Syllabus & Assignments: Fall 2020, 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 8/24/2020 on Blackboard/Collaborate Ultra.
- 14 lectures 7:20-10:00 PM, Mondays 8/24-11/30, except Tuesday 10/13 instead of 10/12, and September 7 is Labor Day Holiday.
- The Final Exam is Monday 12/14/2020 from 7:30-10:15 PM.

Prerequisite: You'll need a working knowledge of algebra. See text pgs A1-A2.

Topics: Logic, Set Theory, Proofs, Probability, Recursion, and Number Theory. We'll follow the textbook in this order: Chapters 5, 9, 4, 6-8, 2, and 3. We will focus on solving problems, using fundamental definitions, theorems, and algorithms. Examples include: P vs. NP problem, Fibonacci numbers, Benford's Law, birthday attacks, SHA-256 hash function, and RSA cryptography.

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 class.

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 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 (Mon 12/14/2020). Exams and Quizzes:
- will be given only once (no makeup exams),
- will be open-book and open-notes,
- No partial credit for purportedly 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 will be assigned one day after each of the first 13 classes. The 12 highest scores count toward your grade. View your pdf's and my comments, if any, in Blackboard/Grade Center.

Final Grade (weighted average)
- 45% Final Exam
- 38% Hour Exams (19% on each of two (2) hour exams)
- 12% Homework and 2 Quizzes (4% homework and each quiz)
- 5% Class participation (for on-line semesters 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.

Semester Schedule

Class	Date	Event	Details and dates are <u>subject to change</u>
(1)	Aug 24, 2020	1st class	
(2)	Aug 31, 2020		
	Sep 7, 2020	** No class	Labor Day Holiday
(3)	Sep 14, 2020		
(4)	Sep 21, 2020		
(5)	Sep 28, 2020	Quiz 1	
(6)	Oct 5, 2020		
(7)	Oct 13, 2020	Tuesday!	Class delayed 1 day for Fall Break
(8)	Oct 19, 2020	Exam 1	
(9)	Oct 26, 2020		
(10)	Nov 2, 2020		
(11)	Nov 9, 2020	Quiz 2	On everything covered through HW#7-#9.
(12)	Nov 16, 2020		
(13)	Nov 23, 2020		
(14)	Nov 30, 2020	Hour Exam 2 & Lecture	
	Dec 14, 2020	FINAL EXAM	The Final Exam will cover everything we covered during the entire semester. Problems will be like in the Exams, Quizzes, Sample Exams, Sample Quizzes, and the problems identified in the Homework table below.

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 8/31/2020
(2)	5.1	7, 13, 16, 32, 57*, 61 (pages 273-274) * On #57, simply calculate the sum for n=5. Don't bother with the part about changing variable.	HW-1 due 8/31/2020
(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 8/31/2020
(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 8/31/2020
(5)	Hints on Row (4): • Such a claim would be proven FALSE by finding even one counterexample, i.e. find one example of an n where the formula fails. • A shortcut (not a proof) for verifying such a formula 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.		
(6)	1.2	#9(c)-(h)	HW-2 due 9/14/2020
(7)	5.1	83 (pg 275) Hint: See #5.1.81 on Blackboard.	HW-2 due 9/14/2020
(8)	5.2	Express $S=\sum_{k=29}^{k=123}(16)*\left(\frac{25}{24}\right)^{-k}$ 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. • This like Sample Quiz-1 #4 solved on Blackboard.	HW-2 due 9/14/2020
(9)	5.6	8, 14 (pages 337) Hint: #5.6.13 on Blackboard is similar to #5.6.14.	HW-2 due 9/14/2020
(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.	HW-2 due 9/14/2020
(11)	5.8	12, 14 (page 363)	HW-2 due 9/14/2020

Row	§	Homework is from the textbook or as cited below.	Due
(12)	Hints: • #5.8.12 & #5.8.14 are like the problems #6 - #7 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 solution to #7 on Sample Quiz 1.		
(13)	1.2	12	
(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). <u>Hints</u>: • 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 "Bogus proof that 8=10" on Blackboard. • On 4.2.13: See the 4.2.14 solution on Blackboard.	
(16)	4.1, 4.2	<u>Hint</u>: In (14)-(15), use the even/odd definitions on page 162. <u>Do not use</u> the familiar even/odd properties listed on pages 186-187 (§ 4.3) - they are derived from the page 162 definitions too!	
(17)	1.3	#15(c),(d),&(e); #17. (pg 23)	
(18)	6.3	24(d)-(f) (pg 413)	
(19)	4.4	28, 41 (pages 198-199)	
(20)	4.5	6, 21 (pages 209-210) Hints: #21 is like #4.5.25 on Blackboard.	
(21)	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.	
(22)	4.10	Find 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 297. Or the Problem 5.6.33 formula (pg 339). [Beware: Some online calculators start the Fibonacci numbers at $F_1=1$, $F_2=1$, $F_3=2$, … .]	
(25)	9.1	4, 8 (page 571) <u>Hints</u>: Mimic Examples #3, #7, and #10 on Blackboard.	

Row	§	Homework is from the textbook or as cited below.	Due
(26)	9.2	#7; #12; #17(a)-(d); #33; #36 Hints: • #7: See the Blackboard solution to #6. to #6, based on a smaller sample space. • #17(a)-(c): Build a possibility tree starting at the leftmost digit. But on 17(d): Start at the rightmost digit (5 choices), then 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.	
(27)	9.1	#14(b)-(c); #20 (Modified Monty Hall) Hints: • #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.	
(28)	9.3	#32 Hints: • A frequency-distribution tree shows 365^n = the size of the sample space for n peoples' birthdays. The subset of paths with no matches has size: 365*364 if n=2; 365*364*363 if n=3,... What value of n makes the probability fall below 50%? • See Blackboard "Example: Birthday-Collision Probabilities (based on 366 days)."	
(29)	9.5	7(a)-(b), 10, 12, 16, 20 Hints: • 9.5.7(a)-(b): See the textbook's solution to #9.5.6, and the solution to Sample Exam 2 #11 • 9.5.10: We did this one in class. • 9.5.12: Count separately the subsets where: (1) both elements are even, and (2) both are odd. • 9.5.16: See the solution to Sample Exam 2 #11. • 9.5.20: See Example 9.5.19 on Blackboard.	
(30)	9.5	Solve Sample Exam 2 #30: What is the probability of receiving exactly 2 aces when drawing 5 cards from a standard 52-card deck? Hint: Count the ways to choose (1) 2 aces, (2) the remaining 3 cards, (3) all hands with 2 aces, and (4) all poker hands.	
(31)	9.6	#4, #13	
(32)	9.6	Suppose we expand (a+b+c+d+e+f+g)^44 and collect together every term where the variables' exponents all match. This is the "multinomial expansion." How many monomials are in this multinomial expansion?	
(33)	9.7	#27, 32, 34. Hint: See Examples 9.7.23, 9.7.26	
(34)	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 "Example of Binomial Trials: Flipping fair and unfair coins" on Blackboard.	
(35)	9.8	#17. Hint: See 9.8.18 & 9.8.19 on Blackboard.	
(36)	9.9	#11, #15	

Row	§	Homework is from the textbook or as cited below.	Due
(37)	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): Use #12(a) and De Morgan laws (pg 395). [Epp places #12(g)-(j) in § 6.1 so we appreciate the De Morgan laws when we see them in § 6.2.]	
(38)	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?	
(39)	6.2	#13. Prove (A-B)∪(C-B)=(A∪C)-B using any of the 3 methods of proof in Example 6.2.9 on Blackboard.	
(40)	6.3	#2, #4, #7, #21 Hints: • Hints for 6.3.2, 6.3.4 are on Blackboard. • Venn-Diagram shading is <u>not</u> acceptable. Shading alone is usually confusing & unconvincing. • <u>Numbered</u> Venn-Diagram regions are 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 will also verify a "∀ sets" identity. However, such proofs are often confusing. See Examples 6.2.9(III) and 6.3.20.	
(41)	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 <u>not</u> use Venn-Diagram shading.	
(42) (43)	7.1 7.2	#2, #5; #12, #51(d),(e),&(f) (pgs 436-439) <u>Note</u>: #51 Will be used in RSA encryption. 13, 17 Hint: See the solutions to #16, #18 on Blackboard.	
(44)	7.3	Study Blackboard Example: Composition of Functions	
(45)	7.3	2, 4, 14 On #14 see the Blackboard Hint; Calculate H(H(x))	
(46)	1.3	#4 Hint: See Week 5/Example 1.3.3	
(47)	7.2	#Solve "H/W-9 Hash Function Problem" on Blackboard	
(48)	8.1	#3(c)&(d). (page 493) Hint: See 8.1.1, solved on Blackboard.	
(49)	8.2	Read page 17 on the Circle relation. #10 (page 503). See the <u>Hint</u> on Blackboard.	

Row	§	Homework is from the textbook or as cited below.	Due
(50)	8.3	#9 [Call 0 = the sum of the elements in φ.]; #15(b),(c),(d) (page 521) Hints: • #9 See Blackboard Examples 8.3.10 and 8.3.8. • #15: Use modular-equivalence definition on pg 518	
(51)	8.4	Study Example 8.4.7 on Blackboard. It shows the power and ease of using modular arithmetic. #2, #4, #8 (page 544) Hints: • 8.4.4(e) wants us to note: [68≡7 (mod 7), by Defn pg 518] => [68 mod 7 = 33 mod 7, by Thrm pg 526] • 8.4.8 is like Example 8.4.7	
(52)	8.4	# Calculate 2^{373} (mod 367). [Hint: If it matters, 2, 367, and 373 are all prime numbers.]	
(53)	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.	
(54)	8.4	#20, 21, 23, 37, 38, 40. (page 545) <u>Hints</u>: For #20,21,23: 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 (<u>mod 55</u>). • 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 (<u>mod 40</u>), where 40=φ(55)=(5-1)*(11-1), (2) 40=φ(55) is the Little Fermat exponent. For #40: <u>Modulus = 713</u> = 23*31, 660 = φ(713)=22*30, encryption e(x)=x^43. 43*307≡1 (<u>mod 660</u>), from #38. So both pairs (e=43,d=307) and (e=307,d=43) work equally well for encryption-decryption (mod 713).	
(55)	8.4	Solve for x: 1014*x ≡ 7 (mod 4,157), 0 ≤ x ≤ 4,156. Hint: See the examples "Solve 122x = 9 (mod 7919)" and "Solving 136y = 14 (mod 7919)" on Blackboard.	
(56)	8.4	Find the RSA decryption exponent d when: p=13, q=17, n=221, and e=37 is the encryption exponent. Hint: Examples on Blackboard are: • "Creating an RSA Encryption-Decryption Pair…" • the solution to SE2 #9.	
(57)	8.4	Solve for x: x^2 ≡ 4 (mod 675,683). Give all 4 solutions - they should 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)."	
(58)	8.4	HW: x = 63826456536845958448. What is the remainder when x is divided by 11?	

Row	§	Homework is from the textbook or as cited below.	Due
(59)	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.	
(60)	2.2	4, 15, 27 (pgs 63-64)	
(61)	2.3	9, 11 (pg 77) These hints refer to Blackboard: • These problems are like Sample Exam-1 #7. • Epp's shortcut method and the common-sense method for determining validity are compared in Table 5 of "Truth Tables, Arguments Forms & Syllogisms."	
(62)	4.5	Suppose we are given an integer x. Now call the statement *s* = "(x^2-x) is exactly divisible by 3." Choose exactly <u>one</u> of the answers A, B, or C and: (A) Prove s is TRUE; <u>or</u> (B) Prove s is FALSE; <u>or</u> (C) Explain why (A) and (B) are impossible	
(63)	2.2	See Blackboard: Two "Problems, on Informal English and Satisfiability." The second problem pertains to the famous "P vs. NP Problem."	
(64)	3.1	12, 18(c)-(d), 28(a)&(c) (pgs 119-121) For 3.1.18(c)-(d): • Use only the ∀ and ∃ quantifiers. 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. • See "Example 3.1.18 (a),(b),&(e)" on Blackboard.	
(65)	3.2	10, 25(b)-(c), 38 (pages 130-131). Note: In #38, *Discrete Mathematics* refers to the phrase *Discrete Mathematics*, <u>not</u> to the subject of Discrete Mathematics.	
(66)	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.	
(67)	3.3	#41(c),(d),(g),(h) (page 145) Hints: (1) See "Order of Quantifiers" on textbook page 138. (2) The solution to Sample Exam 1 #25 (on Blackboard) may also help.	