Discrete Structures. CSCI-150. Spring 2017.

Homework 8. Due Mon. Apr. 3, 2017.

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) $99 + 888 + 44 \cdot 51^{100} = 1 \pmod{10}$

(b) $1 + 2 + 3 + \ldots + 50 \equiv -5 \pmod{10}$

(c) $1 + 3 + 5 + 7 + \ldots + 9999999 \equiv 0 \pmod{5}$

(d) $3333 + 4444 + 5555 + 6666 \equiv 7788 \pmod{1110}$

(e) $33330 \cdot 44440 + 55550 \cdot 66660 \equiv 870 \pmod{1110}$

(f) $3^1 + 3^2 + 3^3 + \cdots + 3^{999} \equiv -1 \pmod{20}$

(g) $42^{1024} \cdot 27^{2048} \equiv 3 \pmod{39}$

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)

Given two numbers,

$$a_0 = 172, \quad a_1 = 61,$$

write out the execution of the extended Euclidean algorithm. Find $a_k = \gcd(a_0, a_1)$ and Bezout's coefficients x_k and y_k, i.e. the numbers such that the following equation is satisfied:

$$x_k a_0 + y_k a_1 = \gcd(a_0, a_1)$$

If the multiplicative inverse of a_1 modulo a_0 exists, find such a number and show why it is a multiplicative inverse. Otherwise, prove that it does not exist.

Problem 5

Repeat the task from the previous problem for numbers

$$a_0 = 800, \quad a_1 = 33.$$

Problem 6 (Graded)

Prove the following statements:

(a) if a is odd then $a^4 \equiv 1 \pmod{4}$,

(b) if 5 does not divide a, then $a^4 \equiv 1 \pmod{5}$.

Problem 7 (Graded)

Prove that if x is a multiplicative inverse of a modulo n, that is

$$x \cdot a \equiv 1 \pmod{n},$$

then $x + n$ is also a multiplicative inverse.

Then, prove that there are infinitely many multiplicative inverses of a modulo n.

Problem 8

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)