Math 522 Exam 10 Solutions

1. Find a primitive root g modulo $m = 18$, and construct a table of indices.
   BONUS: Use this table to solve the congruence $7x^{5^{1001}} \equiv 13 \pmod{18}$.

   A reduced residue system modulo 18 *is* $\{1, 5, 7, 11, 13, 17\}$*, so one need not look far for a primitive root. There will be* $\phi(\phi(18)) = 2$ *choices. The proof of the classification theorem yields 11: 2 is a primitive root mod 3,* $2^2 = 1 + 1 \cdot 3$ *so 2 is a primitive root mod 9, so* $2 + 9 = 11$ *is a primitive root mod 18. Or, you could try the process of elimination:* $7^3 \equiv 13^3 \equiv 1, 17^2 \equiv 1$*, so the only possible choices are 11 and 5.*

   $g = 11$*:*

	1	5	7	11	13	17
	6	5	4	1	$\boxed{2}$	3

   $g = 5$:

	1	5	7	11	13	17
	6	1	2	5	4	3

   For example, the $\boxed{2}$ *entry means that* $11^2 \equiv 13 \pmod{18}$*.*

   BONUS: Using the index 11*, ind* $7x^{5^{1001}} \equiv ind\ 13 \pmod{6}$*. We also have ind* $7x^{5^{1001}} \equiv ind\ 7 + 5^{1001} ind\ x \equiv 4 + (-1)^{1001} ind\ x \equiv 4 - ind\ x \pmod{6}$*. Hence* $4 - ind\ x \equiv 2 \pmod{6}$*, and so ind* $x \equiv 2 \pmod{6}$*. So the (unique modulo 18) solution is* $x = 13$*.*

2. Find a primitive root modulo 250, and prove that it is primitive.

   $250 = 2 \cdot 5^3$*. Following the proof of the classification theorem, we first need a primitive root modulo 5. Either 2 or 3 will work (there are* $\phi(\phi(5)) = 2$ *to choose from).* $2^4 = 1 + 3 \cdot 5, 3^4 = 1 + 16 \cdot 5$*, so by the lemma they are both primitive roots modulo 125. Finally,* $2 + 125$ *is odd, and* 3 *is odd, so the theorem gives both* 127 *and* 3*.*

   To prove they are primitive roots, one way is to mimic the proof of the last part of the classification theorem. 3 is primitive modulo 5, so by the lemma it is primitive modulo 125. Suppose $3^h \equiv 1 \pmod{250}$*, for some* $h < 100$*. Then* $3^h \equiv 1 \pmod{125}$*, but then* 3 *wouldn't be primitive modulo 125.*

   Here is an alternative, direct, way to prove that 3 *is primitive.* $\phi(250) = 100$*, so we want to prove that* 3 *belongs to the exponent* 100*. Certainly* $3^{100} \equiv 1 \pmod{250}$*, since* $gcd(3, 250) = 1$*; the only question is whether this holds for any smaller exponent. We need only try divisors of* 100*, hence* $2, 4, 5, 10, 20, 25, 50$*. It goes pretty fast, since it's quick to calculate mod 250 – take the last three digits mod 250.* $3^1 \equiv 3, 3^2 \equiv 9, 3^4 \equiv 81, 3^5 \equiv 243, 3^{10} = 59049 \equiv 49, 3^{20} = (3^{10})^2 \equiv 49^2 = 2401 \equiv 151, 3^{25} = 3^{20}3^5 \equiv 151 \cdot 243 = 36693 \equiv 193, 3^{50} = 3^{25}3^{25} \equiv 193 \cdot 193 = 37249 \equiv 249 \equiv -1$*.*

3. Exam grades: 104, 102, 91, 89, 88, 86, 86, 86, 80, 79, 78, 75, 75, 55