equiv ac \pmod{m}$, so because $\gcd(a, m) = 1$ we can conclude that $b \equiv c \pmod{m}$.

Slick answer: $c \equiv c \cdot 1 \equiv c(ab) \equiv (ca)b \equiv 1 \cdot b \equiv b \pmod{m}$.

4.4.8 [2 points]

Best answer: prove by contraposition, showing that if there exist x, y such that $ax + my = 1$ then $\gcd(a, m) = 1$.

Proof: If $ax+my = 1$ then $\gcd(a, m) \leq \gcd(ax, m) = \gcd(ax+my, m) = \gcd(1, m) = 1$, so $\gcd(a, m) = 1$.

Also good: If $d|a$ and $d|m$ then $d|ax + my$ for any x and y, so if $ax + my = 1$ then $\gcd(a, m)|1$. Therefore $\gcd(a, m) = 1$.

4.4.16 [2 points]

1. $2 \cdot 6 \equiv 3 \cdot 4 \equiv 5 \cdot 9 \equiv 7 \cdot 8 \equiv 1 \pmod{11}$.
2. $10! \equiv 1 \cdot (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \cdot 10 \equiv 1^6 \cdot (-1) \equiv -1 \pmod{11}$.

4.4.33 [2 points]

$7^{121} \equiv (7^{12})^{10} \cdot 7 \equiv 1^{10} \cdot 7 \equiv 7 \pmod{13}$.

4.4.50

The numbers 4 and 7 are small enough that you could do this by trial and error: for example (3,5) is 5 mod 7, which gives the four options 5,12,19,26. Of these four, only 19 is congruent to 3 mod 4. Some people wrote out all 28 options, which is a little inefficient.

Here's a slicker way that gets at the spirit of the proof for the Chinese Remainder Theorem: observe that 21 corresponds to (1,0) while 8 corresponds to (0,1). This means that (a, b) corresponds to $21a + 8b \bmod 28$. This method is more generalizable and easier to apply to larger cases.

Answers:

1. $(0, 0) \mapsto 0$
2. $(1, 0) \mapsto 21$
3. $(1, 1) \mapsto 21 + 8 = 29 \equiv 1$
4. $(2, 1) \mapsto 2 \cdot 21 + 8 = 50 \equiv 22$
5. $(2, 2) \mapsto 2 \cdot (1, 1) = 2$
6. $(0, 3) \mapsto 3 \cdot 8 = 24$
7. $(2, 0) \mapsto 2 \cdot 21 = 42 \equiv 14$
8. $(3, 5) \mapsto 3 \cdot 21 + 5 \cdot 8 = 103 \equiv 19$
9. $(3, 6) \mapsto (3, 5) + 8 = 27$. (Also, $(3, 6) = (-1, -1) = -(1, 1) = -1 \equiv 27$.)