Discrete Structures. CSCI-150. Summer 2016.

Homework 8. Due Tue. Jul. 5, 2016.

Problem 1

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

(a) 10, (b) -3, (c) 37, (d) 66, (e) -17, (f) -67.

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) $255 + 156 \cdot 7 \equiv 2 \pmod 5$

(c) $1234 + 2345 + 3456 \equiv 0 \pmod 5$

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

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

(f) $2^{12345} \equiv 32 \pmod 6$

Problem 3

Given the following recurrently defined sequence of integers:

$$\begin{aligned} a_0 &= 3, \\ a_n &= 5a_{n-1} + 8 \end{aligned}$$

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,

$$a_0 = 191, \quad a_1 = 125,$$

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

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)