Syllabus & Assignments: Spring 2020, INFS 501 (Section 001, CRN 17163)
Discrete and Logical Structures for Information Systems

Instructor:	Prof. William D. Ellis	E-mail: wellis1@gmu.edu
Office Hours:	By appt. (usually Wednesday 5-6 PM)	L008 Arts & Design Bldg

Blackboard/ Web Site: Syllabus/HW updates, sample problems & solutions, lecture notes etc. are posted weekly <u>after</u> class at http://mymason.gmu.edu.

Schedule: 14 Classes 7:20-10:00 PM Innovation Hall, Room 134
- Wednesdays Jan 22 - Apr 29 except March 11 (Spring Recess)
- The Final Exam is Wednesday May 6, 2020 from 7:30-10:15 PM

Prerequisite: "Completion of 6 hours of undergraduate mathematics." As a practical matter, you need a working knowledge of algebra, including the laws of exponents. Understand textbook pages A1-A2. Several free tutorials may be found on the Internet.

Topics: We will follow the textbook in this order: Chapters 5, 4, 2, 3, and 6-10. We will focus on solving problems, using fundamental definitions, theorems, and algorithms. Examples will include: Fibonacci numbers, the P vs. NP problem, Benford's Law, RSA cryptography, & probabilities related to the Bitcoin Blockchain.

Calculator: You will need a calculator that can display 10 digits and raise numbers to powers. During an exam or quiz: Do <u>not</u> (1) use a computer or cell phone, or (2) share anything with others.

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.

Exams and Quizzes: We will have: (i) 2 Quizzes, (ii) 2 Hour Exams, and (iii) a comprehensive Final Exam (Wednesday May 6, 2020). Exams and Quizzes: (1) will be given only once (no makeup exams), and (2) will be open-book and open-notes. <u>No</u> partial credit will be given for a purported proof to a false statement. During Exams and Quizzes: (1) Use all available classroom space, (2) Avoid sitting close to anyone else, (3) Do not sit next to a friend, and (4) Do not share calculators or anything else.

Grades: 1 Final Exam: 45% of final grade.
2 Hour Exams: 40% of the final grade (20% each)
Homework and 2 Quizzes together: remaining 15% of final grade.

Help: Questions? Send me an e-mail! Use the ^ symbol for exponents, * for multiplication. You may also e-mail a pdf or scanned image.

Homework: Homework assignments will updated weekly 1 day <u>after</u> class. See http://mymason.gmu.edu. Homework will never be accepted late. However, 13 HW assignments must be turned in and only the 12 with the highest scores will be counted toward your grade. Submit on paper, please. If you cannot attend class, scan as a black/white pdf and e-mail. <u>NO</u> grey-scale scans, please!

Honor Code: Honor Code violations are reported to the Honor Committee. See https://oai.gmu.edu/mason-honor-code/,https://cs.gmu.edu/resources/hon For INFS501 during Spring 2020, submitting homework based on collaboration and/or classroom discussion is permitted.

E-mail: Please use only GMU email for all emails with me.

Semester Schedule

Class	Date	Event	Details and dates are subject to change
(1)	Jan 22, 2020	1st class	
(2)	Jan 29, 2020		
(3)	Feb 5, 2020		
(4)	Feb 12, 2020		
(5)	Feb 19, 2020	Quiz 1	
(6)	Feb 26, 2020		
(7)	Mar 4, 2020		
	Mar 11, 2020	** No class	Spring Recess
(8)	Mar 18, 2020	Exam 1	
(9)	Mar 25, 2020		
(10)	Apr 1, 2020		
(11)	Apr 8, 2020	Quiz 2	
(12)	Apr 15, 2020		
(13)	Apr 22, 2020		
(14)	Apr 29, 2020	Hour Exam 2 & Lecture	
	May 6, 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 lines below.

Row	§	Homework is from the textbook or as cited below.	Due
(1)	5.1	7, 13, 16, 32, 57*, 61 (pgs 273-274) * On #57, simply calculate the sum for n=5. Don't do the part about changing variable.	HW-1 due 1/29/2020
(2)	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) • A word formula on Blackboard in "Geometric-Series Summation Formula Generalized & Simplified" works.	HW-1 due 1/29/202
(3)	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 1/29/202
(4)		Hints on (3): • Such a Claim would be proven FALSE if we could find 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.	
(5)	5.1	83 (pg 288) Hint: See #5.1.81 solved on Blackboard.	
(6)	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 in the "Geometric-Series Summation Formula Generalized & Simplified" pdf on BlackBoard. • This like Sample Quiz-1 #3 solved on Blackboard.	
(7)	5.6	8, 14, 33 (pages 337, 339) Hint on #5.6.14: #5.6.13 on Blackboard is similar.	
(8)	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.	
(9)	5.8	12, 14 (page 363)	
(10)		Hints: • #5.8.12 & #5.8.14 are like the problems #5 - #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 #6 on Sample Quiz 1.	
(11)	4.1	4, 6, 9, 13(b) (pages 171-172) Hint #4.1.13(b) is similar to #4.1.14 on Blackboard	

Row	§	Homework is from the textbook or as cited below.	Due
(12)	4.2	2, 13, 19, 27 (page 181-182). On 4.2.19: • After identifying the error, state also whether the “Theorem” is TRUE or FALSE, and explain why. • Hint: Find the error by comparing the given proof with “Bogus proof that 8=10" on Blackboard. Hint on 4.2.13: 4.2.14 is solved on Blackboard.	
(13)	4.1 and 4.2	In sections 4.1-4.2, 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!	
(14)	4.3	7, 28 (pages 187-188)	
(15)	4.4	21, 41 (pages 198-199)	
(16)	4.5	6, 17, 21, 35, 39 (pages 209-210) Hints: #21 is like #4.5.25 on Blackboard. #35 is like #4.5.40 on Blackboard. #39 Show 4 of 6 cases in Q-R Theorem are impossible	
(17)	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.	
(18)	4.10	Find GCD(98741, 247021)	
(19)	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 HW 5.6.33 formula (pg 339). [Beware: Some online calculators start the Fibonacci numbers at $F_1=1$, $F_2=1$, $F_3=2$, … .]	
(20)	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.	
(21)	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.	
(22)	2.2	4, 15, 27 (pgs 63-64)	
(23)	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.”	
(24)	4.5	Suppose we are given an integer x. Now call the statement s = "(x2-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.	

Row	§	Homework is from the textbook or as cited below.	Due
(25)	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.	
(26)	2.2	See Blackboard/Content/Week-6: Two "Problems, on Informal English and Satisfiability." The 2nd problem pertains to the famous "P vs. NP Problem."	
(27)	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.	
(28)	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.	
(29)	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.	
(30)	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 #24 (on Blackboard) may also help.	
(31)	1.2	#7(b),(e)&(f); #9(c)-(j); #12 (pages 14-15) (Section 1.2 fits with Ch. 6 on Set Theory.)	
(32)	6.1	#7b; #12(a),(b),(g),(h),(j); #18; #33 (pgs 388=390) Hints: • #7 is like 6.1.4; see the hint on Blackboard. • #12: Simplify using interval notation (page 382). • #12**(g)** Use #12(a) and the De Morgan laws [page 395]. The De Morgan Laws also simplify #**12(h)-(j)**. • #33: Predict the size of each power set using the theorem on page 410: size |S|=n => |P(S)|=2^n.	

Row	§	Homework is from the textbook or as cited below.	Due
(33)	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?	
(34)	6.2	#13, #17, #35 Hints: • #17 Use the format of Example 6.2.16 or 6.2.18 on Blackboard. After choosing $x \in A \cup C$, get two cases: $x \in A$ and $x \in C$. In each case, Theorem 6.2.1.2 makes every set a subset of itself with any other set. • #35 Assume $A \cap C \neq \emptyset$ and prove by contradiction.	
(35)	6.3	#2, #4, #7, #21 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 may be used to verify or find a counterexample to a "∀ sets" identity. • "Is-an-element" proofs also work for verifying "∀ sets" identities but often they're complicated.	
(36)	6.3	Prove or disprove each of these 2 Claims: (i) ∃ sets A, B & C such that $(A-B)-C=(A-C)-(B-C)$, (ii) ∀ sets A, B & C, $(A-B)-C = (A-C)-(B-C)$.	
(37)	1.3	#15(c),(d),&(e); #17. (pg 23) These tiny problems fit with Ch. 7 on Functions.	
(38)	7.1	#2, #5; #12, #51(d),(e),&(f) (pgs 436-439) <u>Note</u>: #51 Will be used in RSA encryption.	
(39)	7.2	13, 17, 43 Hint for #13, 17: See 7.2.18 solved on Blackboard.	
(40)	7.3	2, 4, 14, 20	
(41)	7.2	See the "H/W-9 Hash Function Problem" on Blackboard	
(42)	8.1	#3(c)&(d). (page 493) Hint: See 8.1.1, solved on Blackboard.	
(43)	8.2	• Read pages 15-18. • #10 (page 503). See the <u>Hint</u> on Blackboard.	
(44)	8.3	• #9 [Call 0 = the sum of the elements in φ.] • #15(b),(c),(d) (page 521) Hints: • #9 is like 8.3.8, 8.3.10, & 8.3.12, solved on Blackboard. • #15: Use the modular-equivalence definition on page 518. (The alternative tests for equivalence on pg 526 should be saved for § 8.4.)	
(45)	8.4	2, 4, 8, 17, 18 (pages 544-545) On 8.4.8, mimic the Blackboard solution to 8.4.7.	

Row	§	Homework is from the textbook or as cited below.	Due
(46)	8.4	Calculate 2^{373} (mod 367). [Hint: If it matters, 2, 367, and 373 are all prime numbers.]	
(47)	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 = h*10^2+t*10+u. For 12b, reduce the 10's (mod 9). For 13b, reduce the 10's (mod 11). The same approach works no matter how many base-10 digits a positive integer x has.	
(48)	8.4	#20, 21, 23, 37, 38, 40. (page 545) <u>Hints</u>: On #20,21,23: Use Examples 8.4.9-8.4.10 (mod 55): • For encryption, Epp chose e=3 (pretty much at random). Thus, H=8 -> 8^3 ≡ 17 (mod 55). • d=27 decrypts, e.g. 17 -> 17^27 ≡ 8 (mod 55). • The pair (e,d)=(3,27) reverse each other because: (1) 3*27=1 (mod 40), and (2) 40=(5-1)(11-1) is the Little Fermat exponent. #40: The modulus = 713=23*31 & encryption e=<u>43</u>. From #38, <u>43</u>*307 ≡ 1 (mod (23-1)(31-1)). Thus, each pair (e=43,d=307) and (e=307,d=43) will work equally well for encryption-decryption (mod 713).	
(49)	8.4	Solve for x: 1014*x ≡ 7 (mod 4,157), 0 ≤ x ≤ 4,156. Hint: See examples "Solve 122x = 9 (mod 7919)" and "Solving 136y = 14 (mod 7919)" on Blackboard.	
(50)	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.	
(51)	9.1	4, 8 (page 571) Hints: Mimic Examples #3, #7, & #10 on Blackboard.	
(52)	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. Hint: Solve 821*x + 823*y = 1. Afterward it's an easy trick. See Blackboard "Square roots (mod pq) two examples."	
(53)	9.1	#14(b)-(c); #20 (Modified Monty Hall) <u>Hint</u> on #20: Mimic the Solution to #4 on Sample Exam II.	
(54)	9.2	#7; #12; #17(a)-(d); #33; #36; #39 Hints: #17(a)-(c) Build a possibility tree starting at the leftmost digit. On 17(d), start at rightmost digit (5 choices), then leftmost (8 choices), ... #33, #36, #39 use the formula on page 582.	
(55)	9.5	7(a)-(b), 12, 16, 20(a)	

Row	§	Homework is from the textbook or as cited below.	Due
(56)	9.5	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 "Flipping Fair and Unfair Coins" on Blackboard.	
(57)	9.8	#17. Hint: (1) Mimic the solution to #18 on Blackboard. (2) Blackboard has a similar solved example, "7 is the Expected Value of the total of two dice."	
(58)	1.4	#4 (pg 35) Sec 1.4 fits with Ch. 10	
(59)	4.9	#7 (page 242)) Sec 4.9 fits with Ch. 10	
(60)	4.9	#5, 16(a) (page 242) Discussed in Class #8 Example on Blackboard	
(61)	10.1	#8; (pages 694) Will be discussed in Class #9; 10 (page 694) Worked-out examples on Blackboard Note #11 appears as Sample Final Exam problem (18)	