Assignment 5.

This homework is due *Thursday* Feb 23.

There are total 42 points in this assignment. 37 points is considered 100%. If you go over 37 points, you will get over 100% for this homework and it will count towards your course grade. Problem 7 is optional and does not affect your grade.

Collaboration is welcome. If you do collaborate, make sure to write/type your own paper *and give credit to your collaborators in your pledge*. Your solutions should contain full proofs. Bare answers will not earn you much.

(1) [3pt] (4.3.16) Show that 2^n divides an integer N if and only if 2^n divides the number made up of the last n digits of N. (*Hint:* $2^k 5^k = 10^k \equiv 0 (\bmod 2^n)$ for $k \geq n$.)

(2) The International Standard Book Number (ISBN) used in many libraries consists of nine digits $a_1, a_2, \ldots, a_9$, followed by a tenth check digit a_{10}, which satisfies

$$a_{10} \equiv \sum_{k=1}^{9} k a_k (\bmod 11).$$

(So, to be exact, sometimes a_{10} is not a digit but rather a symbol '10'.)

(a) [2pt] (4.3.27) Determine whether each of ISBNs below is valid:
0-07-232569-0,
91-76-43-497-5,
1-56947-303-10.

(b) [3pt] (4.3.28) When printing ISBN $a_1 a_2 \ldots a_9$, two unequal digits were transposed. Show that the check digit detected that an error happened.

(c) [3pt] When printing ISBN $a_1 a_2 \ldots a_9$, one of digits was randomly changed for some other number between 0 and 9. Prove that the check digit detected that an error happened. (In other words, a_{10} detects a single error.)

(d) [3pt] Prove that for an invalid ISBN obtained as in the item above, there may be more than one way to correct one of digits $a_0 \ldots a_9$ so that the ISBN becomes valid. (In other words, while a_{10} *detects* a single error, it does not *correct* a single error.)

(e) [3pt] When printing ISBN $a_1 a_2 \ldots a_9$, one of digits came out illegible. Prove that knowing the check digit, one can recover the illegible digit.

(f) [3pt] Give an example that if two digits in $a_1 \ldots a_9$ were randomly changed, the check digit may have been preserved, thus missing that errors happened. (In other words, a_{10} may not detect two errors.)

— see next page —

(3) (part of 4.4.1) Solve the following linear congruences:
 (a) [2pt] $25x \equiv 15 \pmod{29}$.
 (b) [3pt] $6x \equiv 15 \pmod{21}$.
 (c) [3pt] $34x \equiv 60 \pmod{98}$.

(4) (part of 4.4.4) Solve the following sets of simultaneous linear congruences:
 (a) [3pt] $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$.
 (b) [4pt] $2x \equiv 1 \pmod 5$, $3x \equiv 9 \pmod 6$, $4x \equiv 1 \pmod 7$, $5x \equiv 9 \pmod{11}$.

(5) [3pt] (4.4.6) Find the smallest integer $a > 2$ such that

$$2 \mid a, \quad 3 \mid a+1, \quad 4 \mid a+2, \quad 5 \mid a+3, \quad 6 \mid a+4.$$

(6) [3pt] (4.4.10) (Ancient Chinese Problem) A band of 17 pirates stole a sack of gold coins. When they tried to divide the fortune into equal portions, 3 coins remained. In the ensuing brawl over who should get extra coins, one pirate was killed. The wealth was redistributed, but this time an equal division left 10 coins. Again an argument developed in which another pirate was killed. But now the fortune was evenly distributed among the survivors. What was the least number of coins that could have been stolen?

(7) Reminder: an arithmetic series is the series of the form $A = (a + kd : k = 0, 1, 2, \ldots)$. The number d is called the *difference* of the arithmetic series. We will say that A is *integer* if both a and d are integer.
 (a) [0pt] Can the set of positive integers be covered by a finite number of integer arithmetic series with pairwise coprime differences larger than 1? (For example, $(1, 3, 5, 7, \ldots) \cup (2, 5, 8, 11, \ldots) \cup (4, 6, 8, 10, \ldots)$ cover $\mathbb{N}$ but the differences are not coprime; another example: $(1, 4, 7, \ldots) \cup (2, 4, 6, \ldots) \cup (3, 8, 13, \ldots)$ miss 5 and many other numbers.)
 (b) [0pt and a box of cookies] Can the set of positive integers be covered by a finite number of integer arithmetic series with distinct (but not necessarily pairwise coprime) differences larger than 1?