Syllabus & Assignments: Spring 2021, INFS 501, ON-LINE Section 001
Discrete and Logical Structures for Information Systems

Instructor:	Prof. William D. Ellis E-mail: wellis1@gmu.edu Class will be entirely ON-LINE. Office Hrs: By appointment.
"Blackboard" Web Site:	Lectures, syllabus/HW updates, sample problems, solutions, notes etc. are delivered via Blackboard: http://mymason.gmu.edu.
Schedule:	• Lectures begin 1/27/2021 on Blackboard/Collaborate Ultra. • 14 lectures 7:20-10:00 PM, Wednesdays 1/27-4/28/2021. • The Final Exam is Wednesday May 5, 2021 from 7:30-10:15 PM.
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.
Calculator:	You'll need a calculator that can display 10 digits and raise numbers to powers. Calculations for homework, quizzes, and exams are designed around and doable with your calculator. We won't need to learn any software, but I'll use software in lectures.
Textbook:	Discrete Mathematics with Applications, 5th ed. Susanna S. Epp, ISBN-10 1337694193; ISBN-13 978-1337694193; Cengage (Boston MA).
Submit course work in pdfs:	Each Exam, Quiz, and Homework assignment should be submitted in a single pdf via its link in Blackboard. At least 3 different software vendors offer free smart-phone apps that scan to pdf.
Exams and Quizzes:	• We will have: (i) 2 Quizzes, (ii) 2 Hour Exams, and (iii) a comprehensive Final Exam (Wed May 5, 2021). Exams and Quizzes: • will be given only once (no makeup exams), • will be open-book and open-notes, • No partial credit for an attempt at proving a false statement. • Exam and Quiz calculations must be based on your calculator and may not be derived from a computer or the Internet.
Homework:	H/W is assigned one day after each of the first 13 classes. H/W won't be accepted late. Only the 12 highest scores count in your grade. View pdf's, H/W scores, and any comments on Blackboard.
Final grade is 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 go on Patriot Web. Blackboard shows H/W scores only.
Help:	Questions? Send me an e-mail! Use the ^ symbol for exponents, * for multiplication. You may also e-mail a pdf or scanned image.
Honor Code:	Honor Code violations are reported to the Honor Committee. The Honor Code is at https://oai.gmu.edu/mason-honor-code/.
E-mail:	You must use your GMU email account for all emails about your work at GMU. You may forward your campus email elsewhere, but I will respond only to a GMU email account.

Syllabus & HW assignments are posted after each class. Rev 1/13/2021 5:00 PM

Semester Schedule

Class	Date	Event	Details and dates are subject to change
(1)	Jan 27, 2021	1st class	
(2)	Feb 3, 2021		
(3)	Feb 10, 2021		
(4)	Feb 17, 2021		
(5)	Feb 24, 2021	Quiz 1 & Lecture	
(6)	Mar 3, 2021		
(7)	Mar 10, 2021		
(8)	Mar 17, 2021	Hour Exam 1 & Lecture	
(9)	Mar 24, 2021		
(10)	Mar 31, 2021		
(11)	Apr 7, 2021	Quiz 2 & Lecture	
(12)	Apr 14, 2021		
(13)	Apr 21, 2021		
(14)	Apr 28, 2021	Hour Exam 2 & Lecture	
	May 5, 2021	FINAL EXAM	7:30 - 10:15 PM

Row	§	Homework is from the textbook or as cited below.	Due
(1)	1.2	#4; #7(b),(e),(f) (page 14) Hints: See the Examples on pages 7-8.	HW-1 due 2/3/2021
(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. + #61: The product symbols here require multiplying the first n terms in the given sequences.	HW-1 due 2/3/2021
(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 the "pdf Notes On Defining and Summing Sequences" on Blackboard.	HW-1 due 2/3/2021
(4)	5.1	False or True" Why? "∀" means "for all." $\sum_{k=1}^{n}(8k^3+3k^2+k)=n(n+1)^2(2n+1)\forall n\in Z^+$	HW-1 due 2/3/2021
(5)	Hints on Row (4): • Such a claim would be proven FALSE by finding even one "counter-example," i.e. an example of an n for which the formula fails. • A shortcut (not a proof) for verifying a formula like this is check it for 5 (=3+2) different values of n. Here 3 = the highest power of k in ($a_k = 8k^3+3k^2+2$). Always check 2 more values than the highest power of k. This shortcut works because 1 + the degree in k of the terms on the left (1+3) equals the degree of the right side in n (4). • This problem is about summations and basic logic. Proofs come later.		
(6)	1.2	#9(c)-(h). Hint: See Example 1.2.8 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 with at least two decimal digits of accuracy. 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 "pdf Notes On Defining and Summing Sequences" on BlackBoard.	
(9)	5.6	8, 14 (pages 337) Hint: #5.6.13 on Blackboard is similar to #5.6.14.	
(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)	

Row	§	Homework is from the textbook or as cited below.	Due
(12)	Hints: • #5.6.14 is like 5.6.13 solved on Blackboard.. • #5.8.12 & #5.8.14 are like the problems #6 and #8 on Sample Quiz 1. • #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 usually easiest using standard methods instead of using the fun method we saw using recursion.]		
(13)	1.2	12. Hint: See 1.2.11 as solved 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, 13, 19, 27 (page 181-182). Hints: • On 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." • On 4.2.13: See the 4.2.14 solution on Blackboard.	
(16)	4.1, 4.2	Hint: In (14)-(15), use the even/odd definitions on page 162. Do not use the familiar even/odd properties listed on pages 186-187 (§ 4.3) - they are derived from the page 162 definitions too!	
(17)	4.3	7 (pg. 187) Hint: Mimic 4.3.6 solved on Blackboard.	
(18)	1.3	#15(c),(d),&(e). #17 (pg 23)	
(19)	4.3	28 (page 188)	
(20)	4.4	28, 41 (pages 198-199)	
(21)	4.5	6, 21 (pages 209-210) Hints: #21 is like #4.5.25 on Blackboard.	
(22)	4.10	16, 23(b) (pages 255-256) On 23(b), don't worry about syntax. To describe this algorithm, just state: (i) its input, (ii) what it does, and (iii) its output.	
(23)	4.10	Find GCD(98741, 247021)	
(24)	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.	
(25)	6.3	#24(d)-(f) (pg 413)	
(26)	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: Some online calculators start the Fibonacci numbers at $F_1=1$, $F_2=1$, $F_3=2$, … .]	

Row	§	Homework is from the textbook or as cited below.	Due
(27)	9.1	#4, #8, #14(b)-(c) (page 571). Also 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 #3, #7, #10, #12.	
(28)	9.2	#7, #12, #17(a)-(d), #33, #36 Hints: • #7: See Example 9.2.6 on BB. You may instead find the 9.2.6 "Alternate Solution" easier. • #17(a)-(c): Build a possibility tree starting at the leftmost digit. But 17(d) is tricky! First choose the rightmost digit (5 choices). Choose second the leftmost (8 choices),… [Why would starting at the left be bad?] • #33, #36: See the formula on page 582 and the solutions to #35 and #39 on Blackboard.	
(29)	1.2, 6.1, 6.3	Sample Exam-1 #16.	
(30)	9.3	#32 Hint: See Blackboard "Example: Birthday-Collision Probabilities (based on 366 days)."	
(31)	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}?	
(32)	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.	
(33)	9.6	#4, #13 Hints: • See the Blackboard solutions to 9.6.3 and 9.6.12 • 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. Be careful, the theorem on page 636 doesn't differentiate r and n very clearly!	
(34)	9.6	Suppose we expand (a+b+c+d+e+f+g)^44 and consolidate the terms into "monomials" where the variables' exponents all match. This is the "multinomial expansion." Question: How many of these terms (monomials) are in this multinomial expansion?	
(35)	9.7	#27, 32, 34. Hint: See Examples 9.7.23, 9.7.26	

Row	§	Homework is from the textbook or as cited below.	Due
(36)	9.7	Suppose an unfair coin is flipped 8 times. 75% = the probability of landing Heads on each flip. What is the probability of landing exactly 3 Heads? Hint See Blackboard, "Example of Binomial Trials: Flipping fair and unfair coins."	
(37)	9.9	#2, #12. Hints: • See the Blackboard solutions to #1 for #2. • For #12, see the Blackboard solutions to #11 and/or the "viral infections" example.	
(38)	9.9	Do problem #4 on Sample Quiz #2. Hint: It's similar to the "yellow birds" example on Blackboard.	
(39)	9.6 9.7	#5 (Sample Quiz 2). Hint: See "Multinomial Probability Example" on Blackboard.	
(40)	9.7 9.8	Read "Binomial, multinomial probability; Expected Value of a Binomial Distribution" on Blackboard	
(41)	9.8	#17, #20 (textbook); #6 (Sample Quiz 2). Hints: Mimic 9.8.18, or 9.8.19, or the example in "Binomial, multinomial probability; Expected Value of a Binomial Distribution" on Blackboard	
(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 on page 395. Epp places #12(g)-(j) 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. However, "is-an-element-of" proofs are often confusing to read. See Example 6.2.9(III).	

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, #5; #12, #51(d),(e), and (f) (pgs 436-439) Note: #51 Will be used in RSA encryption.	
(48)	7.2	13, 17 Hint: Use the "1-1" definition on page 440; mimic the solutions to Example #16, #18 on Blackboard.	
(49)	7.3	2, 4, 14 On #14 see the Blackboard Hint: Calculate H(H(x))	
(50)	1.3	#4 Hint: Example 1.3.3	
(51)	8.1	#3(c)-(d). (page 493) Hint: See 8.1.1, solved on Blackboard.	
(52)	8.2	Read page 17 about the Circle relation. #10 (page 503). A big Hint is on Blackboard.	
(53)	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	
(54)	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	
(55)	8.4	# Calculate 2^{373} (mod 367). [Hint: If it matters, 2, 367, and 373 are all prime numbers.]	
(56)	8.4 pg 544	12b, 13b [Hint: For a 3-digit number x, if we call x's hundred's digit = "h," the tens digit "t," and the unit's digit "u," then in base-10 x is htu_{10} = h*10^2+t*10+u. For 12b, reduce (mod 9) using 10≡1 (mod 9). For 13b, reduce (mod 11) using 10 ≡ -1 (mod 11). The same approach works no matter how many base-10 digits a positive integer x has.	
(57)	8.4	#20, 23, 38, 40. (page 545) Hints: For #20, 23: Use text Examples 8.4.9-10 (mod 55): • For encryption e(x), Epp randomly chose exponent = 3, so e(x)=x^3, e(8)=8^3 ≡ 17 (mod 55). • d(x) = x^27 decrypts: d(17)= 17^27 ≡ 8 (mod 55) • The pair {e,d}={3,27} reverse each other because: (1) 3*27=1 (mod 40), where 40=φ(55)=(5-1)*(11-1), (2) 40=φ(55) is the Little Fermat exponent. For #40: Modulus = 713 = 23*31, 660 = φ(713)=22*30, encryption e(x)=x^43. 43*307≡1 (mod 660), from #38. So both pairs (e=43,d=307) and (e=307,d=43) work equally well for encryption-decryption (mod 713).	

Row	§	Homework is from the textbook or as cited below.	Due
(58)	8.4	Solve for x: 1014*x ≡ 7 (mod 4,157), 0 ≤ x ≤ 4,156. Hint: See the examples "Solve 122x = 9 (mod 7919)" or "Solving 136y = 14 (mod 7919)" on Blackboard.	
(59)	8.4	Find the RSA decryption exponent d when: p=13, q=17, n=221, and e=37 is the encryption exponent. Hint: See "Creating an RSA Encryption-Decryption Pair..." on Blackboard	
(60)	8.4	HW: x = 63826456536845958448. What is the remainder when x is divided by 11?	
(61)	8.4	Solve for x: $x^2 \equiv 4 \pmod{675,683}$. Give all 4 solutions - they should be between 0 & 675,682. Use 675,683 = 821 * 823, the product of 2 primes. Hint: Solve 821*x + 823*y = 1. Then an easy trick gives solutions to $x^2 \equiv 1 \pmod{675,683}$, $x \neq \pm 1$. See Blackboard "Example: Calculating 4 Square roots (mod pq)." This example shows multiple square roots always exist if the modulus is composite. Multiple square roots enable factoring an RSA modulus as in Row (24) above. RSA is attacked by finding multiple square roots mod the public modulus n. Factoring n = p*q is the hard part. Afterward, an RSA-cracker simply needs to solve $d = e^{-1} \pmod{(p-1)(q-1)}$.	
(62)	2.1	15, 37, 43 (pgs 52-53) Hints: #43 is like #2.1.41 on Blackboard. #37 is like #2.1.33 on Blackboard.	
(63)	2.2	4, 15, 27 (pgs 63-64) Hint on 2.2.4: See the solution to Sample Exam 2 #7	
(64)	2.2	See Blackboard Week #12 for a small HW problem on Satisfiability ("SAT"). The problem of determining whether SAT has a "polynomial time" solution is the million-dollar "P vs. NP" problem.	
(65)	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	
(66)	2.2	See Blackboard week #13 for a HW problem on Informal English.	
(67)	2.3	9, 11 (pg 77) Hints: • These problems are like Sample Exam-2 #4. • Epp's shortcut method and the common-sense method for determining validity are compared in Table 5 of "Truth Tables, Arguments Forms & Syllogisms."	
(68)	3.1	12, 18(c)-(d), 28(a)&(c), 32 (pgs 119-121) For 3.1.18(c)-(d): • See "Example 3.1.18 (a),(b),&(e)" on Blackboard.	

Row	§	Homework is from the textbook or as cited below.	Due
(69)	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 <u>not</u> 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))." <u>Hint</u> On #38, *Discrete Mathematics* refers to the phrase "Discrete Mathematics," <u>not</u> to the entire subject of Discrete Mathematics.	
(70)	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 <u>not</u> us a ∄. <u>Hint</u>: See "Example: Negating a Multiply-quantified statement" on Blackboard.	
(71)	3.3	#41(c),(d),(g),(h) (page 145) Hints: (1) See "Order of Quantifiers" on textbook page 138. (2) The solution to Sample Final Exam #32 (L(x,y) := "x loves y," on Blackboard) may also help.	
(72)	9.1	#20 (Modified Monty Hall) <u>Hints</u>: • #14 Mimic Example 9.1.12 on Blackboard • #20: The first guess will be correct 1/5 (20%) of the time. If we switch, the remaining 80% chance of success must still be divided among 3 doors.	