Homework 7: Problem 3

Jake Levin (jklevin)

Lachlan Kermode

1.

To solve this problem, first we will look to prove that x_s is an integer, and then prove that it is a solution of $ax = 1(\text{mod } m^s)$. To prove that x_s is an integer, we will start by factoring out $\frac{1}{a}$ and simplifying our given equation for x_s:

$$x_s = \frac{1}{a} - (\frac{1}{a})(1 - ax_1)^s$$

$$= \frac{1}{a}(1 - (1 - ax_1)^s)$$

Now looking at $(1 - ax_1)^s$ we know that as we expand this term out, each step of the expansion k will always take the form of $(1 + ...)(1 - ax_1)^{s-k}$. While it is difficult to solve for all the terms following the 1, we do know one key piece of information, and that is that they will always have a factor of a in them. Thus, we know that the $1 - 1$ in our equation will cancel out, and the remainder of our equation will be evenly divisible when multiplied by $\frac{1}{a}$, thus we know that x_s must be an integer.

Now we must prove that $x_s = \frac{1}{a}(1 - (1 - ax_1)^s)$ is a solution of $ax = 1(\text{mod } m^s)$. To do so we will first plug in our value for x_s into the congruence relation we are trying to show and simplify:

$$a \cdot \frac{1}{a}(1 - (1 - ax_1)^s = 1(modm^s)$$
$$= (1 - (1 - ax_1)^s = 1(modm^s)$$

What this tells us is that m^s divides $1 - (1 - a_x 1)^s - 1$. This can be simplified and written as:

$$m^s | - (1 - ax_1)^s$$

Which we know by the definition of congruence also implies that:

$$m^s | (ax_1 - 1)^s$$

The problem has stated that x_1 is a solution to the equation $ax = 1(modm)$, therefore we know that $m | (ax_1 - 1)$. This is all the information we need to complete our proof, since if $m | (ax_1 - 1)$ holds for one instance, then for each subsequent exponentiation of m and $(ax_1 - 1)$, m will always divide $(ax_1 - 1)$. Thus, we also know that m^s does indeed divide $(ax_1 - 1)^s$. Therefore by the definition of congruence we can say that for the given x_s, and given that $ax_1 = 1(mod m)$, x_s is an integer and is a solution of $ax = 1(mod m^s)$.

2.
To prove that $a^n = a(mod n)$ using induction on a, we will first show that $(a+b)^n = a^n + b^n(mod n)$ for any prime n, and the case where $b = 1$. The equality we hope to show true is:

$$(a+1)^n = a^n + 1^n(mod n)$$

To solve this, we will use the binomial theorem to expand $(a+1)^n$ as follows:

$$(a+1)^n = \sum_{k=0}^{n} \binom{n}{k} a^k$$

We will then split up this summation into the case where $k = 0$, where $k = n$, and the remaining cases. When $k = 0$ we know that $\binom{n}{0}a^0 = 1$, and when $k = n$, $\binom{n}{n}a^n = a^n$. We can now rewrite our expansion as:

$$(a+1)^n = a^n + 1 + \sum_{k=1}^{n-1} \binom{n}{k} a^k$$

We can compare this to the equality we hope to show which is, $(a+1)^n = a^n + 1(mod n)$ and realize that all that is left to prove to show this equality holds true is that n evenly divides $\sum_{k=1}^{n-1} \binom{n}{k} a^k$. To do so all we really need to show is that $n|\binom{n}{k}a^k$ for any $k > 0$, $k < n$ (because if each element in the sum is divisible by n, we know the final sum will be as well). To show that $n|\binom{n}{k}a^k$, we will expand out $\binom{n}{k}a^k$ as follows:

$$\binom{n}{k} a^k = \frac{n! a^k}{k!(n-k)!}$$

To show that this is divisible by n, we just have to prove that the numerator is divisible by n, but the denominator does not (otherwise they would just cancel out). We know trivially that because the numerator contains $n!$ that it is divisible by n. A little trickier is showing that $k!(n-k)!$ is not divisible by n, but this can be done by recognizing that because n is prime, and because k is less than n, then there cannot be any factor in $k!(n-k)!$ that equals n, and n has no other factors. Thus we have shown that $n|\binom{n}{k}a^k$, and therefore that

$$(a+1)^n = a^n + 1^n(mod n)$$

.

Having proven this equality, we can use induction on a to prove that $a^n = a(mod n)$. We start with the base case, $a = 0$:

$$0^n = 0(mod n)$$

This is trivially true. Now we will use the predicate $a^n = a(mod n)$ to show that $(a+1)^n = a+1(mod n)$. We start by recognizing that we are looking to show that $n|(a+1)^n - a - 1$. We will then use the equivalence formula we found in the first half of this problem, and rewrite this as:

$$n|a^n + 1^n - a - 1$$

$$= n|a^n - a$$

By the definition of congruence relationships, this can be written as $a^n = a(mod n)$. Since $a^n = a(mod n)$ is our predicate which we assume to be true, we have successfully shown that given our equation for a, our equation for $a+1$ holds true as well. Thus, by using induction on a we have shown that $a^n = a(mod n)$.