Math 345 – Monday 10/30/17

Exercise 32. Find one solution to the following congruences. Make a careful and detailed list of each of your steps. You may use a computer to do any of the intermediate computations.

(a) $x^{329} \equiv 452 \pmod{1147}$

(b) $x^{275} \equiv 139 \pmod{588}$

[Careful: 1147 and 588 aren't prime.]

Exercise 33. In Chapter 17, we described how to compute one kth root of b modulo n, but there may be other solutions. For example, if $a^2 \equiv_n b$, then we also have $(-a)^2 \equiv_n b$.

(a) Let b, k, and n be integers that satisfy

$$\gcd(b, n) = 1 \qquad \text{and} \qquad \gcd(k, \phi(n)) = 1.$$

Show that b has exactly one kth root modulo n.

[Hint: You know there's *at least* one, so you just have to show there isn't *more than* one. So start by supposing a and a' are both kth roots of b modulo n, i.e. $a^k \equiv_n b$ and $(a')^k \equiv_n b$. Now use the tools for finding solutions from class to show that $a \equiv_n a'$.]

(b) Why doesn't part (a) contradict our example above? Namely why doesn't the fact that there is more than one solution to $a^2 \equiv_n b$ for most n and b provide a counterexample to part (a)?

(c) Look at some examples were n is prime and try to find a formula for the number of kth roots of b modulo n (assuming that it has at least one). (Don't try to prove your formula.)

[Try setting $n = 3, 5,$ and 7 and use a computer to compute $a^k \pmod{n}$ for $a = 2, 3, \dots, n-1$ and $k = 1, 2, \dots, n-1$. If you need more data, do more prime n's.]

(d) BONUS. *If you have taken abstract algebra*, the following is possible to show: Suppose that $\gcd(k, \phi(n)) > 1$. Then either b has no kth roots modulo n, or else it has at least two kth roots modulo n. [Hint: Consider the group of units of $\mathbb{Z}/n\mathbb{Z}$.]

Exercise 34. Our method for solving $x^k \equiv_n b$ is first to find positive integers u and v satisfying $ku - \phi(n)v = 1$, and then the solution is $x \equiv_n bu$. However, we only showed that this works provided that $\gcd(b, m) = 1$, since we used Eulers formula $b^{\phi(n)} \equiv_n 1$.

(a) If n is a product of distinct primes, show that $x \equiv_n b^u$ (with u as above) is always a solution $x \equiv_n bu$, even if $\gcd(b, n) > 1$.

[Hint: Check that n divides $(b^u)^k - b$ by checking that each prime divisor of n divides $(b^u)^k - b$. To do that, if $p|n$, then break into cases where $p|b$ or $p \nmid b$. If $p|b$, what can you conclude? If $p \nmid b$, check that $p-1|\phi(n)$, and then plug that information into "$ku = \phi(n)v+1$", and compute $(b^u)^k \pmod{p}$ using Fermat.]

(b) Show that our method does not work for the congruence $x^5 \equiv 6 \pmod{9}$ (by finding u and plugging in).