

Name:

Collaborator(s)¹:

Math 453, Section X13, Prof. Hildebrand, Spring 2011

HW Assignment 4, due Monday, 2/21/2011

Instructions

- **Rules:** The usual: Write your name on the cover sheet and staple the sheet to the assignment. Do the problems in order, and make sure that each problem is clearly labelled. The assignment is due in class at the above due date.
- **Write-up:** Solutions, rather than answers, are expected for all problems. Write legibly, using proper mathematical notation and terminology, and in complete sentences. For proofs you can use any result covered in class, the class handouts, and the relevant sections of the Strayer text.

HW 4 Problems

All problems are from Chapter 2 of Strayer, Sections 2.2–2.5.

- | | | |
|-----------|--------------|------------|
| 1. *28(d) | 5. *43(a)(b) | 9. *59 |
| 2. *32 | 6. *51(b)(c) | 10. *62(a) |
| 3. *33(d) | 7. *52 | |
| 4. *36 | 8. *57(b) | |

11. Prove that $453 \cdot 347^n + 408^{n+1}$ is divisible by 5 for all *odd* positive integers n .

12. **Extra credit.² A self-correcting ISBN numbering scheme.** This problem is motivated by the ISBN check number scheme mentioned in Friday’s class. Consider a modified ISBN check number scheme that involves 10 digits x_1, x_2, \dots, x_{10} , where the first 8 digits are arbitrary digits with values in $\{0, 1, \dots, 9\}$ and the last two digits x_9 and x_{10} are check digits with values in $\{0, 1, \dots, 9, 10\}$ (where a “10” would be represented as “X”, as in the usual ISBN scheme), and two checksums, S and T , defined by $S = \sum_{i=1}^{10} x_i$ and $T = \sum_{i=1}^{10} ix_i$. Define the number to be **valid** if the checksums S and T are both congruent to 0 modulo 11. Prove that, with this scheme, one is able to **correct** any single digit error; that is, given a number that is the result of a single digit error in a valid ISBN number, one can, in an unambiguous manner, reconstruct the original (correct) ISBN number. Give a simple algorithm/formula for finding the correct number. (More precisely, find a formula/algorithm (which may involve the checksums of the modified number) that gives the location of the error, and another formula/algorithm that gives the original digit at this location.) Illustrate your algorithm/formula with a few random numerical examples. For instance, take the first 8 digits in your UIN (or a phone number, etc) as x_1, \dots, x_8 , find the corresponding check digits x_9 and x_{10} to get a valid (in the above sense) 10-digit ISBN, then create several “botched” versions of this number, each obtained by changing one of the digits, apply the algorithm on these “botched” versions, and verify that it correctly reconstructs the original number.

*** Turn page for comments and hints ***

¹If you worked with another student or in a small group on this assignment, list the names of all students involved.

²No hints, help, or group work on extra credit problems, as this would defy the intent of these problems. The problems require nothing more than the techniques and results covered class, but are out of the ordinary in one way or another, and require more thought and insight than the typical regular homework problem. If such a problem piques your interest, give it a try; otherwise, no harm done—problems at this level aren’t exam material.

Comments and Hints

- **Solving congruences:** The first four problems (through #36) in this assignment are purely computational problems that ask you to solve a given linear congruence or a given system of linear congruences. You must do these problems using appropriate algorithms, as in the examples in Sections 2.2 and 2.3 of Strayer. Trying to arrive at the answer by guessing would defy the purpose of the problem (which is to practice the appropriate algorithm). You won't get credit for answers arrived at by guessing or by brute force methods. Make sure to read/review the examples worked out in Sections 2.2 and 2.3 of Strayer, and the key theorems (Theorem 2.7 and Theorem 2.10 on p. 9 of the Definitions/Theorem handout) before working on these problems.
- **Problem 36:** This is a fun puzzle (involving pirates killing each other off ...) whose solution amounts to solving a system of congruences, and hence is a perfect case for the Chinese Remainder Theorem. There are many puzzles of this type that boil down to solving simultaneous congruences. (Another example is Problem 37 (not assigned). Those who have taken Math 347 may recognize this as a version of the "Coconuts Problem".)
- **Fermat's Theorem and "congruence magic".** Most of the remaining problems are exercises in "congruence magic", similar to the examples from Friday's class. As illustrated in class, this can be easy and painless even if the numbers involved are gigantic, such as $3^{1000000} \pmod{7}$. If the modulus is a prime number, this becomes even easier since then Fermat's Theorem (see Section 2.5) can be applied to get an exponent that gives something congruent to 1. In the general case, such an exponent can still be found, but may require by a bit of trial and error, as illustrated in the class examples on Friday.
- **Congruences to composite moduli:** For several of the problems (e.g., 57 and 59), the following general result is useful: A congruence to a product of distinct primes (or powers of distinct primes) is equivalent to a system of congruences modulo the individual primes (or prime powers). For example, since $42 = 2 \cdot 3 \cdot 7$, the congruence modulo $x \equiv a \pmod{42}$ is equivalent to the system of congruences $x \equiv a \pmod{2}$, $x \equiv a \pmod{3}$, $x \equiv a \pmod{7}$. (This is just a special case of the Chinese Remainder Theorem.)