Math 255 - Spring 2018
Homework 7

This homework is due on Monday, March 5.

1. (a) Let a, b and m be integers with $m > 0$. Prove or disprove that if $a \equiv b \pmod{m}$, then $a^2 \equiv b^2 \pmod{m}$.
   (b) Let a, b and m be integers with $m > 0$. Prove or disprove that if $a^2 \equiv b^2 \pmod{m}$, then $a \equiv b \pmod{m}$ or $a \equiv -b \pmod{m}$.
2. Find all integers $m > 1$ such that $1848 \equiv 1914 \pmod{m}$.
3. Show that the difference of two consecutive cubes is never divisible by 5.
4. Let n be an integer. Show that if $n \equiv 4 \pmod{9}$ then n cannot be written as the sum of two cubes.
5. (a) Please give a multiplication table for the ring $\mathbb{Z}/12\mathbb{Z}$.
   (b) List all units in the ring $\mathbb{Z}/12\mathbb{Z}$.
   (c) List all zero divisors in the ring $\mathbb{Z}/12\mathbb{Z}$.
6. (a) It is a fact that $(7, 23) = 1$. Give an integer solution to the equation $7x + 23y = 1$.
   (b) It is also a fact that the equivalence class of 7 in $\mathbb{Z}/23\mathbb{Z}$ is a unit. Please give any representative for the class that is its multiplicative inverse. In other words, please give any integer v such that

$$7v \equiv 1 \pmod{23}.$$

   Hint: Consider part (a), and in particular the whole equation modulo 23.

Extra problem for graduate credit:

7. Let k, m and x be integers. Show that for $k > 0$ and $m \geq 1$, $x \equiv 1 \pmod{m^k}$ implies that $x^m \equiv 1 \pmod{m^{k+1}}$.