

## Problem Set 3

Due on Wednesday, February 15, 2012.

### Part A. Written problems

#### Problem 1: Zero divisors

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

- (a) Explain why there are no zero divisors in  $\mathbf{Z}_p$  when  $p$  is prime.
- (b) Find a zero divisor in  $\mathbf{Z}_{39}$ .
- (c) What is the value of the first element to repeat in the sequence

$$(5^1 \bmod 39), (5^2 \bmod 39), (5^3 \bmod 39), (5^4 \bmod 39), \dots?$$

- (d) Do you think it is possible to find a non-zero number  $x \in \mathbf{Z}_{39}$  and a number  $k \geq 0$  such that  $x^k \equiv 0 \pmod{39}$ ? Why or why not? Would your answer change for some RSA modulus  $n$  other than 39?
- (e) Suppose  $n$  is not required to be an RSA modulus. Can you find numbers  $n, x, k$  such that  $x \not\equiv 0$  but  $x^k \equiv 0 \pmod{n}$ ?

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  $(a_1, a_2, \dots, a_k)$ , not all of which are zero; namely, it is the largest integer  $d \geq 1$  such that  $d \mid a_j$  for all  $j = 1, 2, \dots, k$ . Describe an efficient algorithm for computing  $\gcd(a_1, \dots, a_k)$ , and explain why it computes the correct answer.

#### Problem 3: Euler's totient function

Compute  $\phi(2200)$ . Show your work.

#### Problem 4: Euler theorem

Compute  $2^{591207} \bmod 2200$ .

**Problem 5: Extended Euclidean algorithm**

Use the extended Euclidean algorithm to solve the Diophantine equation

$$539x - 1387y = 1$$

Show the resulting table of triples as in slide 34 of lecture 8 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.]

**Part B. Programming problem****Problem 6: Factoring the RSA modulus knowing the public and private keys**

Bob's public RSA key is  $n = 1501$ ,  $e = 323$ . Eve manages to learn that his decryption key is  $d = 539$ . Implement the randomized factoring algorithm shown on slide 49 of lecture 9 notes. Use your program to factor  $n$ . Once you have the factorization of  $n$ , compute  $\phi(n)$ , and check your answer by verifying that  $ed \equiv 1 \pmod{\phi(n)}$ .