Syllabus & Assignments: Spring 2019, INFS 501 (Section 001, CRN 20355)

Instructor: Prof. William D. Ellis E-mail: wellis1@gmu.edu
Office Hours: By appt. (usually Wednesdays 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 Arts & Design Bldg. Room 2026
- Wednesdays except no class on March 13 during Spring Vacation
- The Final Exam is Wednesday May 8, 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. Several free tutorials may be found on the Internet. Also see textbook Appendix pages A1-A3.

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. As examples, we'll learn about the P versus NP problem, RSA public-key cryptography, Benford's Law, and 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, 4th ed. (8/4/2010) By Susanna S. Epp, ISBN-10: 0495391328; ISBN-13: 978-0495391326. <u>No</u> e-books may used during any quiz or exam.

Exams and Quizzes: We will have: (i) 2 Quizzes, (ii) 2 Hour Exams, and (iii) a comprehensive Final Exam (Wednesday May 8, 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. <u>No</u> 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 smart watches. Do <u>not</u> 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 be on the weekly Syllabus updates. See http://mymason.gmu.edu. Homework will never be accepted late. However, 13 HW assignments will be turned in, but 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 http://cs.gmu.edu/wiki/pmwiki.php/HonorCode/CSHonorCodePolicies Collaborating on homework or submitting solutions based on classroom discussion is okay but only for INFS501 in Spring 2019.

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

Semester Schedule: Dates & data for Quizzes 1-2 and Exams 1-2 <u>may change</u>.

Class	Date	Event	Details - some are tentative
(1)	Jan 23, 2019	1st Class	
(2)	Jan 30, 2019		
(3)	Feb 6, 2019		
(4)	Feb 13, 2019		
(5)	Feb 20, 2019	Quiz 1	
(6)	Feb 27, 2019		
(7)	Mar 6, 2019		
	Mar 13, 2019	no class!	Spring Vacation
(8)	Mar 20, 2019	Hour Exam 1 & Lecture	
(9)	Mar 27, 2019		
(10)	Apr 3, 2019		
(11)	Apr 10, 2019	Quiz 2	
(12)	Apr 17, 2019		
(13)	Apr 24, 2019		
(14)	May 1, 2019	Hour Exam 2 & Lecture	
(15)	May 8, 2019	FINAL EXAM	

Row	§	Homework from the textbook or written out below.	Due
(1)	5.1	7, 13, 16, 32, 57*, 61, 83 * For 5.1.57, only calculate the sum for n=5. Don't bother changing variable like the problem asks.	HW-1 due 1/30/2019
(2)	5.2	23, 27, 29. Hint: Try using Example 5.2.2 on page 251 & Example 5.2.4 on page 255.	HW-1 due 1/30/2019
(3)	5.2	False or True? Why? $\forall$ 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 1/30/2019
(4)	5.2	Express $S=\sum_{k=29}^{k=123}\left(\frac{25}{24}\right)^{-k}$ 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 what the sum should look like. • Use Theorem 5.2.3 on page 253, 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.	
(5)	5.2	11, 12	
(6)	5.6	8, 14, 33	
(7)	5.7	2(b)&(d), 4, 25	
(8)	5.8	12, 14	
(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 321) and 5.8.5 (pg 325). • How to factor any Characteristic Equation is explained in the solution to #6 on Sample Quiz 1.	
(10)	4.1	3, 5, 8. Follow § 4.1 and do not rely on the well-known even/odd properties on page 167 in § 4.2. (The §4.2 properties are based on §4.1 too!)	
(11)	4.1	12, 27, 36, 50	
(12)	4.2	2, 7, 28 Hint on #28: Write r is the format of a rational number, following the definition of "rational." Then use the algebra of fractions to show 3r^2-2r+4 can be expressed in the same format.	
(13)	4.3	5, 21, 41	

Row	§	Homework from the textbook or written out below.	Due
(14)	4.4	6, 17, 21, 35, 42 Hints: #17 is like #4.4.19 on Blackboard. #21 is like #4.4.25 on Blackboard. #35 is like #4.4.43 on Blackboard. #42 is like #4.4.30 on Blackboard	
(15)	4.8	12, 16; 20(b) [Don't worry much about syntax. To describe an algorithm, we must describe: (i) its input, (ii) what it says to do, and (iii) its output.]	
(16)	4.8	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. <u>Hint</u>: See the Hint on Blackboard.	
(17)	4.8	Find GCD(98741, 247021)	
(18)	4.8, 5.8	Write the Fibonacci no. F_{400} in scientific notation, e.g. $F_{30} \approx 1.35*10^6$. Note: Be careful using and formulas on the Internet. Epp defines the Fibonacci sequence starting with F_0=1, F_1=1 while some other authors (like Wikipedia) start with F_1=1, F_2=1.	
(19)	2.1	15, 37, 43 (page 38) Hints: #43 is like #2.1.41 on Blackboard. #37 is like #2.1.33 on Blackboard.	
(20)	2.2	4, 15, 27. #4 is like #19 on the Sample Exam.	
(21)	2.3	10, 11 (page 62) Hints: • These problems are like #7 solved in the Sample Exam on Blackboard. • Epp's shortcut method and the common-sense method for determining validity are compared in Table 5 of "Truth Tables, Arguments Forms & Syllogisms."	
(22)	4.4	Suppose we are given an integer x. Now call the statement *s* = "(x^2-x) is exactly divisible by 3." Choose <u>one</u> of the answers A, B, or C and either: **(A)** Prove s is TRUE; **(B)** Prove s is FALSE; <u>or</u> **(C)** Explain why (A) and (B) are impossible.	
(23)	2.2	Posted on Blackboard/Content/Week 6 are two (2) of the ten (10) HW-6 Problems due 3/6/2019	
(24)	3.1	12, 18(c)-(d), 28(a)&(c), 32(b)&(d) (pgs 106-108)	
(25)	3.2	10, 25(b)-(c), 38 (pages 116-117). Note: In #38, "Discrete Mathematics" refers to the phrase "Discrete Mathematics," not to the subject of Discrete Mathematics.	
(26)	3.3	#41(c),(d),(f),(g),(h) (page 130)	
(27)	3.3	Sample Quiz-2, #1 & #2	

Row	§	Homework from the textbook or written out below.	Due
(28)	1.2	#7(b),(e)&(f); #9(c)-(j); #12 (Section 1.2 fits with Ch. 6 on Set Theory.)	
(29)	6.1	#7b; #12(a),(b),(g)&(j); #13; #18, #33 <u>Hints</u>: #7 See the Hint on Blackboard. #7 is like 6.1.4. #12: Writing [-3,2) for "-3 <= x < 2" etc. is OK. #12 makes us want the Set Identities on pg 355. #13 See the Hint on Blackboard. #33 Predict the size of each power set using the theorem on page 369: size |S|=n => |P(S)|=2^n.	
(30)	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?	
(31)	6.2	#10, #14, #32 Hints: Hints for #14 and #32 are on Blackboard	
(32)	6.3	#2, #4, #7 <u>Hints</u>: Hints for #2, #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 they're often complicated.	
(33)	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).	
(34)	1.3	#15(c),(d),&(e); #17. (pg 22) These tiny problems fit with Ch. 7 on Functions.	
(35)	7.1	#2; #5; #51(d),(e),&(f) (pg 393) <u>Note</u>: #51 Will be used in RSA encryption.	
(36)	7.2	See the "H/W-9 Hash Function Problem" on Blackboard	
(37)	7.2	8, 13(b), 17	
(38)	7.3	2, 4, 11, 17	
(39)	8.1	#3(c)&(d). <u>Hint</u>: See 8.1.1, solved on Blackboard.	
(40)	8.3	#9 [0= the sum of the elements in the empty set φ.] #15(b),(c),(d) <u>Hints</u>: #9: Like #8, 10, & 12, solved on Blackboard. #15: Use the definition on page 473.	
(41)	8.4	2, 4, 8, 17, 18	

Row	§	Homework from the textbook or written out below.	Due
(42)	8.4	Calculate 2^{373} (mod 367). [Hint: If it matters, 2, 367, and 373 are all prime numbers.]	
(43)	8.4	12b, 13b [Hint: If we call the hundred's digit "h," the tens digit "t," and the unit's digit "u," then the 3-digit base-10 number 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 digits a positive integer has.]	
(44)	8.4	Solve for x: 1014*x ≡ 7 (mod 4,157), 0 ≤ x ≤ 4,156.	
(45)	8.4	#20, 21, 23, 37, 38, 40. 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.	
(46)	8.4	Under RSA: p = 13, q = 17, n = 221, & e = 37 is the encryption exponent. Find d = decryption exponent. See Blackboard, "Example: Creating an RSA Encryption-Decryption Pair." We also solved Sample Exam 2 #10.	
(47)	8.4	Solve for x: x^2 ≡ 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. <u>Hint</u>: See "Square roots (mod pq) two examples.pdf," on BlackBoard. This shows multiple square roots exist under a composite modulus. Multiple square roots allow factoring the RSA modulus as in Row (16) above. RSA is attacked by finding multiple square roots mod the public modulus n, to factor n = pq - that's the hard part. Then an RSA-cracker only needs to solve d = e^{-1} (mod (p-1)(q-1)).	
(48)		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."	
(49)	10.1	4, 19, 20, 29, 34 (pages 639-640)	
(50)	10.2	8(b),(c)&(d); 9; 10 (pages 657-658)	

Row	§	Homework from the textbook or written out below.	Due
(51)	10.4	#4, #11, #13, #15. 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.	
(52)	9.1	10, 12(b)(ii)-(iii), 14(b)-(c), 20	
(53)	9.2	7, 17(a),(b)&(d), 33	
(54)	9.5	7(a)-(b), 12	
(55)	9.8	HW-14 will be done in class on 5/1/2019. HW-14 consists of probability problems related to the Blockchain,	