Worksheet 12: Order, Primitive Roots, Review

Problem 1. Suppose $\gcd(a, n) = 1$ and that a has order k modulo n.

(a) Show that $a^m \equiv 1 \bmod n$ if and only if $k \mid m$.

(b) Show that, if $a^x \equiv a^y \bmod n$ for some integers x and y, then $x \equiv y \bmod k$.

Problem 2. Suppose $\gcd(a, n) = 1$ and the order of a mod n is k. Let h be a positive integer. Show that the order of a^h mod n is $k/\gcd(h, k)$.

Problem 3. (a) Verify that 2 is a primitive root modulo 11. *Note.* Do this efficiently using Euler's theorem and problem 1(a).

(b) Find all of the other primitive roots modulo 11. *Note.* Do this efficiently using problem 2.

Problem 4. Let p be a prime. How many (congruence classes of) primitive roots are there modulo p?

Problem 5. Suppose a is a primitive root modulo p for an odd prime p. Show that $a^{(p-1)/2} \equiv -1 \bmod p$. *Hint.* Use problem 2.

Problem 6. Find a number a such that $a^{19} \equiv 50 \bmod 137$. *Note.* Use Sage? Problem 1(b) might also be helpful.

Problem 7. Find a solution to the following system of congruences.

$$2x \equiv 1 \bmod 5$$
$$5x \equiv 9 \bmod 11$$

Problem 8. Find the last two digits of $7^{4{,}000{,}000{,}000{,}000}$.

Problem 9. Suppose $\gcd(a, 30) = 1$. Show that 60 divides $a^4 - 1$.

Problem 10. Show that $13 \mid 11^{12n+6} + 1$ for all non-negative integers n.