CISC 1100: HW 5

SOLUTIONS

1) Find all of the inverses in the following $(mod\, n)$:
a) $(mod\, 11)$

$1^{-1} = 1, 2^{-1} = 6, 3^{-1} = 4, 5^{-1} = 9, 7^{-1} = 8, 10^{-1} = 10$

b) $(mod\, 13)$

$1^{-1} = 1, 2^{-1} = 7, 3^{-1} = 9, 4^{-1} = 10, 5^{-1} = 8, 6^{-1} = 11, 12^{-1} = 12$

c) $(mod\, 12)$

Only $1, 5, 7, 11$ are coprime to 12, so $1^{-1} = 1, 5^{-1} = 5, 7^{-1} = 7, 11^{-1} = 11$.

d) $(mod\, 8)$

Only $1, 3, 5, 7$ are coprime to 8, so $1^{-1} = 1, 3^{-1} = 3, 5^{-1} = 5, 7^{-1} = 7$.

e) What do you notice about the inverses $(mod\, 12), (mod\, 8)$? Guessing, what do you think this means about the elements with an inverse $(mod\, 12), (mod\, 8)$?

Both sets of inverses are the same size, and have the property that every element with an inverse is its own inverse. This suggests that multiplication in $(mod\, 8)$ and $(mod\, 12)$ behave quite similarly.

In fact, mod multiplication of invertible elements (elem. w/ inverses) forms what is called a "group," which is a fundamental structure to many branches of mathematics and CS. What we have shown is that there is actually no difference between the "groups" derived from $(mod\, 12), (mod\, 8)$.

2) Solve the following equations, if possible. If there are multiple solutions, list them. If not possible, explain.
a) $4x \equiv 5 (mod\, 7)$

$4^{-1} = 2$ here, so $x \equiv 2 \cdot 5 \equiv 3 (mod\, 7)$

b) $7x \equiv 9 (mod\, 11)$

From before, $7^{-1} = 8$ so $x \equiv 8 \cdot 9 \equiv 6 (mod\, 11)$

c) $2x \equiv 8 (mod\, 13)$

From before, $2^{-1} = 7$ so $x \equiv 7 \cdot 8 \equiv 4 (mod\, 13)$

d) $4x \equiv 5 (mod\, 12)$

Here, 4 has no inverse. It is valid to check all possible values for x to show that this has no solution. A wittier way to do this, however, is to note that $5^{-1} = 5$, so that $20x \equiv 1 (mod\, 12)$ i.e. $8x \equiv 1 (mod\, 12)$. If there were such an x, then 8 would have an inverse, which it does not. So there are no solutions.

e) $4x \equiv 4 (mod\, 8)$

Again 4 has no inverse, however it is obvious that $x = 1$ is a solution. Since we know that there is only a unique solution if we have an inverse, we know there has to be another option.

Again we may run through all of the options for x. A wittier way is to notice that if I multiply 4 by any even number, the result is divisible by $8 \equiv 0 (mod\, 8)$. So we need only check the odd numbers. On doing so one finds that in fact every odd number works. So $x = 1, 3, 5, 7$.

3) At a hotel, there are three international clocks behind the concierge. One is GMT (+0 hours), one is PST (-8 hours) and one is ET (-5 hours). If it is 6:04pm in New York City, what hour is the hour hand on the GMT clock and on the PST clock?

We don't care about the minute hand. The hours are $(mod\, 12)$. Let the hour hand in GMT be $x (mod\, 12)$. Then the hour hand in ET is $x - 5 (mod\, 12)$ and the hour hand in PST is $x - 8 (mod\, 12)$. Since NYC is ET, we know that $6 \equiv x - 5 (mod\, 12)$, so $x = 11$. Therefore the hour hand is on 11 on the GMT clock and on $11 - 8 = 3$ on the PST clock.

4) Solve this system of equations:

$$2x \equiv 5 (mod\, 9)$$

$$4x \equiv 5 (mod\, 7)$$

Hint: $9(-3) - 7(-4) = 1$

$2^{-1} = 5$ in $(mod\, 9)$ and we found x for the second equation in 2(a). Therefore this system is:

$$x \equiv 7(mod\, 9)$$
$$x \equiv 3(mod\, 7)$$

Consequently we have

$$x - 7 = 9k$$
$$x - 3 = 7q$$

Which on combining gives us

$$9k - 7q = -4$$

The hint tells us that $9(-3) - 7(-4) = 1$, which lets us skip the step of finding integer solutions. All we need to do is multiply both sides by -4:

$$-4[9(-3) - 7(-4)] = -4(1)$$
$$9(12) - 7(16) = -4$$

So $k = 12, q = 16$ will provide a solution. In either case we get $x = 115$. Plugging this in to the original problem confirms our answer.

5) There are two gears that work on one crank. The first gear has seven spokes and moves 4 spokes every crank. The second gear has nine spokes and moves 2 every crank. How many cranks will it take for both gears to be on the 5th spoke?

This problem is modeled by $2x \equiv 5(mod\, 9), 4x \equiv 5(mod\, 7)$. This is the system of equations just solved, so $x = 115$ will be an answer. If I were feeling cruel, I could have asked for the least number of cranks; this is the smallest positive integer equivalent to 115 mod 63, which is $x = 52$.