Problem Set 5

Due on Monday, November 2, 2015.

Problem 1: Zero divisors

An element \( a \in \mathbb{Z}_n - \{0\} \) is said to be a zero divisor modulo \( n \) if \( ab \equiv 0 \pmod{n} \) for some \( b \in \mathbb{Z}_n - \{0\} \).

(a) Explain why there are no zero divisors in \( \mathbb{Z}_p \) when \( p \) is prime.

(b) Find a zero divisor in \( \mathbb{Z}_{35} \).

(c) What is the value of the first element to repeat in the sequence

\[
(3^1 \mod 35), (3^2 \mod 35), (3^3 \mod 35), (3^4 \mod 35), \ldots
\]

In all cases, justify your answers.

Problem 2: Greatest common divisor

The definition of greatest common divisor can be extended naturally to a sequence of numbers \((a_1, a_2, \ldots, a_k)\), not all of which are zero; namely, it is the largest integer \( d \geq 1 \) such that \( d \mid a_j \) for all \( j = 1, 2, \ldots, k \). Describe an efficient algorithm for computing gcd\((a_1, \ldots, a_k)\), and explain why it computes the correct answer.

Problem 3: Euler’s totient function

Compute \( \phi(3500) \). Show your work.

Problem 4: Euler theorem

Compute \( 3^{907211} \mod 3500 \).

Problem 5: Extended Euclidean algorithm

Use the extended Euclidean algorithm to solve the Diophantine equation \( 601x - 714y = 1 \). Show the resulting table of triples as in slide 15 of lecture 13 notes.

[Note: You may write a program to produce the table if you wish, but these numbers are small enough to make it quite feasible to carry out the computation by hand or with the aid of a pocket calculator.]
Problem 6: Primitive roots

(a) Find a primitive root $g$ of $p = 751$ and use the Lucas test to prove that you have one. (See lecture 14 notes.)

(b) Find a non-trivial\(^1\) number $g \in \mathbb{Z}_{751}^*$ that fails to be a primitive root of $p$, and use the Lucas test to prove your answer correct.

You may write a program to perform the arithmetic calculations involved in applying the Lucas test.

\(^1\)Non-trivial means $g \not\in \{1, p - 1\}$. 