Syllabus & Assignments: Spring 2022, INFS 501, Section 001
Discrete and Logical Structures for Information Systems

Instructor:	Prof. William D. Ellis, wellis1@gmu.edu Office Hours: By appt.
"Blackboard" Web Site:	Syllabus/HW updates, sample problems, solutions, notes etc. are delivered via Blackboard: http://mymason.gmu.edu.
Schedule:	14 Classes 7:20-10:00 PM Planetary Hall 206 • Wednesdays January 26 thru May 4, 2022 • The Final Exam will be 7:30-10:15 PM on Wednesday May 11, 2022
Prerequisite:	You'll need a working knowledge of algebra. See text pgs A1-A2.
Topics:	Logic, Set Theory, Recursion, Number Theory, Proofs, and Probability. We'll follow the textbook in this order: Chapters 5, 4, 9, 6-8, 2, and 3. We will focus on solving problems, using fundamental definitions, theorems, and algorithms. Examples include: RSA cryptography, Fibonacci numbers, birthday attacks, Benford's Law, SHA-256 hash function, and the P vs. NP problem.
Equipment:	You'll need (1) A calculator that can display 10 digits and raise numbers to powers. Really. Homework, quizzes, and exam are doable with your calculator; (2) A webcam on your home computer to use if a lecture moves on-line for a snow-closure or any other emergency. The GMU bookstore has a $30 webcam.
Textbook:	Discrete Mathematics with Applications, 5th ed. By Susanna S. Epp, ISBN-10: 1337694193; ISBN-13: 978-1337694193; Cengage (Boston MA). <u>No</u> e-book may used be during any quiz or exam, but you may print and bring pages from an e-book.
Covid-19:	Complete https://itsapps2.gmu.edu/symptom/Account/Login before coming to campus. Masks must be worn at all times in class.
Exams and Quizzes:	We will have: (i) 2 Quizzes, (ii) 2 Hour Exams, and (iii) 1 comprehensive Final Exam (Wed May 11, 2022). Exams and quizzes: • will be given only once (no makeup exams or quizzes), • will be open-book and open-notes. During exams & quizzes: • <u>No</u> partial credit for an attempt at proving a false statement. • Exam and Quiz calculations must be based on your calculator and may <u>not</u> be derived from a computer or the Internet. • Do not use or display cellphones or computers.
Homework:	H/W is assigned one day <u>after</u> each of the first 13 classes. H/W won't be accepted late. Only the 12 highest scores count in your grade. Submit on paper, or if you prefer, submit a black/white pdf on Blackboard. Free smart phone apps now produce good pdfs.
Final grade: = the weighted average of letter grades	45% Final Exam, 40% Hour Exams: 20% for each of two (2) Hour Exams, 15% Homework and 2 Quizzes: 5% each for Quizzes and for the H/W. Final Grades will be posted on Patriot Web, not on Blackboard.
For Help:	Questions? Send me an e-mail! Use the ^ symbol for exponents, * for multiplication. Or, we may chat via Blackboard Collaborate.
Honor Code:	Honor Code violations are reported to the Honor Committee. The Honor Code is at https://oai.gmu.edu/mason-honor-code/. For INFS501 this semester, submitting homework based on collaboration and/or classroom discussion is permitted.
E-mail:	Please use your GMU email account for all emails with me about your work at GMU. I will respond only to a GMU email account.

Semester Schedule

Class	Date	Event	Details and dates are subject to change
(1)	Jan 26, 2022	1s t class	
(2)	Feb 2, 2022		
(3)	Feb 9, 2022		
(4)	Feb 16, 2022	Quiz 1 & Lecture	
(5)	Feb 23, 2022		
(6)	Mar 2, 2022		
(7)	Mar 9, 2022		
	Mar 16, 2022	No Class	Spring Recess
(8)	Mar 23, 2022	Hour Exam 1 & Lecture	
(9)	Mar 30, 2022		
(10)	Apr 6, 2022		
(11)	Apr 13, 2022	Quiz 2 & Lecture	
(12)	Apr 20, 2022		
(13)	Apr 27, 2022		
(14)	May 4, 2022	Hour Exam 2 & Lecture	
(15)	May 11, 2022	FINAL EXAM	7:30-10:15 PM

Row	§	Homework is from the textbook or as cited below.		Due
(1)	1.2	#7(b),(e),(f); #9(c)-(h) (page 14) Hint: See textbook pages 7-8 and Examples 1.2.1, 1.2.4, and 1.2.8 on Blackboard.		HW-1 due 2/2/2022
(2)	5.1	7, 16, 32, 57*, 61 (pages 273-274) * #57: Simply calculate the sum for n=5. Don't bother with the part about "changing variable."		HW-1 due 2/2/2022
(3)	5.2	#23, 27, 29. (pg 288) Hint on #23: • Compare with Example 5.2.2 (pg 281) Hints on #27, 29: • Compare Example 5.2.4 (pg 285) • Try the word formula in "Notes On Defining and Summing Sequences" on Blackboard.		HW-1 due 2/2/2022
(4)	5.1	True or False? Why? "∀" means "for all."	$\sum_{k=1}^{k=n} \left(8k^3+3k^2+k\right) = n\left(n+1\right)^2\left(2n+1\right) \ \forall\, n \in \left\{1,2,3,4\right\}$	HW-1 due 2/2/2022
(5)	Note on Row (4): This problem is about understanding summation symbols and using logic - it's not about proofs. We'll see later how such a statement, if it's TRUE, may be proved by math induction.			
(6)	1.2	12 (pg 14) Hint: See the solution to 1.2.11 on Blackboard.		
(7)	5.1	83 (pg 275) Hint: See #5.1.81 on Blackboard.		
(8)	5.2	Express $S = \sum_{k=29}^{k=123} (1.6) * \left(\frac{25}{24}\right)^{-k}$ as a decimal number accurate to within .01. For example, your answer might look like "S = 52.33." Hints: • You're adding 95 actual numbers. Compute a few of them to judge the sum's approximate size. • Use Theorem 5.2.2 on page 283, or use the word-formula on page 4 of the BlackBoard pdf "Notes On Defining and Summing Sequences."		
(9)	5.6	8, 14 (pages 337) Hints: • 5.6.8 is like Example 5.5.6 on Blackboard. • 5.8.14: See hint on Blackboard and Example 5.6.13		
(10)	5.7	2(b)&(d), 4, 25 (pages 350-351) Hint: Blackboard has a hint on 5.7.2(d) plus solved examples 5.7.1(c) & 5.7.7.		
(11)	5.8	12, 14 (page 363)		
(12)	<u>Hints</u>: • #5.6.14 is like 5.6.13 solved on Blackboard.. • #5.8.12 & #5.8.14 are like the Blackboard 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). • Tips on how to factor a Characteristic Equation are in the hint to #7 on Sample Quiz 1. (Factoring is easiest using standard methods instead of using the fun recursion/Excel example from class.)			

Row	§	Homework is from the textbook or as cited below.	Due
(13)	1.3	#15(c),(d),&(e) (pg 23) Hint: We already discussed 1.3.15 in class. Also, see Example 1.3.13 on Blackboard.	
(14)	4.1	4, 9, 13(b) (pages 171-172) Hint #4.1.13(b) is similar to #4.1.14 on Blackboard	
(15)	4.2	2, 9, 13, 19, 27 (page 181-182). Hints: • For 4.2.9: (i) Call the given integer n. (ii) Use the hypothesis on n (i.e., the information given on n) to write an equation: (n-1) = ... (iii) Now factor (n-1). (iv) Explain, like in 4.2.14, why each factor > 1, thereby showing (n-1) cannot prime. • 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 Blackboard pdf "Bogus proof that 8=10." • For 4.2.13: See the 4.2.14 solution on Blackboard	
(16)	4.3	7 (pg. 187) Hint: Mimic 4.3.6 solved on Blackboard.	
(17)	4.1 4.2 4.3	Hint: For §§ 4.1-4.2, use the even-odd definitions on page 162, NOT the familiar even/odd properties shown on pages 186-187 (in § 4.3). They are derived from the page-162 definitions too!	
(18)	4.3	28 (page 188)	
(19)	4.4	28, 41 (pages 198-199)	
(20)	4.5	6, 21 (pages 209-210) Hint: #21 is like #4.5.25 on Blackboard.	
(21)	4.10	16, 23(b). For 23(b), see the Hint on Blackboard. Also, syntax isn't important in 23(b). In plain English, describe in separate bullets this algorithm's: • input, • action (what it does with the input), and • output.	
(22)	4.10	Calculate GCD(98741, 247021)	
(23)	4.10	Observe: $247{,}710^2 - 38{,}573^2$ = 61,360,244,100 - 1,487,876,329 = 59,872,367,771 = 260,867*229,513. Now factor 260,867 in a non-trivial way. Blackboard has a hint, and the spreadsheet "Excel: Euclidean Algorithm" may ease your calculations.	
(24)	4.10 5.8	Write the Fibonacci no. F_{400} in scientific notation, e.g. $F_{30} \approx 1.35*10^6$. Use Epp's definition $F_0=1$, $F_1=1$, ... on page 333. Or the Problem 5.6.33 formula (pg 339). Beware: The Fibonacci numbers are sometimes indexed differently on-line as $F_1=1$, $F_2=1$, $F_3=2$, … .	

Row	§	Homework is from the textbook or as cited below.	Due
(25)	6.1 6.2	Sample Exam 1 problem #1 Hint: • See the SE1 #6 solution under Blackboard Week 6.	
(26)	6.3	(pg 413) #24(d)-(f) (pg 413)	
(27)	9.1	#4, #8, #14(b)-(c) (page 571). # redo #14(b)-(c) assuming the infection probabilities are 30% for Mr. A, 60% for Mr. B, and 40% for Mr. C. Hints: Mimic Blackboard Examples 9.1.3, 7, 10, 12.	
(28)	9.2	#7, #17(a)-(d), #33, #36 Hints: • #7: See BB Example 9.2.6, or 9.2.6 Alternate Solution. • #17 is like BB Example 9.2.12, but more advanced. It should help to visualize the choices in a possibility tree. • #17(d) is tricky! First choose the rightmost digit (5 choices); then the leftmost (8 choices)! [Why start at the right instead of the left?] • #33, #36: See the formula on page 582 and the solutions to #35 and #39 on Blackboard.	
(29)	9.3	#32 Hint: See Blackboard "Example: Birthday-Collision Probabilities (based on 366 days)."	
(30)	7.2	The birthday hash-function BD: {All people} -> {1,2,...,366} by mapping x -> the 3-digit Julian date of x's birthday. For example, BD(x)=61 if x is born on March 1, 2020; and BD(x)=60 if x is born on March 1, 2021. Question: The BD function produces a "collision" for which 2 members of this subset of the domain: {Charles Darwin, Albert Einstein, Mahatma Gandhi, Abraham Lincoln}?	
(31)	9.5	7(a)-(b), 10, 12, 16, 20 Hints: • 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: 9.5.14 on Blackboard similarly adds and subtracts C(n,r) values. • 9.5.20: See Example 9.5.19 on Blackboard.	
(32)	9.6	#4 Hint: • 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 the theorem on page 636! • See the Blackboard solution to 9.6.3.	
(33)	9.6	#13 Hint: See the Blackboard solution to 9.6.12.	

Row	§	Homework is from the textbook or as cited below.	Due
(34)	9.7	#24 Hint: Mimic Blackboard Example 9.7.23	
(35)	9.7	#27, 34. Hint: See Examples 9.7.26, 9.7.32, 9.7.33	
(36)	9.7	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>: Read "Binomial Probabilities and Expected Values" on Blackboard	
(37)	9.8	Sample Quiz 2 problem #4 Expected Value (binomial).	
(38)	9.8	Read "Expected Value of a Binomial Distribution" on Blackboard. Then do problem #3 on Sample Quiz 2.	
(39)	9.8	#17, #20 (textbook); #6 (Sample Quiz 2 - geometric random variable). <u>Hints</u>: Mimic 9.8.18, or 9.8.19.	
(40)	9.9	#2, #12. Hints: • For #2, see the Blackboard solution to 9.9.1 • For #12, see the Blackboard solution to 9.9.11 and/or the "viral infections" example.	
(41)	9.9	Do problem #4 on Sample Quiz #2. Hint: It's similar to the "yellow birds" example in Blackboard/Week 8.	
(42)	6.1	#7b; #10(f)-(h); #12(a),(b),(g),(h),(j) (pg 388) Hints: • #7,#10: See 6.1.4, 6.1.10(a)-(e) on Blackboard. • #12: Simplify with Interval Notation (page 382). • #12(g): You may use #12(a) and De Morgan laws § 6.2 (pg 395). Epp puts this problem in § 6.1 so we appreciate the De Morgan laws when we get to § 6.2.	
(43)	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?	
(44)	6.2	#13. Prove ∀ sets A, B, C, $(A-B)\cup(C-B)=(A\cup C)-B$. Use any of the 3 methods of proof in Example 6.2.9.	
(45)	6.3	#2, #4, #7 Hints: • Hints for 6.3.2, 6.3.4 are on Blackboard. • Venn-Diagram shading is not acceptable. Shading alone is usually confusing & unconvincing. • Numbered Venn-Diagram regions are good - they're best for verifying or finding a counterexample to a "∀ sets" identity. See Examples 6.2.9(I) and 6.3.5. • An "is-an-element-of" proof [like the HW-8 solution to 6.1.7(b)] will also verify a "∀ sets" identity. But, "is-an-element-of" proofs are often confusing., e.g. see version (iii) in Example 6.2.9	

Row	§	Homework is from the textbook or as cited below.	Due
(46)	6.3	Prove or disprove each of these 2 Claims: • ∃ sets A, B & C such that (A-B)-C=(A-C)-(B-C), • ∀ 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 not use Venn-Diagram shading. Hint: • See the 6.3.13 Example on Blackboard.	
(47)	7.1	#2. Hint: See the solution to #1 on page A-72.	
(48)	7.1	#5; #12, #51(d),(e), and (f) (pgs 436-439) Note: #51 Will be used in RSA encryption.	
(49)	7.2	13, 17 Hint: Use the "1-1" definition on page 440; mimic the solutions to Example #16, #18 on Blackboard.	
(50)	7.3	2, 14 Hint on #14: See Blackboard Example 7.3.4.	
(51)	7.3	Do #11 on Sample Quiz-2. Hint: See "Example: Composition of Functions in Blackboard/Week 9.	
(52)	1.3	• Read the definition of "relation from A to B" and the Example on pg 16. Every one of the arrow diagrams in 1.3.15 (HW-3) represents relations. • Do #4 (pg 22) Hint: #4 is like 1.3.3, which is solved on Blackboard.	
(53)	7.3	#20. Hint: Drawing a picture could help.	
(54)	8.1	#3(c)-(d). (page 493) Hint: See 8.1.1, solved on Blackboard.	
(55)	8.2	#11 (page 503). Hint: See the solution to 8.2.10 on Blackboard	
(56)	8.3	#9 [Call 0 = the sum of the elements in φ.]; #15(b),(c),(d) (page 521) Hints: • #9 See Blackboard Examples 8.3.8, 8.3.10, 8.3.12 • #15: Use modular-equivalence definition on pg 518	
(57)	8.4	• #2, #4, #8 (page 544). Hints: • 8.4.4 is like Example 8.4.3 • 8.4.8 is like Example 8.4.7	
(58)	8.4	# Calculate 2^{373} (mod 367).	
(59)	8.4	#9 on Sample Exam 2 (Find the remainders when x =83415754463525152283 is divided by 11 & 9.) Hint: See Examples 8.4.12b & 8.4.13b on Blackboard	
(60)	8.4	#17, #18 Hint: See Blackboard solutions, to 8.4.16 and Line (58). These are for RSA examples 8.4.37,38,40. We often need successive squaring even if we can factor the public-modulus (713).	

Row	§	Homework is from the textbook or as cited below.	Due
(61)	8.4	#20 Hint: See Example 8.4.21 on Blackboard. Convert WELCOME into a string of integers like in 8.4.2. Next, reduce each integer x -> e(x) = x^3 (mod 55), e.g., L -> 12 -> 12^3 ≡ 23 (mod 55). This problem mimics Example 8.4.9 on page 537.	
(62)	8.4	#37 This problem is like 8.4.20, only we convert COME into a string of integers like in 8.4.2. Next, reduce each integer x -> e(x) = x^43 (mod 713), e.g., C -> 3 -> 3^43 ≡ 675 (mod 713).	
(63)	8.4	Solve for x: 1014*x ≡ 7 (mod 4,157), 0 ≤ x ≤ 4,156. <u>Hint</u>: See the Blackboard Examples: (1), 8.4.27, or (2) Solve 122x = 9 (mod 7919), or (3) Solving 136y = 14 (mod 7919).	
(64)	8.4	#38 <u>Hint</u>: This problem is like Line (63), only now we're asked to solve 43*x≡1 (mod 660). Inverting (mod 660) is how RSA engineers decryption (mod 713) (public). So, it's an RSA secret that 660 = φ(731)!	
(65)	8.4	#40 (page 545) <u>Hints</u>: Text Example 8.4.10 (pg 538) and problem 8.4.23 on Blackboard decrypt x -> d(x)≡x^27 (mod 55)-> letter equivalent. #40 is like 8.4.23, but here the public modulus is 713 = 23*31 & encryption e(x)=x^43. φ(713) = 22*30 = 660 is the secret Little Fermat modulus. 307 is the secret decryption exponent because we solved 43*307 ≡1 (mod 660) in 8.4.38.	
(66)	8.4	Find the RSA decryption exponent d when: p=13, q=17, n=221, and e=37 is the encryption exponent. <u>Hint</u>: See "Creating an RSA Encryption-Decryption Pair..." on Blackboard	
(67)	8.4	Solve for x: x^2 ≡ 4 (mod 675,683). Give all 4 solutions - they should all be between 0 & 675,682. Use 675,683 = 821 * 823, the product of 2 primes. <u>Hint</u>: Solve 821*x + 823*y = 1. Then an easy trick gives solutions to x^2 ≡ 1 (mod 675,683), x ≠ 1. See Blackboard Example: Calculating 4 Square roots (mod pq). This problem shows unusual square roots exist under a composite modulus. Finding the unusual roots is the hard part. Those unusual roots allow factoring the RSA modulus as in row (23) above, so an RSA-cracker may solve d = e^{-1} (mod (p-1)(q-1)). We'll also see how to factor a modulus using a "birthday attack."	
(68)	2.1	15, 37 (pgs 52-53) <u>Hints</u>: •#43 is like #2.1.41 on Blackboard. •#37 is like #2.1.33 on Blackboard.	

Row	§	Homework is from the textbook or as cited below.	Due
(69)	2.2	4, 15, 27 (pgs 63-64). Hint on 2.2.4: See the Blackboard solution to problem #7 on Sample Exam-2.	
(70)	2.2	See Blackboard Week #12 for a little HW problem on a Satisfiability ("SAT") problem.	
(71)	4.5	Suppose we are given an integer x. Now call the statement *s* = "$(x^2$-x) is exactly divisible by 3." Choose exactly one of the answers A, B, or C and: (A) Prove s is TRUE; or (B) Prove s is FALSE; or (C) Explain why (A) and (B) are impossible.	
(72)	2.2	See Blackboard Week #13 for a HW problem on Informal English.	
(73)	2.3	11 (pg 77) Hints: • This problem is like 2.3.9 and Sample Exam-2 #4, already solved on Blackboard. • Epp's shortcut vs. the common-sense method for determining validity are compared in the Blackboard pdf "Truth Tables, Arguments Forms & Syllogisms," Table 5.	
(74)	3.1	18(c)-(d); 28(a)&(c); 32(b),(d) (pgs 119-121) • Hint for 3.1.18(c)-(d): See "Example 3.1.18 (a),(b),&(e)" on Blackboard.	
(75)	3.2	#10, 25(b)-(c), 38 (pages 130-131). Also, • ∀ and ∃ are the only quantifiers that may be used. Do not put any slashes through a quantifier, e.g. do not us a ∄. • No negation symbol (¬) may appear outside a quantifier or an expression involving logical connectives, e.g. instead of "¬(∀x.(P(x)->Q(x)))," write "∃x.(P(x)∧¬Q(x))." Hint On #38: *Discrete Mathematics* refers to the phrase "Discrete Mathematics," not to the entire subject of Discrete Mathematics.	
(76)	3.3	Let s := (∀x.(P(x)∧∃y∃z.Q(x,y,z))) -> (∃x∃y.R(x,y)). Negate s and simplify ¬s so: • No negation symbol (¬) appears outside a quantifier or an expression involving logical connectives. • Use only the ∀ and ∃ quantifiers. Do not put any slashes through a quantifier, e.g. do not us a ∄. Hint: See "Example: Negating a Multiply-quantified statement" on Blackboard.	
(77)	3.3	#41(c),(d),(g),(h) (page 145) Hints: See "Order of Quantifiers," textbook pg 128	