Math 1580 – Problem Set 1. Due Friday Sep. 16, 4pm

(1) (Problem 1.9, 1.10, parts (a) and (c)) Use the Euclidean algorithm (Theorem 1.7) to compute $\gcd(a, b)$ for the values below, and then use the extended Euclidean algorithm (Theorem 1.11) to find integers u and v such that $au+bv = \gcd(a, b)$. (Feel free to use a calculator to do the division step.)
   (a) $a = 291$, $b = 252$.
   (b) $a = 139024789$, $b = 93278890$.

(2) (Problem 1.14, Proof of Proposition 1.13(a)) Let $m \geq 1$ be an integer and suppose that

$$a_1 \equiv a_2 \pmod{m} \quad \text{and} \quad b_1 \equiv b_2 \pmod{m}.$$

Prove that

$$a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod{m} \quad \text{and} \quad a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{m}.$$

(3) (Problem 1.15) Write out the following tables for $\mathbb{Z}/m\mathbb{Z}$ and $(\mathbb{Z}/m\mathbb{Z})^*$.
   (a) Addition and multiplication tables for $\mathbb{Z}/3\mathbb{Z}$.
   (b) Addition and multiplication tables for $\mathbb{Z}/6\mathbb{Z}$.
   (c) Multiplication table for $(\mathbb{Z}/9\mathbb{Z})^*$.
   (d) Multiplication table for $(\mathbb{Z}/16\mathbb{Z})^*$.

(4) (Problem 1.18) Suppose that $g^a \equiv 1 \pmod{m}$ and $g^b \equiv 1 \pmod{m}$. Prove that

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

(5) (Problem 1.23 parts (a) and (d))
   (a) 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 to 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.)
   (b) 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.

(6) (Problem 1.25 parts (a) and (c)) Use the square-and-multiply algorithm described in Section 1.3.2 to compute the following powers
   (a) $17^{183} \pmod{256}$.
   (b) $11^{507} \pmod{1237}$.

(7) (Problem 1.26) Let $\{p_1, \ldots, p_r\}$ be a set of prime numbers, and let

$$N = p_1 p_2 \cdots p_r + 1.$$

Prove that N is divisible by some prime not in the original set. Use this fact to deduce that there must be infinitely many prime numbers. (This proof of the infinitude of primes appears in Euclid's *Elements.* Prime numbers have been studied for thousands of years.)