

Syllabus & Assignments for COMP 502, Spring 2025
Mathematical Foundations of Computer Science

Instructor	Prof. William D. Ellis, wellisl@gmu.edu
Office Hours	By appointment, usually via Zoom.
H/W Grader	Ms. Deepika Naik, dnaik2@gmu.edu
Web Site	<ul style="list-style-type: none"> • Syllabus/HW updates, practice problems, solutions, etc. are posted after lectures in Canvas/Modules: http://canvas.gmu.edu. • No Final Exam solutions or scores will be posted on Canvas.
Schedule	14 Classes 7:20-10:00 PM 206 Planetary Hall <ul style="list-style-type: none"> • Wednesdays Jan. 22 through Apr. 30 <u>except</u> March 12, 2025 • The Final Exam will be 7:30-10:15 PM on Wednesday May 7, 2025
Prerequisite	A working knowledge of algebra. Review textbook pages A1-A3.
Course Content	Logic, sequences, recursion, number theory, set theory, functions, relations, RSA cryptography, probability, graph theory, algorithm complexity. We will solve problems using fundamental definitions, theorems, and algorithms. We'll start with textbook Chapter 5, then follow the remaining Chapters 1-11 in order.
Required Hardware	(i) A calculator capable of displaying 10 digits and raising numbers to powers. Homework, Quizzes and Exams, often require such a calculator. (ii) You'll need a webcam for any Office Hour appointments, or when bad weather might force a lecture online.
Graded Exams and Quizzes	We will have: (i) 2 Quizzes, (ii) 2 Hour Exams, and (iii) 1 comprehensive Final Exam. The Quizzes and Exams: <ul style="list-style-type: none"> • Will be given only once (no makeup Quizzes or Exams), and • No partial credit for any attempt at proving anything false. <p style="text-align: center;">During Quizzes & Exams:</p> <ul style="list-style-type: none"> • You may <u>not</u> provide, accept, or seek help from anyone else. • Calculations must be based on your calculator and <u>not</u> be derived from the Internet, Bluetooth, a computer, or a smart watch. • Bring any notes, including copies of pages from the textbook or copies of handwriting, but <u>nothing with original handwriting</u>. • Do <u>not write</u> on anything except your exam or on any blank pages that are part of your original pre-printed exam. • Do <u>not</u> provide, receive or exchange with anyone else any materials including papers, erasers, and calculators. • Do <u>not</u> sit near friends. I will move some students randomly. • Do <u>not</u> use or display cell phones, computers, smart watches.
Textbook	Discrete Mathematics with Applications, 5th ed. By Susanna S. Epp, ISBN-10: 1337694193; ISBN-13: 978-1337694193; Cengage MA <ul style="list-style-type: none"> • Rental fee (\$53.05) for the e-book version is automatically included in your tuition bill. If you "opt out" before 11:59 PM on Feb. 11, 2025, then the fee should be refunded to you. • To view the e-book, click on "Course Materials" in Canvas. • The GMU Bookstore may have emailed you more instructions, "Subject: Your Digital Materials Are Available." • We need the 5th ed., but some students supplement study with an inexpensive hard-copy 3rd or 4th ed. purchased on-line.
Final grade = weighted average of letter grades	45% - Final Exam 40% - 2 Hour Exams X 20% each 15% - 2 Quizzes X 5% each + Homework 5% Final Grades will be posted on Patriot Web, <u>not</u> on Canvas.
Help & Email	Send me any questions always using GMU email - never via Canvas!

Syllabus & HW assignments are updated the day AFTER each lecture.

Homework Upload a black/white pdf no more than 30 minutes after class. Late H/W submissions will not be accepted. Credit is given for any serious attempt, even if incorrect, at solving a problem. H/W is assigned after each lecture except the last one (April 30). Only the highest 12 of the 13 H/W scores are counted.

GMU Policies This course abides by GMU's [Common Policies Addendum](#).

Honor Code

- The minimum (Level 1) Sanction for Cheating is "0% on the assessment and an additional letter grade reduction in the final course grade." See GMU's webpage [Academic Standards](#).
- The webpage contains a link to "Academic Standards Code as in effect on 8/7/2024" - a copy is also posted under Canvas/Modules.
- Honor Code allegations are resolved by GMU's Honor Committee.
- For submitting homework in COMP 502/Spring 2025 only, it is okay (i.e., there's no HC violation) to collaborate with anyone, use artificial intelligence (AI), or copy from classroom discussions.

Semester Schedule

Lecture	Date	Event	All event dates are subject to change
(1)	Jan 22, 2025	1st class	
(2)	Jan 29, 2025		
(3)	Feb 05, 2025		
(4)	Feb 12, 2025		
(5)	Feb 19, 2025	Quiz-1, Lecture	
(6)	Feb 26, 2025		
(7)	Mar 05, 2025		
	Mar 12, 2025	No Class	Spring Recess
(8)	Mar 19, 2025	Exam 1, Lecture	
(9)	Mar 26, 2025		
(10)	Apr 02, 2025		
(11)	Apr 09, 2025	Quiz-2, Lecture	
(12)	Apr 16, 2025		
(13)	Apr 23, 2025		
(14)	Apr 30, 2025	Exam 2, Lecture	
(15)	May 07, 2025	FINAL EXAM 7:30 - 10:15 PM	On everything we covered during the entire semester, ending with section 11.3. Study these Canvas documents: <ul style="list-style-type: none"> • HW, Examples, and Sample Problems in Weeks #1-#14, • Solutions to Quizzes and Exams, • Practice Quizzes and Exams. • Week 12 pdf: Binomial Probabilities and Expected Values

Syllabus & HW assignments are updated the day AFTER each lecture.

Row	§	Homework is from the textbook or as cited below.		Due
(1)	1.2	#7(b), (e), (f); #9(c)-(h) (page 14) <u>Hint</u> : See textbook pages 7-8 and Examples 1.2.1, 1.2.2, 1.2.4, and 1.2.8 on Canvas.		HW-1 due 1/29/2025
(2)	5.1	7, 16, 32, 57 (modified)*, 61 (pages 273-274) * #57 (modified) Only calculate the sum for n=5. Ignore the textbook asking about "changing variable." See Example 5.1.55 in Canvas/Modules.		HW-1 due 1/29/2025
(3)	5.2	#23, 27, 29. (pg 288) <u>Hint on #23</u> : Compare with Example 5.2.20 in Canvas <u>Hints on #27, 29</u> : • Use the "Simplified formula for summing a geometric series" in Canvas/Modules/Week 1, <u>or</u> See the textbook formula and example on pages 283 and 285; or see Canvas Example 5.2.25(b); <u>Another Hint on #29</u> : Test your answer using n=3.		HW-1 due 1/29/2025
(4)	5.1	True or False? Why? "∀" means "for all."	$\sum_{k=1}^{k=n} (8k^3 + 3k^2 + k) = n(n+1)^2(2n+1) \forall n \in \{1, 2, 3, 4\}$	HW-1 due 1/29/2025
(5)	<u>Hint</u> : Row (4) asks us to verify 4 different but similar formulas, one each for n=1, 2, 3, 4: • For n=1, does $8*1^3 + 3*1 + 1 = 1*(1+1)^2*(2*1+1)$? • For n=2, does the <u>sum</u> $(8*1^3 + 3*1 + 1) + (8*2^3 + 3*2 + 2) = 2*(2+1)^2*(2*2+1)$, ...?			
(6)	1.2	12 (pg 15) <u>Hint</u> : Compare Canvas solution #1.2.11.		HW-2 due 2/5/2025
(7)	5.1	83 (pg 275) <u>Hint</u> : See #5.1.81 on Canvas.		HW-2 due 2/5/2025
(8)	5.2	Express $S = \sum_{k=29}^{k=123} (16) * \left(\frac{25}{24}\right)^{-k}$ as a decimal number accurate to within .01. For example, your answer might look like "S = 52.33." <u>Hints</u> : • We're adding 95 actual numbers. Compute a few of them to judge the sum's approximate size. • Use the theorem on page 283, or Canvas/Modules/Week 1 "Simplified formula for summing a geometric series." • See the Solution to Sample Quiz-1, #4.		HW-2 due 2/5/2025
(9)	5.6	8, 14 (page 337) <u>Hints</u> • 5.6.8 is like Example 5.6.6 on Canvas. • 5.6.14: See the Hint on Canvas & Example 5.6.13.		HW-2 due 2/5/2025
(10)	5.7	2(b)&(d), 4, 25 (pages 350-351) <u>Hint</u> : • 5.7: See the Canvas hint for 5.7.2(d). • has a hint plus solved Examples 5.7.1(c) & 5.7.7.		HW-2 due 2/5/2025
(11)	5.8	12, 14 (page 363) See the HW-2 Hints in Row (12) below.		HW-2 due 2/5/2025

Syllabus & HW assignments are updated the day AFTER each lecture.

Row	§	Homework is from the textbook or as cited below.	Due
(12)		<u>Hints</u> : • For #5.6.14, see the 5.6.13 solution on Canvas. • #5.8.12 & #5.8.14 are like the Canvas solutions to #7 and #8 for Sample Quiz 1. Also see "4 Sample Recurrence Relations Solved." • #5.8.12 & #5.8.14 use Theorems 5.8.3 (pg 357) and 5.8.5 (pg 361). • The Canvas solution to Sample Quiz 1 #7 shows how to factor the Characteristic Equation using standard methods.	
(13)	2.1	#15, #37, #43 (pgs 52-53) <u>Hints</u> : • #37 is like #2.1.33 on Canvas. • #43 is like #2.1.41 on Canvas.	HW-3 due 2/12/2025
(14)	2.2	#4, #15, #27 (pgs 63-64). <u>Hint</u> • 2.2.4: See Canvas "Example: Solution to SE-2 #7, rewriting a statement in an if-then format."	HW-3 due 2/12/2025
(15)	2.2	Solve "HW Problem on Informal English" on Canvas. <u>Hints</u> : See • The Spock example in the Canvas document "Spock and Limbaugh Examples: Sound vs. Valid Arguments & Informal English." • Remark 2 on textbook page 62 on informal language.	HW-3 due 2/12/2025
(16)	2.2	Do "HW Assignment: A small satisfiability ("SAT") problem" on Canvas/Modules/Week #3	HW-3 due 2/12/2025
(17)		Assume x is an integer. Consider the statement $s := "(x^2 - x) \text{ is exactly divisible by } 3."$ Choose and answer <u>exactly one</u> of (A), (B), or (C): (A) Explain why s is TRUE; <u>or</u> (B) Explain why s is FALSE; <u>or</u> (C) Explain why neither (A) nor (B) is possible.	HW-3 due 2/12/2025
(18)	2.3	#9 (pg 77) <u>Hints</u> : See Canvas Week #2: • "Example: Test a syllogism's validity," <u>or</u> • "Example: Sample Exam-2 #4 Solution," <u>or</u> • "Example 2.3.11." • The rationale for Epp's incomplete shortcut for determining validity is compared to common sense in Table 5 of "Handy Summary of Logic Facts: Truth Tables, Argument Forms, and Syllogisms." The comparison helps us answer <u>the question Epp ignores</u> : When at least one false premise appears in <u>every</u> row of the truth table, is the argument valid?	HW-3 due 2/12/2025
(19)	3.1	#12, #18(c)-(d); #28(a)&(c); #32(b),(d) pgs 119-121 <u>Hints</u> See Canvas Example 3.1.18 (a),(b),&(e). • 3.1.28: To void remembering order of operations, put a parenthesis before "Real" and after "Neg(x)."	HW-4 due 2/19/2025

Row	§	Homework is from the textbook or as cited below.	Due
(20)	3.2	<p>#10, #25(b)-(c), #38 (pages 130-131).</p> <p>In these problems:</p> <ul style="list-style-type: none"> • \forall and \exists are the only quantifiers that may be used here. Do not put any slashes through a quantifier, e.g. do not use a \exists. • No negation symbol (\neg) may appear outside a quantifier or an expression involving logical connectives, e.g. instead of "$\neg(\forall x.(P(x) \rightarrow Q(x)))$," write "$\exists x.(P(x) \wedge \neg Q(x))$." <p><u>Hints</u>: • On #10, see Examples 3.2.9 and/or 3.2.17.</p> <ul style="list-style-type: none"> • On #38: <i>Discrete Mathematics</i> refers to the phrase "Discrete Mathematics," <u>not</u> to the subject Discrete Mathematics. 	HW-4 due 2/19/2025
(21)	3.1 3.2	Solve "Homework Problem: Convert plain English to a quantified predicate formula" on Canvas/Week 4.	HW-4 due 2/19/2025
(22)	3.3	<p>#41(c), (d), (g), (h) (page 145)</p> <p><u>Hints</u>: See the Order of Quantifiers example discussed in class, namely $L(x, y) := "x \text{ loves } y"$ (pg 138).</p>	HW-4 due 2/19/2025
(23)	3.3	<p>Let $s := (\forall x.(P(x) \wedge \exists y \exists z.Q(x, y, z))) \rightarrow (\exists x \exists y.R(x, y))$. Negate s and simplify $\neg s$ so:</p> <ul style="list-style-type: none"> • No negation symbol (\neg) appears outside a quantifier or an expression involving logical connectives (like \wedge, \vee, or \rightarrow). • Use only the \forall and \exists quantifiers. Do not put any slashes through a quantifier, e.g. do <u>not</u> use a \exists. <p><u>Hint</u>: See "Example: Negating a Multiply-quantified statement" on Canvas.</p>	HW-4 due 2/19/2025
(24)	1.3	<p>#15(c), (d), & (e) (pg 23)</p> <p><u>Hint</u>: We already discussed 1.3.15 in class. Also, see Example 1.3.13 on Canvas.</p>	HW-5 due 2/26/2025
(25)	4.1	<p>4, 9, 13(b) (pages 171-172)</p> <p><u>Hint</u>: Canvas #4.1.13(b) is similar to #4.1.14.</p>	HW-5 due 2/26/2025
(26)	4.2	<p>9, 13, 19, 27 (page 181-182).</p> <p><u>Hints</u>: • For 4.2.9: (1) Call the given integer n. (2) Use the hypothesis on n (i.e., the information given about n) to write an equation: $(n-1) = \dots$ (3) Now factor $(n-1)$. (4) Explain why each factor is > 1, thereby showing $(n-1)$ cannot be prime (like in 4.2.14).</p> <ul style="list-style-type: none"> • For 4.2.13: See the 4.2.14 solution on Canvas • For 4.2.19: (i) Identify the error, then state also whether the "Theorem" is TRUE or FALSE, then explain why. (ii) Find the error by comparing the given "proof" with the Canvas pdf "Bogus proof that $8=10$." 	HW-5 due 2/26/2025
(27)	4.3	<p>7 (pg. 187) <u>Hint</u>: Mimic 4.3.6 which we solved in class and is solved on Canvas.</p>	HW-5 due 2/26/2025

Row	§	Homework is from the textbook or as cited below.	Due
(28)	4.1 4.2	<u>Hint:</u> For the section 4.1-4.2 problems, use the even-odd definitions on page 162, NOT the familiar even/odd properties shown in § 4.3 (pages 186-187). Those pg-186-187 properties are derived from the page-162 definitions too!	
(29)	4.3	28 (page 188)	HW-5 due 2/26/2025
(30)	4.4	28, 41 (pages 198-199)	HW-6 due 3/5/2025
(31)	4.5	6, 21, 39 (pages 209-210) <u>Hint:</u> • #39. Break into 6 cases. (Examples 4.5.17 & 37 break into 2 cases. Canvas has another Hint for #39. • #21 is like #4.5.25 on Canvas.	HW-6 due 3/5/2025
(32)	4.10	23(b). <u>Hints:</u> • See the Hint on Canvas. Don't fuss over syntax. In plain English, describe in separate bullets this algorithm's: (1) input, (2) action (what it does with the input), and (3) output. • The solution to 4.3.7 (HW-5) uses the Euclidean Algorithm to reduce a fraction to lowest terms	HW-6 due 3/5/2025
(33)	4.10	Calculate GCD(98741, 247021). <u>Hint:</u> See the solution to 4.10.16 on Canvas.	HW-6 due 3/5/2025
(34)	4.10 & 5.8	Write the Fibonacci no. F_{400} in scientific notation, e.g. $F_{30} \approx 1.35 \cdot 10^6$. Use Epp's definition $F_0=1$, $F_1=1$, ... on page 333; or use the formula in # 5.6.33 on page 339.	HW-6 due 3/5/2025
(35)	4.10	# Observe: $247,710^2 - 38,573^2$ $= 61,360,244,100 - 1,487,876,329$ $= 59,872,367,771 = 260,867 \cdot 229,513$. Now factor 260,867 in a non-trivial way. <u>Hints:</u> • Mimic the factorization examples on Canvas. • "Excel: Euclidean Algorithm" on Canvas can help with your calculations.	HW-6 due 3/5/2025
(36)	4.10	#1 on Sample Quiz-2 <u>Hint:</u> See Canvas Week 7: "Example: Lamé's Theorem Estimate of the Number Steps in a GCD Calculation."	HW-7 due 3/19/2025
(37)	6.1	Of a population of students taking 1-3 classes each, exactly: 19 are taking English, 20 are taking Comp Sci, 17 are taking Math, 2 are taking only Math, 8 are taking only English, 5 are taking all 3 subjects, and 7 are taking only Computer Science. How many are taking exactly 2 subjects?	HW-7 due 3/19/2025

Row	§	Homework is from the textbook or as cited below.	Due
(38)	6.1	#7b; #10(f)-(h); #12(a),(b),(g),(h),(j) (pg 388) <u>Hints</u> : • #7, #10: See 6.1.4, 6.1.10(a)-(e) on Canvas. • #12: Interval notation on page 382 may simplify. • #12(g): Use #12(a) and De Morgan laws (pg 395). [Note: Epp places #12(g)-(j) in § 6.1 to make us like the De Morgan laws when we encounter them in § 6.2.]	HW-7 due 3/19/2025
(39)	6.2	#13. Show $(A-B) \cup (C-B) = (A \cup C) - B$ using any of the 3 methods of proof in Example 6.2.9 on Canvas.	HW-7 due 3/19/2025
(40)	6.3	#4, #7 <u>Hints</u> : • Venn-Diagram shading is <u>never</u> acceptable. Shading alone is usually confusing & unconvincing. • <u>Numbered</u> Venn-Diagram regions are best for verifying or finding a counterexample to a "V sets" identity. See Examples 6.2.9(I) and 6.3.5. • An "is-an-element-of" proof will also verify a "V sets" identity. However, such proofs are often confusing. See Examples 6.2.9(III) and 6.3.20.	HW-7 due 3/19/2025
(41)	6.3	Prove or disprove each of these 2 Claims: • \exists sets A, B & C such that $(A-B)-C = (A-C)-(B-C)$, • \forall sets A, B & C, $(A-B)-C = (A-C)-(B-C)$. A proof may use any method, including I-III in Ex. 6.2.9, except do <u>not</u> use Venn-Diagram shading. <u>Hint</u> : See Examples on Canvasweek 7, 6.3.13 or the "Example: Solution to Sample Quiz 2 #4, problem..."	HW-7 due 3/19/2025
(42)	6.3	# Suppose the set S has size $ S =4$, T is the power set $T=P(S)$ and U is the power set $U=P(T)$. What is the size of U? Your answer should be in a format like, "The size $ U =18,419$." <u>Hint</u> : Use the number-of-subsets formula on page 410.	HW-7 due 3/19/2025
(43)	6.3	# $S = \{1, 2, 3, \dots, 10\}$. A subset $X \subseteq S$ contains either 9 or 10 but <u>not both</u> together in X. Exactly how many such subsets X are possible? <u>Hints</u> • Draw a picture (Venn Diagram) for the power set $P(S)$ with 3 bubbles, one each for the subsets X that contain: (i) 9, (ii) 10, and (iii) both. • See Canvas Example: Counting subsets that contain certain elements	HW-7 due 3/19/2025
(44)	7.1	#2, #12, #51(d),(e), & (f) (pgs 436-439) <u>Note</u> : #51 Will be used in RSA encryption.	HW-8 due 3/26/2025
(45)	7.2	#13, #17 <u>Hint</u> : Mimic Canvas Examples #16 and #18. • The "1-1" definition is on page 440, and • The "onto" definition is on page 446. Both concepts are illustrated in Example 7.2.8.	HW-8 due 3/26/2025
(46)	7.2	#8 & #8.5 on Sample Quiz #2 • An "onto" function is defined on page 446.	HW-8 due 3/26/2025

Row	§	Homework is from the textbook or as cited below.	Due
(47)	7.3	4, 14, 20	HW-8 due 3/26/2025
(48)	1.3	1.3.4 • <u>Hint</u> : See Canvas Example 1.3.3	HW-8 due 3/26/2025
(49)	8.1	#3(c)&(d). (page 493) Hint: See 8.1.1, solved on Canvas.	HW-9 due 4/2/2025
(50)	8.2	#11 (page 503). <u>Hint</u> : See the solution to 8.2.10 on Canvas, <u>or</u> "Practice problems: Properties Enjoyed By Equivalence Relations"	HW-9 due 4/2/2025
(51)	8.3	#9 [Call 0 = the sum of the elements in ϕ .]; #15(b), (c), (d) (page 521) <u>Hints</u> : • #9 See Canvas Examples 8.3.8, 8.3.10, 8.3.12 • #15: Use the modular-equivalence definition on page 518; or Canvas "Two Reasons Why 76^{googol} has Remainder 1 When Divided by 77," paragraph 2.	HW-9 due 4/2/2025
(52)	8.4	#2, #4, #8 (page 544). <u>Hints</u> : • 8.4.4 is like Example 8.4.3. • 8.4.8 is like Example 8.4.7.	HW-9 due 4/2/2025
(53)	8.4	# Calculate $2^{373} \pmod{367}$. <u>Hint</u> : Canvas "Example: Powers of 3 (mod 257)" <u>or</u> textbook page 531	HW-9 due 4/2/2025
(54)	8.4	#18. <u>Hints</u> : For successive squaring examples, see Canvas "Example: Powers of 3 (mod 257)," <u>or</u> Canvas Example 8.4.17 (the format is a little different), <u>or</u> the examples on textbook page 531.	HW-9 due 4/2/2025
(55)	8.4	#15 Practice Quiz-2 <u>Hints</u> : • See Canvas "Examples 8.4.12 & 8.4.13..." Reduce $83415754463525152283 \pmod{9}$ like reducing 305; and $\pmod{11}$ like reducing 4321. • Whenever reducing $\pmod{11}$ start the +1, -1, ... factors from the rightmost digit!	HW-9 due 4/2/2025
(56)	8.4	#20 <u>Hint</u> : See Example 8.4.21 on Canvas. Here, we convert WELCOME into a string of integers like in H/W 8.4.2. Next, reduce each integer $x \rightarrow e(x) = x^3 \pmod{55}$, e.g., $L \rightarrow 12 \rightarrow 12^3 \equiv 23 \pmod{55}$. This problem mimics Example 8.4.9 on page 537.	HW-10 due 4/9/2025
(57)	8.4	#37 See Examples 8.4.21, 8.4.23, and "RSA Examples: Sample Exam-2 #10, #11 Solutions." Only here we convert COME into a string of integers like in H/W 8.4.2. Next, reduce each $x \rightarrow e(x) = x^{43} \pmod{713}$, e.g., $C \rightarrow 3 \rightarrow 3^{43} \equiv 675 \pmod{713}$.	HW-10 due 4/9/2025
(58)	8.4	#27 <u>Hints</u> : • Mimic either of the examples on pages 533 (GCD=6) and page 535 (GCD=1), <u>or</u> mimic the 1st half of these examples on Canvas: • Solve $122x = 9 \pmod{7919}$ discussed in class, • Solving $136y = 14 \pmod{7919}$.	HW-10 due 4/9/2025

Syllabus & HW assignments are updated the day AFTER each lecture.

Row	§	Homework is from the textbook or as cited below.	Due
(59)	8.4	Solve for x : $1014x \equiv 7 \pmod{4,157}$, $0 \leq x \leq 4,156$. <u>Hint</u> : (1a) Express $\text{GCD}=1$ as a linear combination of 1014 and 4157 like on pages 533 ($\text{GCD}=6$), 535 ($\text{GCD}=1$), or H/W 8.4.27 ($\text{GCD}=14$); (1b) Multiply both sides of $1014x \equiv 7 \pmod{4,157}$ by 1014^{-1} (calculated in step (1a)). You may also want to mimic either of these two Canvas Examples: (2) Solve $122x \equiv 9 \pmod{7919}$ discussed in class, (3) Solving $136y \equiv 14 \pmod{7919}$.	HW-10 due 4/9/2025
(60)	8.4	#38, 40 <u>Hint</u> : These problems are like Line (66), except we're solving $43x \equiv 1 \pmod{660}$. Since the public RSA modulus is 713, if a hacker could calculate $\phi(731) = 660$, he could discover the decryption exponent by solving $43x \equiv 1 \pmod{660}$.	HW-10 due 4/9/2025
(61)	8.4	Find the RSA decryption exponent d when: $p=13$, $q=17$, $n=221$, and $e=37$ is the encryption exponent. <u>Hints</u> : • See the example on page 536, or • Canvas "Example: Creating an RSA Encryption-Decryption Pair when $n=821*823$."	HW-10 due 4/9/2025
(62)	8.4	Solve for x : $x^2 \equiv 4 \pmod{675,683}$, all 4 solutions must be between 0 & 675,682. Use $675,683 = 821*823$, the product of 2 primes. <u>Hint</u> : Solve $821a+823b = 1$. Then the four $\text{sqrt}(1)$ are $\{+/-1, +/- (821a-823b)\} \pmod{675,683}$. Now multiply each of the four $\text{sqrt}(1)$ by 2, to get four $\text{sqrt}(4)$. See Canvas: "Two Examples: Finding four Square Roots (mod pq)."	HW-11 due 4/16/2025
(63)	9.1	#4; #8; #14(b)-(c); #Redo 14(b)-(c) using: 30% for Mr. A; 60% for Mr. B; and 40% for Mr. C. <u>Note</u> : \exists 4 HW problems here, each marked with a #. <u>Hints</u> : Mimic Canvas Examples 9.1.3, 7, 10, 12.	HW-11 due 4/16/2025
(64)	9.2	#7, #17(a)-(d) <u>Hints</u> : • #7: See BB Example 9.2.6, & its Alternate Solution. • #17 is like Canvas Example 9.2.12, but #17(d) is tricky! Try choosing the rightmost digit first (5 choices); then the leftmost (8 choices)! (Why start at the right instead of the left?)	HW-11 due 4/16/2025
(65)	9.2	#33 <u>Hint</u> : See Example 9.2.39.	HW-11 due 4/16/2025
(66)	9.3	#32 <u>Hint</u> : Mimic Canvas "Example: Birthday-Collision Probabilities..." using 365 instead of 366 days.	HW-11 due 4/16/2025

Row	§	Homework is from the textbook or as cited below.	Due
(67)	9.5	7(a)-(b), 10, 12, 16, 20 <u>Hints</u> : <ul style="list-style-type: none"> 9.5.7(a)-(b): We did a similar problem, 9.5.6 in class. 9.5.6 is also solved in the textbook. 9.5.12: Count separately the subsets where: (1) both elements are even, and (2) both are odd. 9.5.16: See 9.5.14 on Canvas - it similarly adds and subtracts $C(n,r)$ values. 9.5.20: See Example 9.5.19 on Canvas. 	HW-12 due 4/23/2025
(68)	9.5	Problem #27 on Practice Problems for Exam 2, calculate: $C(32,0)+C(32,1)+\dots+C(32,32)$	HW-12 due 4/23/2025
(69)	9.6	#4 <u>Hints</u> : • $C(r+n-1,r) = C(r+n-1,n-1)$ is the number of ways for selecting r objects (repetitions allowed) from among n varieties. The text differentiates r and n not so well - see page 636! <ul style="list-style-type: none"> See the solution to 9.6.3, or Question 2 in the Canvas document "Example: Roll a Die 10 Times, Tally the Numbers Shown" 	HW-12 due 4/23/2025
(70)	9.6	#13 <u>Hint</u> : See the solution on Canvas to 9.6.12 .	HW-12 due 4/23/2025
(71)	9.6	5 people are chosen at random. E is the event that <ul style="list-style-type: none"> 1 of the 5 has birthday February 29; 3 of the 5 have birthday April 1; and 1 of the 5 has birthday October 31. Assume everyone's probability is $1/366$ for being born on every date possible in a year. <u>Calculate</u> P = the probability of E . <u>Hint</u> : • Name the 5 people P,Q,R,S,T . <ul style="list-style-type: none"> The sample space is $\Omega=S \times S \times S \times S \times S$ (the Cartesian product) where S is the set of 366 possible birthdays. The 1st coordinate is P's birthday, the 2nd coordinate is Q's birthday, etc. The size of Ω is 366^5. Calculate the size of E using the MISSISSIPPI formula (page 629). 	HW-12 due 4/23/2025
(72)	9.7	#24, 34 (two Binomial Theorem problems) <u>Hint</u> : Mimic Canvas Examples 9.7.23, 9.7.33	HW-13 due 4/30/2025
(73)	9.8	#32 on Practice Exam-2 (Gambler's Exp. Val.) <u>Hints</u> : See Canvas solutions to 9.8.20, 9.8.17, 9.8.19	HW-13 due 4/30/2025
(74)	9.9	#2, #12. <u>Hints</u> : <ul style="list-style-type: none"> For #2, see the Canvas solution to 9.9.1 For #12, see the Canvas solution to 9.9.11 and/or the "viral infections" example. 	HW-13 due 4/30/2025
(75)	9.9	Exam-2 Practice Problems on Conditional Probability: #28 (Urns), #29 (voter genders). <u>Hint</u> : See Canvas solution to 9.9.11 & "Yellow Birds."	HW-13 due 4/30/2025
(76)	9.9	<ul style="list-style-type: none"> Practice Problem Exam 2 #33 (Expected Value-coin). See Class Notes on Canvas: Binomial Probabilities and ... and Example 9.9.9 on textbook pages 671-672. 	HW-13 due 4/30/2025

Syllabus & HW assignments are updated the day AFTER each lecture.

Row	§	Homework is from the textbook or as cited below.	Due
(77)	9.9	An unfair coin is flipped 8 times. The probability of landing Heads is 75% on each flip. <u>Question</u> : What is the probability of landing exactly 3 Heads? <u>Hint</u> : A similar problem is solved on pages 671-672, Example 9.9.9(a), except there the unfair coin is flipped 10 times, $P(\text{heads})=80\%$ on each flip, and it asks about having exactly 8 successes.	HW-13 due 4/30/2025
(78)	11.2	Read ahead: "Big_O_and_Algorithm Complexity_v3.pdf" (1 page + a table) in Canvas	HW-13 due 4/30/2025

Syllabus & HW assignments are updated the day AFTER each lecture.