Math 255 - Spring 2018
Homework 8 Solutions

1. (a) Since $(2, 17) = 1$, there will be a unique solution. Furthermore, it might be easy to see that $2 \cdot 9 = 18 \equiv 1 \pmod{17}$, and therefore $2^{-1} \equiv 9 \pmod{17}$. (If this is not clear, no worries, we can do the Euclidean algorithm to find the inverse of 2 modulo 17. This always works but I will start to point out the little tricks that go faster.)

   Therefore, multiplying both sides of the equation by 9, we get

$$\begin{aligned} 9 \cdot 2x &\equiv 9 \cdot 1 \pmod{17} \\ x &\equiv 9 \pmod{17} \end{aligned}$$

   and the unique solution is $x \equiv 9 \pmod{17}$.

   (b) We have that $(6, 15) = 3$, and $3|15$, so there will be three solutions. We begin by dividing **everything** by 3, to obtain the equation

$$2x \equiv 5 \pmod{7}.$$

   Now $(2, 7) = 1$, so this equation has a unique solution. Furthermore, since $2 \cdot 4 = 8 \equiv 1 \pmod 7$, we have that $2^{-1} \equiv 4 \pmod 7$. Therefore multiplying both sides by 4 we get

$$\begin{aligned} 4 \cdot 2x &\equiv 4 \cdot 5 \pmod{7} \\ x &\equiv 6 \pmod{7}. \end{aligned}$$

   Now to solve the problem it remains to lift $x \equiv 6 \pmod 7$ to the possible congruence classes modulo 21. The lifts are

$$x \equiv 6, 13, 20 \pmod{21}.$$

   Therefore those are the 3 solutions modulo 21.

   Note that $x \equiv 6 \pmod 7$ is the same as $x \equiv -1 \pmod 7$. If we "naively" lift $x \equiv -1 \pmod 7$ to $x \equiv -1 \equiv 20 \pmod{21}$, we still get a valid lift!

   (c) Since the numbers are small, we can compute $(36, 102)$ by factoring each into their prime factors: $36 = 2^2 \cdot 3^2$ and $102 = 2 \cdot 3 \cdot 17$, so $(36, 102) = 6$. Since 6 does not divide 8, this congruence has no solution.

   (d) We have that $(4, 18) = 2$, and 2 divides 8, so this congruence has two solutions. We begin by dividing **everything** by 2, and we get the equation

$$2x \equiv 4 \pmod{9}.$$

   Here $(2, 9) = 1$, so we **can** divide by 2 on both sides (really we multiply by 2^{-1}, whatever it may be), to get the solution $x \equiv 2 \pmod 9$.

We now lift $x \equiv 2 \pmod 9$ to the possible congruence classes modulo 18; the lifts are

$$x \equiv 2, 11 \pmod{18}.$$

These are the two solutions modulo 18.

Note that we may not divide both sides by 4 in the equation $4x \equiv 8 \pmod{18}$, since 4 is not a unit modulo 18 ($4^{-1} \pmod{18}$ does not exist). If we are careless and we try anyway, we get only the solution $x \equiv 2 \pmod{18}$ and miss the solution $x \equiv 11 \pmod{18}$, which is incorrect. In short, we can only divide by 2 if 2^{-1} exists!

(e) Here we use the Euclidean Algorithm to compute $(20, 1984)$, because 1984 is a bit of a large number:

$$\begin{aligned} 1984 &= 20 \cdot 99 + 4 \\ 20 &= 5 \cdot 4. \end{aligned}$$

Therefore $(20, 1984) = 4$, and since 4 divides 984, this congruence has four solutions.

We again divide everything by 4 to get the congruence

$$5x \equiv 246 \pmod{496},$$

which has a unique solution. To find $5^{-1} \pmod{496}$, we can certainly use the Euclidean Algorithm and back-substitution; that would be very fast and easy. But here is a trick: We have that

$$495 \equiv -1 \pmod{496}.$$

Since $495 = 5 \cdot 99$, it means that

$$5 \cdot 99 \equiv -1 \pmod{496},$$

and multiplying both sides by -1 we get

$$5 \cdot (-99) \equiv 1 \pmod{496}.$$

Therefore we have

$$5^{-1} \equiv -99 \equiv 397 \pmod{496}.$$

We now use this to solve

$$5x \equiv 246 \pmod{496},$$

which gives

$$x \equiv 246 \cdot 397 \equiv 97,662 \equiv 446 \pmod{496}.$$

(We can get this last congruence by subtracting from $97,662$ multiples of 496:

$$\begin{aligned}97,662 &\equiv 97,663 - 496 \cdot 100 \equiv 48,062 \pmod{496}\\ &\equiv 48,062 - 496 \cdot 80 \equiv 8382 \pmod{496}\\ &\equiv 8382 - 496 \cdot 15 \equiv 942 \pmod{496}\\ &\equiv 942 - 496 \equiv 446 \pmod{496}.)\end{aligned}$$

In any case, it only remains to lift $x \equiv 446 \pmod{496}$ to its preimages modulo 1984:

$$x \equiv 446, 942, 1438, 1934 \pmod{1984}.$$

Those are the four solutions we were promised!

2. The key is to translate this problem into an equation we can solve. The sequence

$$a, 2a, 3a, \ldots, ba$$

can be written more compactly as

$$ax \quad \text{for} \quad 1 \leq x \leq b.$$

Furthermore, something is a multiple of b if and only if it is congruent to 0 modulo b.

Therefore, the question is: As x ranges over $1 \leq x \leq b$, how many solutions does the equation

$$ax \equiv 0 \pmod{b}$$

have? In fact, if we allow $x = 0$ instead of $x = b$ (which is okay because $0 \equiv b \pmod{b}$), all we are asking is: How many solutions does the equation

$$ax \equiv 0 \pmod{b}$$

have?

We apply Theorem 1 to answer this question. We note first that since every integer divides 0, then certainly (a, b), no matter what it is, divides 0. Therefore, there are always exactly (a, b) solutions to this equation, and therefore (a, b) multiples of b in the sequence $a, 2a, \ldots, ba$.

We illustrate this with two examples: If $(a, b) = 1$, then the only multiple of b in the sequence is ba. However, if $a = 14$ and $b = 6$, then $(14, 6) = 2$, and there are indeed 2 multiples of 6 in the sequence

$$14, 28, 42 = 6 \cdot 7, 56, 70, 84 = 6 \cdot 14.$$