Syllabus & Assignments: Fall 2019, INFS 501 (Section 001, CRN 70229)

Instructor: Prof. William D. Ellis E-mail: wellis1@gmu.edu
Office Hours: By appt. (usually Mondays 5-6 PM) 4456 Engineering Bldg

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

Schedule: 14 Classes 7:20-10:00 PM Innovation Hall, Room 134

- Mondays Aug. 26-Dec. 2, except 10/15 (Tues), Labor Day holiday
- The Final Exam is Monday Dec. 16, 2019 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, 6, 7, 8, 10, and 9. We will focus on problem solving; and we will use fundamental definitions, theorems, and algorithms. Examples will include: Fibonacci numbers, P vs. NP problem, RSA public-key cryptography, Benford's Law, and Bitcoin Blockchain.

Calculator: You will need a calculator that can display 10 digits and raise numbers to powers. During an exam or quiz: Do not (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). No e-book may used be during any quiz or exam, but you may print and bring relevant pages from an e-book.

Exams and Quizzes: We will have: (i) 2 Quizzes, (ii) 2 Hour Exams, and (iii) a comprehensive Final Exam (Monday Dec. 16, 2019). Exams and Quizzes will be given only once - no makeup exams. Use all available classroom space, avoid sitting close to anyone else, and do not sit next to a friend. No partial credit will be given for a purported proof to a false statement. During exams and quizzes do not use or display cellphones, computers, or watches. Do not share calculators or anything else. Exams and quizzes will be open-book and open-notes.

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 after 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. NO 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 this semester, submitting homework based on collaboration and/or classroom discussion is permitted.

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

Syllabus and HW assignments posted after each class. Rev 8/15/2019 (10:10 PM)

Semester Schedule

Class	Date	Event	Details and dates are subject to change
(1)	Aug 26, 2019	1st class	
	Sep 2, 2019	** No class	Labor Day holiday
(2)	Sep 9, 2019		
(3)	Sep 16, 2019		
(4)	Sep 23, 2019		
(5)	Sep 30, 2019	Quiz 1	On everything covered through HW #3, ending with section 4.2. Problems will be like in: • the sample Quiz, • the Homework, • the Notes On Defining and Summing Sequences pdf (Blackboard Week 1).
(6)	Oct 7, 2019		
(7)	Oct 15, 2019	Tuesday!	Class moved from Monday Columbus Day
(8)	Oct 21, 2019	Hour Exam 1 & Lecture	
(9)	Oct 28, 2019		
(10)	Nov 4, 2019		
(11)	Nov 11, 2019	Quiz 2	
(12)	Nov 18, 2019		
(13)	Nov 25, 2019		
(14)	Dec 2, 2019	Hour Exam 2 & Lecture	
	Dec 9, 2019	** No class	Reading day
	Dec 16, 2019	FINAL EXAM	The Final Exam will cover everything from the entire semester. Problems will be like in the Exams, Quizzes, Sample Exams & Quizzes, and HW 1-14. (“HW-14” will be solved in class on 12/2/2019.)

Row	§	Homework is from the textbook or as cited below.	Due
(1)	5.1	7, 13, 16, 32, 57*, 61 (pgs 273-274) * For 5.1.57, simply calculate the sum for n=5. Don’t do the part about changing variable.	HW-1 due 9/9/2019
(2)	5.2	23, 27, 29. (pg 288) Hints: #23 is like Example 5.2.2 (pg 281); #27, 29 like Example 5.2.4 (pg 285)	HW-1 due 9/9/2019
(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 9/9/2019
(4)	Hints on (3): • Such a Claim would be proven FALSE if we could find even one counterexample, i.e. find one value for 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)	
(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 53 numbers. Compute a few of them to judge the approximate size of the sum. • Use Theorem 5.2.2 on page 283, or use the word-formula in the “Geometric-Series Summation Formula Generalized & Simplified” pdf on BlackBoard. • A solved example is #3 in Sample Quiz 1 on Blackboard.	HW-2 due 9/16/2019
(7)	5.6	6, 14, 33 (pages 337, 339)	
(8)	5.8	12, 14 (page 363)	
(9)	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). • How to factor any Characteristic Equation is explained in the solution to #6 on Sample Quiz 1.		
(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)	4.1	3, 5, 9, 13 (pages 171-172)	
(12)	4.2	2, 27 (page 171-172)	
(13)	4.3	7, 28 (pages 187-189))	
(14)	4.4	21, 41	

Row	§	Homework is from the textbook or as cited below.	Due
(15)	4.5	6, 18a, 21, 35, 39 (pages 209-210) Hints: #21 is like #4.5.25 on Blackboard. #35 is like #4.5.40 on Blackboard.	
(16)	4.10	12, 16, 23(b) (pages 255-256) On 23(b), don't worry about syntax. To describe an algorithm, just state: (i) its input, (ii) what it says to do, and (iii) its output.	
(17)	4.10	Find GCD(98741, 247021)	
(18)	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).	
(19)	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. See Blackboard for a hint & the spreadsheet "Excel: Euclidean Algorithm" may ease your calculation.	
(20)	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.	
(21)	2.2	4, 15, 27 (pgs 63-64)	
(22)	2.3	10, 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."	
(23)	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.	
(24)	2.2	Posted on Blackboard/Content/Week-6 are 2 problems on Informal English & Satisfiability (related to the P vs. NP Problem)	
(25)	3.1	12, 18(c)-(d), 28(a)&(c), 32(b)&(d) (pgs 119-121) For 3.18, see the 3.18 Example on Blackboard. Also, • 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 ∄.	
(26)	3.2	10, 25(b)-(c), 38 (pages 130-131). Note: In #38, "Discrete Mathematics" refers to the phrase "Discrete Mathematics," not to the subject of Discrete Mathematics.	

Row	§	Homework is from the textbook or as cited below.	Due
(27)	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 ∄.	
(28)	3.3	#41(c),(d),(g),(h) (page 145)	
(29)	3.3	#1 & #2 On Sample Quiz-2.	
(30)	1.2	#7(b),(e)&(f); #9(c)-(j); #12 (pages 14-15) (Section 1.2 fits with Ch. 6 on Set Theory.)	
(31)	6.1	#7b; #13; Hints: #7 See the Hint on Blackboard. #7 is like 6.1.4. #13 See the Hint on Blackboard.	
(32)	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?	
(33)	6.1	#12(a),(b),(g)&(j); #18; #33 Hints: • #12: Writing [-3,2) for "-3 <= x < 2" etc. is OK. • #12: motivates Set Identities (pgs 294-395). • #33: Predict the size of each power set using the theorem on page 409: size |S|=n => |P(S)|=2^n.	
(34)	6.2	#10, #14, #32 Hints for 6.2.14 and 6.2.32 are on Blackboard	
(35)	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 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 22) These tiny problems fit with Ch. 7 on Functions.	
(38)	7.1	#2, #5; #51(d),(e),&(f) (pgs 436-439) Note: #51 Will be used in RSA encryption.	

Row	§	Homework is from the textbook or as cited below.	Due
(39)	7.2	8, 13(b), 17 Hint: 7.2.17 ≈ 7.2.18 which is solved on Blackboard	
(40)	7.3	2, 4, 11, 17	
(41)	7.2	See the "H/W-10 Hash Function Problem" on Blackboard	
(42)	8.1	#3(c)&(d). (page 493) Hint: See 8.1.1, solved on Blackboard.	
(43)	8.3 pg 521	#9 [Call 0 = the sum of the elements in φ.] #15(b),(c),(d) Hints: #9: Like 8.3.8, 8.3.10, & 8.3.12, solved on Blackboard. #15: Use the definition on page 473.	
(44)	8.4	2, 4, 8, 17, 18 (page 544-545)	
(45)	8.4	Calculate 2^{373} (mod 367). [Hint: If it matters, 2, 367, and 373 are all prime numbers.]	
(46)	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.	
(47)	8.4	Solve for x: 1014*x ≡ 7 (mod 4,157), 0 ≤ x ≤ 4,156. See examples	
(48)	8.4	#20, 21, 23, 37, 38, 40. (page 545) Hints: #20-21 use Example 8.4.9: encryption e =3 (mod 55). For example, H = 8 -> 8^3 = 17 (mod 55). #23 uses Example 8.4.10: decryption d=27 (mod 55). For example 17 -> 17^27 = 8 (mod 55). Examples 8.4.9-8.4.10 reverse each other, e.g. (mod 55) H = 8-> 17(encrypt) -> 8 = H(decrypt) The pair (e,d)=(3,27) reverse each other because 3*27=1 (mod 40) and 40 = (5-1)(11-1)=40 is the Little Fermat exponent (mod 55). #40 Modulus = 713=23*31 & encryption e=43 are given. From #38, 43*307 = 1 (mod (23-1)(31-1)), so use decryption d = 307.	
(49)	8.4	Under RSA: p = 13, q = 17, n = 221, & e = 37 is the encryption exponent. Find d = decryption exponent. See Blackboard Week 11: • Examples: Creating an RSA Encryption-Decryption Pair; Solution to SE2 #10 on Blackboard/Week-11 • The solutions to Sample Exam 2, #6 & #10.	

Row	§	Homework is from the textbook or as cited below.	Due
(50)	8.4	Solve for x: $x^2 \equiv 4$ (mod 675,683). Give all 4 solutions. All 4 answers should be between 0 & 675,682. Use 675,683 = 821 * 823, the product of 2 prime numbers. Hint: See "Square roots (mod pq) two examples.pdf," on Blackboard. This example shows multiple square roots always exist if the modulus is composite. Multiple square roots enable factoring an RSA modulus as in row (19) 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 only needs to solve d = e^{-1} (mod (p-1)(q-1)).	
(51)	8.4	What integer x satisfies: (a) 1 ≤ x ≤ 2,622,187; (b) x = 510 (mod 661); and (c) x = 479 (mod 3967)? Here, 661*3967 = 2,622,187. Hint: See Blackboard, either: (1) The solution to SE2 #22.5, (2) "Example: Simultaneous Equations and the Chinese Remainder Theorem," or (3) Section 3.3 on page 8 of the lecture notes, "Summary: Little Fermat, RSA, & Chinese Remainder Theorem."	
(52)	1.4	#4 (pg 35) Sec 1.4 fits with Ch. 10 - Graph Theory.	
(53)	4.9	7, 8, 18, 20 (pages 242-243) (Sec 4.9 fits with Ch. 10 - Graph Theory.)	
(54)	10.1	8(b),(c)&(d); 9; 10; 13 (pages 657-658)	
(55)	10.3	#4, #11, #13, #15 (page 719-720) On 4, 11, & 13, explain why the given pair of graphs cannot be isomorphic. Hints: #13: Look for circuits of length 5. #15: There are 11 non-isomorphic simple graphs with 4 vertices.	
(56)	9.1	10; 12(b)(ii)-(iii); 14(b)-(c) (pages 571-573) 20 (Modified Monty Hall)	
(57)	9.2	7; 12; 17(a),(b)&(d); 33 (pages 585-588)	
(58)	9.5 pg 631	7(a)-(b) [n-choose k = n-choose (n-k)] 12 [# ways for even total of 2 pos integers <= 101] 16	
(59)	9.5	Suppose a fair coin is flipped 9 times. What is the probability that heads occurs at least 3 times?	
(60)	9.8	#18 (Expected total value after 3 balls are drawn)	
(61)	9.8	"HW-14" will be solved in class on 12/2/2019. HW-14 consists of probability problems related to the hash function used in the Bitcoin Blockchain.	