Handout 19 Introduction to Communication Systems
Homework 10 November 26, 2009

This is your third graded homework. Please consider the following rules:

- **You have two weeks to hand in your solution.**
- **Each problem should be answered in one piece of paper, otherwise your answers will not be graded.**
- **Your name and number should be written on each piece of paper.**

PROBLEM 1. For the following statements, decide whether or not it is correct. Justify your answer with a short proof for true statements and with a counterexample for false ones.

a) If a and b are two integer numbers and each of them is divisible by the other, then $a = b$.

b) If $a^2 \equiv 1 \pmod{12}$ then $a \equiv 1$ or $(-1) \pmod{12}$

c) If $a \equiv b \pmod m$ and $c \equiv d \pmod m$ then $a.c \equiv b.d \pmod m$

d) If $a^n - 1$ is a prime number then $a = 2$ and n is also a prime number.

e) For every positive integer m, $m^2 + m + 41$ is always a prime number.

PROBLEM 2. Show that the summation of all the positive integer numbers smaller than 2009 which are co-prime with respect to 2009, is divisible by 2009.

PROBLEM 3. Consider an RSA cryptosystem in which every letter of the plaintext is encoded by its alphabetic position + 9. For example a is encoded as 10, b is encoded as 11 and z is encoded as 35. (We only consider lower-case letters) Suppose that $m = 71$ and $K = 3$.

a) Encrypt the plaintext "epfl"

b) Using the public key K, find the private key k.

c) Decrypt the ciphertext 16-13-6

PROBLEM 4. Find three consecutive integer numbers $n, n + 1, n + 2$ so that n is divisible by 11, $n + 1$ is divisible by 10 and $n + 2$ is divisible by 9.

PROBLEM 5. Suppose that a, b and n are positive integer numbers.

a) Show that if n is an odd number then $a^n + b^n$ is divisible by $a + b$.

b) Show that if $n = 4k + 2$ then $a^n + b^n$ is divisible by $a^2 + b^2$

c) Suppose that $p = 4k + 3$ is an odd prime number. Use the previous parts to show that if $a^2 + b^2$ is divisible by p then both a and b must be divisible by p. (Hint: Use the fact that if a is not divisible by p then $a^{p-1} \equiv 1 \pmod p$.)