ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
School of Computer and Communication Sciences

Handout 18 Introduction to Communication Systems
Solutions to Homework 10 December 4, 2008

PROBLEM 1. 1. Since $a \equiv a' \pmod{m}$, it implies that $a - a' = km$ for some integer k. Thus multiplying both sides by t we get

$$at - a't = (kt)m$$

which implies that $at \equiv a' \pmod{m}$.

2. We are given that $ad \equiv a'd \pmod{m}$ and $\gcd(d, m) = 1$. From the given information we have

$$d(a - a') = mk$$

for some integer k. Dividing both sides of the above equation by d we get

$$(a - a') = \frac{mk}{d}$$

Since $\gcd(d, m) = 1$ and $a - a'$ is an integer, we must have that d divides k. Let $k = jd$ for some integer j. Thus we have

$$(a - a') = mj$$

which implies that $a \equiv a' \pmod{m}$.

PROBLEM 2. Note that in this problem we assume that we do not divide the pieces into further smaller pieces. Let the size of each subgroup be m. Then $n = dm$ for some d. Thus there are d number of subgroups each of size m. If each group got exactly the same number of pieces, it means that $5005 = dk$ for some integer k. Thus 5005 and n must have a common divisor greater than 1.

We know that the total number of integers smaller than 5005 which are coprime to 5005 is given by $\phi(5005)$. All the remaining integers have a common factor greater than 1 with n, thus the total number of choices for n is $5005 - \phi(5005)$=2125.

PROBLEM 3. In this problem we formulate congruence equations and then solve them using the Chinese Remainder theorem.

1. After equally dividing k dimsums amongst 4 friends we have 3 dimsums remaining, this means that the remainder of k on division by 4 is 3. Thus we have the first congruence equation:

$$k \equiv 3 \pmod{4}$$

On the next day, k pieces are equally divided amongst 5 friends and 2 pieces remain. This implies that

$$k \equiv 2 \pmod{5}$$

Thus we have to solve the following set of congruences:

$$k \equiv 3 \pmod{4}$$
$$k \equiv 2 \pmod{5}$$

This can be solved by the Chinese Remainder theorem to get $k = 27$. $k = 7$ is not a solution since we will get one piece per person. Thus money $= 27 \times 5 = 135$CHF.

2. We can argue similar to the first part. In this case we must solve:

$$k \equiv 3 \pmod 4$$
$$k \equiv 2 \pmod 6$$

This implies

$$k = 4a + 3$$
$$k = 6b + 2$$

for some integers a, b. Which implies that $6b + 2 = 4a + 3$, which is not possible for any $a, b \in \mathbb{Z}$ because $6b + 2$ is 0 modulo 2 and $4a + 3$ is 1 modulo 2. Thus in the second scenario, they pay nothing because they can not satisfy both the congruences.

PROBLEM 4. 1. We choose K such that $\gcd(K, \phi(m)) = 1$. Here $\phi(m) = \phi(11 \cdot 3) = (11 - 1)(3 - 1) = 20$. One choice for K is $K = 7$. It satisfies $\gcd(K, m) = 1$. With this choice of K, we choose k such that

$$Kk \equiv 1 \pmod{\phi(m)}.$$

We can easily calculate the inverse of K using the extended Euclid algorithm and the Bezout's identity to yield $k = 3$. It is easy to check that $3 \times 7 = 21 \equiv 1 \pmod{20}$. Thus we have $(K, k) = (7, 3)$.