CSCI2110 Discrete Mathematics **Last Updated:** October 11, 2010
Homework 2 **Due Date: 22-Oct-2010 17:00 sharp**

This homework contains 20 points. You are encouraged to collaborate on the homework, but you must write your own solutions and list your collaborators on your solution sheet (you will not lose any mark by doing this). Please drop your submissions into the dropbox near SHB 924.

Problem 1 (4 pts). You plan to buy a new handset that worths $\$6,000$. The loan officer offers you the following deal.

$2000 at the start of each month for three months to pay for the handset, and an option of choosing one of the following repayment plans:

1. Repay $500 at the start of each month for the next 11 months.
2. Repay $400 at the start of each month for the next 16 months.

Assume the monthly interest rate is 8%.

(a) (2 pts.) Which plan is a better option so that the loan profit made by the officer is minimized? Show your steps clearly.

Now you have chosen the better plan and have repaid the loan for half year. Before you make the next payment the loan officer contacted you and offer you another plan to repay the loan:

3. Repay $450 at the start of each month for the next 6 months.

You can switch your current plan to this plan, while you must pay for $900 as administrative fee.

(b) (2 pts.) Is it better to switch the plan? Please explain.

Problem 2 (4 pts).

(a) (1 pt.) Prove that for any integer p, there exists an integer k such that $6p+5$ can be written as $3k-1$. Prove or disprove whether the converse holds.

(b) (3 pts.) Prove the followings:

(i) (1 pts.) Show that if a and b are positive integers, then

$$(2^a - 1) \bmod (2^b - 1) = 2^{a \bmod b} - 1.$$

(Hint: Use long division.)

(ii) (2 pts.) Hence show that $2^a - 1$ and $2^b - 1$ are relatively prime if and only if $\gcd(a, b) = 1$.

Problem 3 (4 pts).

(a) (2 pts.) Prove the followings:

(i) (1 pt.) Prove that $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ is divisible by 3 and 5 for every integer n. *(Hint: Use Fermat's Little Theorem.)*

(ii) (1 pt.) Hence prove that $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ is an integer for every integer n.

In lectures you have learned how to test if an integer N is divisible by $K = 9$. This time you are going to prove the rules for $K = 7$ and $K = 13$.

(b) (2 pts.) You may have noticed that a hint "$1000 \equiv -1 \pmod 7$" appears in lecture notes. In fact there is a similar method to test divisibility of $K = 7$ to that of $K = 11$. Describe such method and prove that the condition(s) is(are) sufficient and necessary. *(Hint: A very similar test works for $K = 13$.)*

Problem 4 (4 pts). Joe claims himself to have discovered a perfect check digit scheme for 10-digit student ID. The scheme starts by adding all odd-positioned numbers, denoted by X. Then let Y be the sum of all even-positioned numbers. Let R be the remainder of $3X + Y$ divided by 10. The check digit D will be such that $D = 10 - R$.

(a) (2 pts.) Determine exactly when it can be used to detect single digit error. Prove your answer.

(b) (2 pts.) Determine exactly when it can be used to detect single transposition error. Prove your answer.

Problem 5 (4 pts). N people are going to rent for a safe deposit box in a bank. They put in their money into this single box. For security reasons, the password M is not disclosed to anybody, while each of the N people is given a pair of integers (R_i, K_i) such that $M \bmod K_i = R_i$. They are told that K_i and K_j do not have common factors greater than 1 for $i \neq j$. They are also told that $M < K_1 K_2 \cdots K_N$. The box adopts single trial policy, meaning that it will not be opened forever once the wrong password is entered. It implies that it is infeasible to try the passwords ranging from 0 to $K_1 K_2 \cdots K_N - 1$ multiple times.

(a) (3 pts.) Let $N = 3$. The table below shows three pairs of integers they have on their hands:

Person	(R_i, K_i)
1	$(175, 383)$
2	$(239, 457)$
3	$(350, 521)$

How to recover the password M? Show your steps clearly.

(b) (1 pt.) In general for every positive integer N, the password M can always be recovered if $(R_1, K_1), \cdots (R_N, K_N)$ are all present. Furthermore it is very secure in the sense that any $N-1$ of them cannot steal the remaining person's money without the missing pair of integers (R_i, K_i) he holds. Consider the case when $N = 3$ along with the table below:

Person	(R_i, K_i)
1	$(3, 17)$
2	$(10, 16)$
3	$(0, 15)$

Verify that any two of them cannot uniquely determine the password.