Discrete Structures. CSCI-150. Fall 2014.

Homework 9. Due Wed. Nov 5, 2014.

Important announcement:
If you can, try to finish this homework by Monday (November, 3). Then I will grade it and give it back to you on Wednesday, so you get it graded before the midterm.

Problem 1

For $a, b \in \mathbb{Z}$, prove that if $a \mid b$ and $b \mid a$ then $a = b$ or $a = -b$.

Problem 2 (Graded)

First, prove that $k(k+1)$ is even for any $k \in \mathbb{Z}$.

Then, for positive $n \in \mathbb{Z}$, prove that if n is odd then $8 \mid (n^2 - 1)$.

Hint: An integer x is even if and only if $2 \mid x$.

Problem 3 (Graded)

Decide whether each of these integers is congruent to 3 modulo 7.

(a) 37

(b) 66

(c) -17

(d) -67

Problem 4 (Graded)

In this problem, <u>don't use a calculator</u>. The answers can be derived without doing much computation, try to find these simple solutions.

Prove or disprove:

(a) $4 + 5 + 6 \equiv 0 \pmod{5}$

(b) $55 + 56 + 7 \equiv 3 \pmod{5}$

(c) $1004 + 2005 + 3006 \equiv 0 \pmod{5}$

(d) $15 + 111^5 \cdot (-10) \equiv 5 \pmod{11}$

(e) $1112 \cdot 2224 \cdot 4448 + 2221 \equiv 7 \pmod{1111}$

(f) $20 \cdot 10 \cdot (-10) \cdot (-20) \equiv 13000000000 \pmod{9}$

Problem 5 (Graded)

(a) What is the definition of relative primes (co-primes)?

(b) Use Euclid's algorithm to prove that 287 and 120 are relative primes. (Write out all the steps of the algorithm).

(c) Since they are relative primes, there exist Bezout coefficients x and y such that

$$287 \cdot x + 120 \cdot y = 1.$$

These coefficients are $x = 23$ and $y = -55$. Now, your task is to find a miltiplicative inverse of 287 modulo 120, and a multiplicative inverse of 120 modulo 287. Prove that they are multiplicative inverses.

Problem 6

Prove that for all positive $n \in \mathbb{Z}$:

$$3 \mid (n^3 + 2n).$$

It can be done either <u>by induction</u>, or <u>by cases</u>.

The proof by induction is standard. If you decide to prove it by cases, consider the remainder (n **rem** 3), it can be equal to 0, 1, or 2, so we can say that for any n: $n = 3k$, or $n = 3k + 1$, or $n = 3k + 2$.