Discrete Structures. CSCI-150. Spring 2016.

Homework 8. Due Wed. Apr. 6, 2016.

Problem 1

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

(a) 38, (b) 66, (c) 67, (d) -3, (e) -17, (f) -18.

Problem 2 (Graded)

In this problem, don't use a calculator. 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 3

Given the following recurrently defined sequence of integers:

$$a_0 = 3,$$
$$a_n = 5a_{n-1} + 8$$

Prove by induction that all elements in this sequence are congruent to 3 modulo 4, or in other words:

$$\forall n \geq 0 : \qquad a_n \equiv 3 \pmod{4}$$

Problem 4 (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 5 (Graded)

We want to prove that 119 has infinitely many multiplicative inverses modulo 198.

(a) Prove that such a multiplicative inverse exists.

(b) Verify that 5 is one of them.

(c) Prove that there are infinitely many inverses. Hint: Consider the number $(5 + n \cdot 198)$

(d) **Generalize the statement:** Try to prove that for any two positive integers a and b that are relative primes, there are infinitely many multiplicative inverses of a modulo b.

Problem 6 (Graded)

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

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

It can be done either by induction, or by cases.

The proof by induction would be 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 $n = 3k + 2$.

In either case, it can be useful to employ modular arithmetic in your proof, because for example, to prove that $3 \mid (n^3 + 2n)$, you, in fact, have to show that $n^3 + 2n \equiv 0 \pmod{3}$.

Problem 7

Find the GCD of two numbers, if you know their prime factorizations:

$$2^5 \cdot 3^9 \cdot 5^{16} \cdot 11 \qquad \text{and} \qquad 2^2 \cdot 3 \cdot 5^{11} \cdot 7 \cdot 11^2 \cdot 13$$

(There is no need to do Euclid's algorithm here)