Use the PDF problem set posted to the course website; its problem numbering differs from the textbook.

Recitation problems (ungraded)

Attempt these before recitation. We will use recitation to work through selected solutions and the ideas behind them; they are chosen to prepare you for the graded problems below.

(1) DMC Problem 10.26 (a), (b)
(2) DMC Problem 10.35 (a), (b)
(3) DMC Problem 10.14 (b), (c)
(4) DMC Problem 10.41 (a), (c)
(5) DMC Problem 10.51 (a)–(d)
(6) DMC Problem 11.23 (a)
(7) DMC Problem 11.27
(8) DMC Problem 11.42 (a), (c), (e)
(9) DMC Problem 11.52
(10) DMC Problem 11.57 (b)

Problems to submit (100 points)

Show your work and explain your reasoning. A correct answer without adequate justification may receive little or no credit. Write in complete, grammatically sound sentences and submit legible work. The number in square brackets is the number of points each problem is worth.

(1) **[12]** DMC Problem 10.27, including the parenthetical runtime bound
(2) **[12]** DMC Problem 10.35 (c)
(3) **[8]** DMC Problem 10.46
(4) **[8]** DMC Problem 10.52 (e), (f), (h), (j)
(5) **[10]** DMC Problem 10.54 (a)–(d)
(6) **[8]** DMC Problem 11.18
(7) **[10]** DMC Problem 11.31 (a), (c)
(8) **[12]** DMC Problem 11.46
(9) **[6]** DMC Problem 11.53
(10) **[14]** DMC Problem 11.60

Bonus challenge: Fermat's Little Theorem and RSA (up to 10 bonus points)

This problem is completely optional and is meant to be substantially more challenging than the required homework. Each part is graded all-or-nothing: a complete proof earns the listed bonus points, while an incomplete proof earns no points for that part. Bonus points are added to your homework score, up to a maximum score of **110/100**. These problems are adapted from DMC Exercises in the text of Chapter 10; you can look to these exercises for guidance.

(a) **[5 bonus points] Fermat's Little Theorem.** Prove that if p is prime and k is any integer, then $k^p \equiv k \pmod{p}$.

(b) **[5 bonus points] RSA decryption.** Let $n = pq$, where p and q are distinct primes. Let e be any

number relatively prime to $(p-1)(q-1)$, and let d be such that $ed \equiv 1 \pmod{(p-1)(q-1)}$. Prove that for all integers M, we have $(M^e)^d \equiv M \pmod{n}$.