MPCS 50103 Discrete Mathematics—Autumn 2019

Homework 3. Revised: October 17, 2019. This problem set is due Monday October 21 at 11:59 pm.

Reading: Rosen 7e, chapter 4, sections 4.4, 4.6; chapter 6, sections 6.1; 6.3–6.4.

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 4.4, exercises 7, 16, 17, 33, 35, and 36, on pages 285–286.

2. **"DO"** Rosen 7e, section 4.6, exercise 23, on page 305.

3. **"DO"** Rosen 7e, section 6.1, exercises 33, 41, 47, and 49, on pages 397–398.

4. **"DO"** Rosen 7e, section 6.3, exercises 11, 31, and 43, on pages 413–415.

Homework Problems: DUE Monday October 21 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.
- **In this problem set, do not simplify exponents, factorials, or binomial coefficients. For example, write 2^8, not 256; 5!, not 120; "6 choose 3" in symbolic form, not 20.**

1. **HW** Use Fermat's little theorem to perform the following tasks.
    - Find an integer $0 \le a < 73$, with $a \equiv 9^{794} \pmod{73}$. Show your work and explain your answer. (2 points)
    - Solve the congruence $x^{103} \equiv 4 \pmod{11}$. Hint: use the fact that $x^{10} \equiv 1 \pmod{11}$ from Fermat's little theorem. Explain your answer. (3 points)

2. **HW**
    - Compute $14^{100} \pmod{25}$ by the method of repeated squaring. Show your work. (1 point)

- The congruence $7^{1734250} \equiv 1660565 \pmod{1734251}$ is true. Can you conclude that 1734251 is a composite number? Explain your answer. Do NOT factor! (2 points)
- The congruence $2^{52632} \equiv 1 \pmod{52633}$ is true. Can you conclude that 52633 is a prime number? Explain your answer. Do NOT factor! (2 points)

3. **HW** In an RSA cryptosystem, $p = 5$ and $q = 7$.
   - Find the smallest encryption exponent $e > 1$ which is legal for RSA encryption and the corresponding decryption exponent d. Show your work and explain. (2 points)
   - Encrypt the message $M = 3$. Show your work. (1 point)
   - How many legal (e, d) pairs are there, not including (e =1, d = 1) in this RSA cryptosystem? Would they all result in different encryptions of 3? Explain your answers. (2 points)

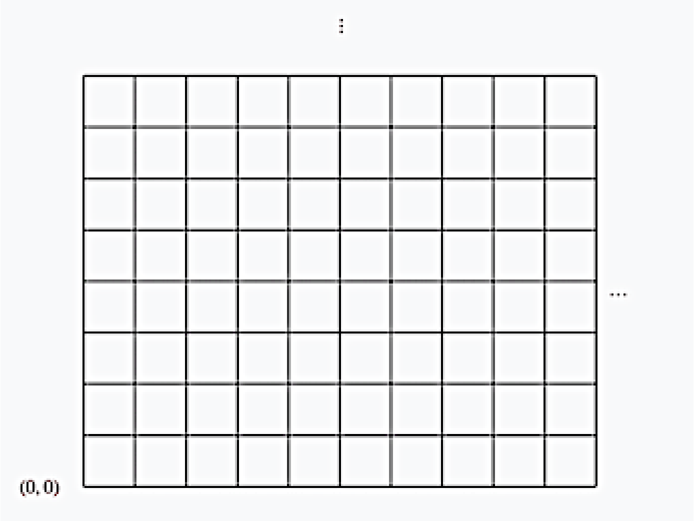
4. **HW** Answer each of the following counting questions. Do **not** simplify exponents, factorials, or binomial coefficients.
   - There are 31 students in a class, including Alice and Bob. How many ways are there to choose two soccer teams (11 players) so that Alice and Bob are not on the team together?
   - There are 2 women and 7 men in a chess club. A team of four persons must be chosen for a tournament, and there must be at least 1 woman on the team. In how many ways can this be done?
   - How many ways are there to arrange 7 Cubs fans and 5 Sox fans in a row in such a way that no Sox fans stand next to each other?
   - How many ways are there to arrange n men and n women around a circular table so that men and women alternate?

   Show your work and explain your answers. Use basic counting rules (inclusion-exclusion, sum, product, complementary counting). (See esp. Rosen section 6.1.) Do not prove by exhaustion. (2 points each)

5. **HW** A **standard deck of cards** consists of 52 cards. These come in 13 ranks or *kinds* (A, K, Q, J, 10, 9, 8, 7, 6, 5, 4, 3, 2) of four cards each. They are also grouped into four *suits* (spades ♠, hearts ♥, diamonds ♦, clubs ♣), with one card of each kind in each suit. A **five-card hand** is a subset (unordered) of 5 of the 52 cards in a standard deck chosen at random.
   Answer each of the following questions. Do **not** simplify exponents, factorials, or binomial coefficients.
   - How many five-card hands have at least one card in every suit?
   - How many five-card hands have at least three cards of the same kind?
   - How many five-card hands have no ace and at least one king?
   - How many five-card hands have no ace, exactly one king, and at least one diamond?

   Show your work and explain your answers. Use basic counting rules (inclusion-exclusion, sum, product, complementary counting) and properties of combinations. (See esp. Rosen section 6.3.) Do not prove by exhaustion. (3 points each)

6. **HW** Suppose a street grid starts at position (0, 0) and extends up and to the right:



A shortest route along streets from $(0,0)$ to (i,j) is $i+j$ blocks long, going i blocks east and j blocks north.

- How many shortest routes $(0,0)$ to (i,j) are there? (1 point)
- Suppose that the block between (k,l) and $(k+1,l)$ is closed, where $k < i$ and $l \le j$. How many shortest routes are there from $(0,0)$ to (i,j)? Show your work and explain your answer. (2 points)
- How many shortest routes are there from $(0,0)$ to (i,j) that that do not go through either of the points (k,l) or $(k+3,l+3)$, where $k+3 < i$ and $l+3 < j$? Show your work and explain your answer. (2 points)

Gerry Brady
Thursday October 17 05:22:12 CDT 2019