ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

School of Computer and Communication Sciences

Handout 17 Introduction to Communication Systems

Homework 10 November 20, 2008

Problem 1 (Congruences). 1. If $a \equiv a'$ (mod m), show that for any integer t

$$at \equiv a't \text{ (mod} m).$$

2. If $ad \equiv a'd$ (mod m) and d and m are relatively prime, show that

$$a \equiv a' \text{ (mod} m).$$

Does this property still hold if d and m are not relatively prime ?

Problem 2 (Euler's Birthday Party). Euler invites a group of n friends to celebrate his 251-st birthday. He has ordered a humongous Nusstorte from Spruengli. The cake is already been cut into 5005 pieces. Euler asks his n friends to split into subgroups of equal size. Amazingly, each group gets exactly the same number of pieces. How many possible choices of n are there?

Problem 3 (A trip to China Town). (i) Four friends go to eat dim sum at a restaurant. They order k pieces. After dividing equally they are left with 3 pieces. Since the food was delicious, the next evening they take along one additional friend and order again k pieces. Dividing again fairly, they are left with 2 pieces. One piece costs 5 CHF and a single piece per person is not enough. What is the minimum amount of money they paid ?

(ii) Assume exactly the same situation as above except that on the second evening they take along two additional friends.

Problem 4 (RSA Encryption). In this problem we perform RSA encryption and decryption. Assume that each letter of the English alphabet is represented by its position, i.e. $A = 1, B = 2, \ldots$. For the RSA scheme, we encode using integers modulo 33. Thus $m = 11 \cdot 3$.

- Compute the public key, secret key pair (K, k).
- Pair up with the person next to you. Encrypt the plaintext $CIPHER$. Ask your neighbor to decrypt.