Math 565, Problem Set 2: *due Wednesday, January 17*

1. Suppose that $g^a \equiv 1 \pmod{m}$ and that $g^b \equiv 1 \pmod{m}$. Prove that
$$g^{\gcd(a,b)} \equiv 1 \pmod{m}.$$

2. Let $m \in \mathbb{Z}$.
   i) Suppose that m is odd. What integer between 1 and $m-1$ equals $2^{-1} \bmod m$?
   ii) More generally, suppose that $m \equiv 1 \pmod{b}$. What integer between 1 and $m-1$ is equal to $b^{-1} \bmod m$?

3. i) Find a single value x that simultaneously solves the two congruences
$$x \equiv 3 \pmod{7} \quad \text{and} \quad x \equiv 4 \pmod{9}.$$
   [Hint: Note that every solution of the first congruence looks like $x = 3 + 7y$ for some y. Substitute this into the second congruence and solve for y; then use that to get x.]
   ii) Find a single value x that simultaneously solves the two congruences
$$x \equiv 13 \pmod{71} \quad \text{and} \quad x \equiv 41 \pmod{97}.$$
   iii) Find a single value x that simultaneously solves the three congruences
$$x \equiv 4 \pmod{7} \quad \text{and} \quad x \equiv 5 \pmod{8} \quad \text{and} \quad x \equiv 11 \pmod{15}.$$
   iv) Prove that if $\gcd(m,n) = 1$, then the pair of congruences
$$x \equiv a \pmod{m} \quad \text{and} \quad x \equiv b \pmod{n}$$
   has a solution for any choice of a and b. Also give an example to show that the condition $\gcd(m,n) = 1$ is necessary.

4. Let p be a prime and let q be a prime that divides $p-1$.
   i) Let $a \in \mathbb{F}_p^*$ and let $b = a^{(p-1)/q}$. Prove that either $b = 1$ or else b has order q in $\mathbb{F}_p^*$.

ii) Suppose that we want to find an element of $\mathbb{F}_p^*$ of order q. Using i), we can randomly choose a value of $a \in \mathbb{F}_p^*$ and check whether $b = a^{(p-1)/q}$ satisfies $b \neq 1$. How likely are we to succeed? In other words, compute the value of the ratio

$$\frac{\#\{a \in \mathbb{F}_p^* : a^{(p-1)/q} \neq 1\}}{\#\mathbb{F}_p^*}.$$

[Hint: use the Primitive Root Theorem.]

5. Let p be a prime such that $q = \frac{1}{2}(p-1)$ is also prime. Suppose that g is an integer satisfying

$$g \not\equiv \pm 1 \pmod{p} \quad \text{and} \quad g^q \not\equiv 1 \pmod{p}.$$

Prove that g is a primitive root modulo p.