MPCS 50103 Discrete Mathematics—Autumn 2019

Homework 2. Revised: October 10, 2019. This problem set is due Monday October 14 at 11:59 pm.

Reading: Rosen 7e, chapter 4, sections 4.1, 4.3–4.4.

Homework assignment

- "DO" exercises are strongly recommended to check your understanding of the concepts. **Solve them but do not submit them**.
- **Problems labeled "HW" are homework problems that you are required to submit**.
- You are responsible for the material covered in **both** "DO" exercises and HW problems.

"Do" Exercises (solve but do *not* submit):

1. **"DO"** Rosen 7e, section 4.1, exercises 3, 4, 5, 7, 8, 13, and 37 on pages 244–245.

2. **"DO"** Rosen 7e, section 4.3, exercises 5, 33b, 35, and 39e, on pages 272–274.

3. **"DO"** Rosen 7e, section 4.4, exercises 5c, 11b, and 17, on pages 285–285.

Homework Problems: DUE Monday October 14 at 11:59 pm

- **Collaboration policy:** There is no penalty for acknowledged collaboration. To acknowledge collaboration, give the names of students with whom you worked at the beginning of your homework submission and mark any solution that relies on your collaborators' ideas. Note: you must work out and write up each homework solution by yourself without assistance.
  DO NOT COPY or rephrase someone else's solution.
  The same requirement applies to books and other written sources: you should acknowledge all sources that contributed to your solution of a homework problem. Acknowledge specific ideas you learned from the source.
  DO NOT COPY or rephrase solutions from written sources.
- **Internet policy:** Looking for solutions to homework problems on the internet, even when acknowledged, is STRONGLY DISCOURAGED. If you find a solution to a homework problem on the internet, do not not copy it. Close the website, work out and write up your solution by yourself, and cite the url of website in your writeup. Acknowledge specific ideas you learned from the website.
  Copied solutions obtained from a written source, from the internet, or from another person will receive ZERO credit and will be flagged to the attention of the instructor.
- Write out your work for every problem. If you just write your answer without showing your work, you will not receive credit.

1. **HW**
   - Prove that the product of any three consecutive positive integers is divisible by 6. (2 points)
   - Find (without actual multiplication) the smallest positive integer n such that $n!$ is divisible by 990. (2 points)
   - **Definition.** An integer a is a perfect square if there is an integer b such that $a = b^2$.
     Prove that if a positive integer has an odd number of divisors, then it is a perfect square. (3 points)

2. **HW**
   - Prove: for all integers x, either $x^2 \equiv 0 \pmod 4$ or $x^2 \equiv 1 \pmod 4$. (2 points)
   - Some prime numbers can be represented as the sum of two squares; e.g., $5 = 2^2 + 1^2$, $13 = 2^2 + 3^2$. Others, such as 3, 7, 11, cannot.
     - Make a table of all prime numbers < 200. Next to each prime p write its expression as the sum of two squares if p can be so represented; otherwise, write "none" next to p. (2 points)

  - Based on the data collected in your table, make a conjecture describing which primes can be represented as the sum of two squares and which primes cannot. Your conjecture should be go like this, where you fill in the blank:

    > It seems from the data displayed in the table that a prime p can be represented as a sum of two squares if and only if either $p = 2$ or p satisfies -------.

    (2 points)
  - Give a simple proof that the primes you conjectured cannot be represented as a sum of two squares indeed cannot. (3 points)

3. **HW** Let p and q be distinct prime numbers, i.e., $p \neq q$. What is the number of distinct divisors of the following numbers?
   - pq. Explain your answer. (1 point)
   - p^2q. Explain your answer. (1 point)
   - p^2q^2. Explain your answer. (1 point)
   - p^nq^m, where n and m are positive integers. Explain your answer. (2 points)

4. **HW**
   - Prove: if a, b, and m are integers such that $m \geq 2$ and $a \equiv b \pmod{m}$, then $a^2 \equiv b^2 \pmod{m}$. (2 points)
   - Prove: if a, b, m, and n are integers such that $m \geq 2, n \geq 1$, and $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$. (Hint: induction.) (3 points)

5. **HW Definition.** A *multiplicative inverse* of an integer a modulo m, where m is an integer ≥ 2, is an integer x such that $ax \equiv 1 \pmod{m}$.
   - Prove: a has a multiplicative inverse modulo m if $\gcd(a, m) = 1$. (3 points)
   - Find a multiplicative inverse of a modulo m for each of the following pairs of integers or prove that a multiplicative inverse does not exist. Use the Euclidean algorithm. Show your work.
     - $a = 3, m = 62$. Your answer should be in the range $\{0, \ldots, 61\}$ if a multiplicative inverse exists.
     - $a = 13, m = 21$. Your answer should be in the range $\{0, \ldots, 20\}$ if a multiplicative inverse exists.
     - $a = 21, m = 91$. Your answer should be in the range $\{0, \ldots, 90\}$ if a multiplicative inverse exists.

     (2 points each)

6. **HW** Your ChicagoID (on the back of your Student ID card) represents **you** to the computers of this University. Documentation for creation and validation of ChicagoID numbers can be found at the following site: ChicagoID Generation Specification. This problem follows the notation in the Chicago ID documentation.

   Identifier format: A ChicagoID is string of 9 characters: $CD_1D_2D_3\ D_4D_5D_6\ D_7A$, where $D_1 \ldots D_7$ are integers in the range $0 \leq D_i \leq 9$, A is an uppercase alphabetical character (A through Z inclusive), and C is an integer in the range $0 \leq C \leq 9$.

   Check digit: Instead of being chosen, the integer C is calculated from the values of the other characters after they are chosen. The method is described at the ChicagoID site and is repeated here:

   • Step 1. Let $D_1 \ldots D_7$ be each chosen at random and independent from any previous choice. Let A be a number between 65 and 90, inclusive, chosen in the same way. A is split into the 10s and the 1s parts to form two new integers A_1 and A_2, with $6 \leq A_1 \leq 9, 0 \leq A_2 \leq 9$.

   • Step 2. Let D_1 be in slot 1 of the array, D_2 in slot 2 and so on; A_1 occupies slot 8 and A_2 occupies slot 9. If a slot number is even, replace its value with the sum of the digits of the number which is twice the original value. Example: if 6 is in an even-numbered slot, it would

be replaced by 3, since the sum of the digits of 12, which is twice 6, equal 3.
These substituted values are obviously still $0 \le D_i \le 9$; the same rule applies to A_1 since it occupies an even-numbered slot.

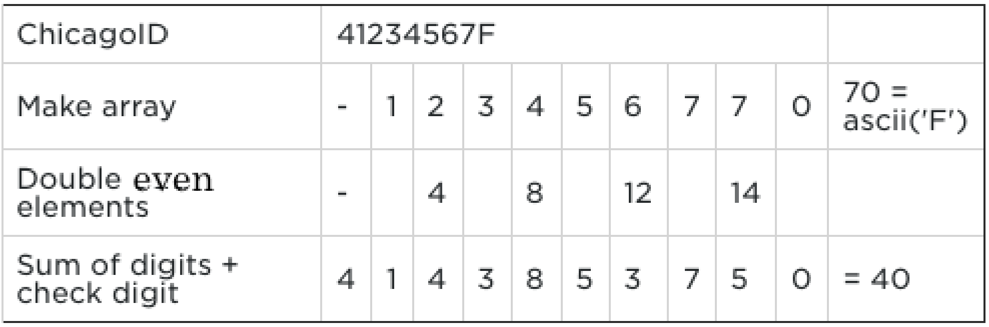
- Step 3. Sum the digits of all these values, under mod 10.
- Step 4. Determine a value for C that, when added to the sum in step 3, results in a zero, also under mod 10. That is, the following equation is satisfied:

$$C + D_1 + D_2' + D_3 + \ldots + D_6' + D_7 + A_1' + A_2 \equiv 0 \pmod{10}$$

where D_i' is the new value of D_i after doubling it and adding its digits.

A check digit C is considered *infeasible* if it does not satisfy the above equation. A ChicagoID is *valid* if the above equation is satisfied.

Example:



ChicagoID	41234567F										
Make array	-	1	2	3	4	5	6	7	7	0	70 = ascii('F')
Double even elements	-		4		8		12		14		
Sum of digits + check digit	4	1	4	3	8	5	3	7	5	0	= 40

Now perform the following tasks:

- Write down your ChicagoID, then change both C and one other slot so that it is still valid. Show it is still valid. (2 points)
- Write down your ChicagoID, then make minimum number of changes (two values) without changing C so that it is still valid. Show it is still valid. (2 points)
- Let S_1 be a valid ChicagoID sequence (not including C). Let S_2 be another sequence formed by changing only one value of S_1. Prove or disprove that a single feasible C value exists for both sequences. (2 points)
- Let S_1 be a valid ChicagoID sequence (not including C). Let S_2 be another sequence formed by changing more than one value of S_1. Prove or disprove that a single feasible C value exists for both sequences. (2 points)
- Let S_1 be a valid ChicagoID sequence (not including C). **Consider only an error that swaps the position of adjacent values in the next two questions.**
  - (a) Show that there exist two sequences that differ from each other by exactly one swap but have the same check digit C. (2 points)
  - (b) Describe a modification to Step 1 above (in the random choice of D values) to disarm the issue that your solution of (a) exploits. What is the issue? (2 points)

(*Acknowledgment to Colin Hudler*)

Gerry Brady
Thursday October 10 15:50:34 CDT 2019