Syllabus & Assignments: Fall 2018, INFS 501 (Section 001, CRN 70332)

Instructor:	Prof. William D. Ellis	E-mail: wellis1@gmu.edu
Office Hours:	By appointment (usually Monday 5-6 PM)	5321 Engineering Bldg.

Blackboard/ Web Sit: 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 206
- Mondays except Columbus Day class moved to Tuesday Oct 9, 2018
- The Final Exam is Monday December 17, 2018, 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.

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> share a calculator or use a computer or cell phone.

Textbook: Discrete Mathematics with Applications, 4th ed. (8/4/2010) By Susanna S. Epp, ISBN-10: 0495391328; ISBN-13: 978-0495391326. A copy will be on 2-hour reserve at the Johnson Center Library. Ebooks <u>cannot</u> be used during an exam.

Exams and Quizzes: We will have: (i) 2 Quizzes, (ii) 2 Hour Exams, and (iii) a comprehensive Final Exam (Monday Dec 17, 2018). 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 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 be on the weekly Syllabus updates. See http://mymason.gmu.edu. Homework will never be accepted late. However, of the 13 assignments, 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 & e-mail. However, no 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 Fall 2018.

E-mail: Use only GMU email for all emails with me, per privacy rules.

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

Class	Date	Event	Details
(1)	Aug 27, 2018	1st Class	
	Sep 3, 2018		Labor Day Holiday
(2)	Sep 10, 2018		
(3)	Sep 17, 2018		
(4)	Sep 24, 2018	Quiz 1	
(5)	Oct 1, 2018		
(6)	Oct 9, 2018	Tuesday!	Moved from Columbus Day.
(7)	Oct 15, 2018	Hour Exam 1 & Lecture	Exam 1 will be on everything we covered in class through HW5, ending in § 2.3. Problems will be like in the Homework and Quiz 1.
(8)	Oct 22, 2018		
(9)	Oct 29, 2018		
(10)	Nov 5, 2018	Quiz 2	Quiz 2 will be on everything that we covered in Chapters 3, 6, sections 7.1-7.2, and related sections in Chapter 1. Problems will be like in H/W #6-#9.
(11)	Nov 12, 2018		
(12)	Nov 19, 2018		
(13)	Nov 26, 2018		
(14)	Dec 3, 2018	Hour Exam 2 & Lecture	
(15)	Dec 17, 2018	FINAL EXAM	The Final Exam will cover everything from the entire semester.

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 9/10/2018
(2)	5.2	23, 27, 29. <u>Hint</u>: Try using Example 5.2.2 on page 251 & Example 5.2.4 on page 255.	
(3)	5.2	False or True? Why? ∀ Means "for all" $\sum_{k=1}^{n}(8k^3+3k^2+k)=n(n+1)^2(2n+1)\forall n\in Z^+$ <u>Hint</u>: Test validity using the first 5 (=3+2) values for n because the summands $8k^3$ + ... have degree 3. Always test 2 more sums than the summands' degree. If the formula is true, it would be provable by mathematical induction. However, mathematical induction isn't needed anywhere in HW-1.	
(4)	5.2	Express $\sum_{k=8}^{k=60}1.05^{-k}$ as a decimal number with at least two decimal digits of accuracy. For example, your answer might look like "S = 52.33." <u>Hints</u>: • 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 #15 on the "Sample Sequences and Progressions Lecture Notes" on BlackBoard.	
(5)	5.6	2, 8, 14, 33 <u>Hints</u>: • On 5.6.14, you may use the Hint on Blackboard. You may also mimic "Second Order Recurrence Example" (Part 1) on BlackBoard. (You'll need different values for the constants raised to powers & for the recursion-coefficients A & B). • On 5.6.33, you may choose to use the Hint on Blackboard.	
(6)	5.7	1c, 2(b)&(d)	
(7)	5.7	4, 23, 25	
(8)	5.8	12, 14 <u>Hints</u>: • #12 uses Thrm. 5.8.3 (pg 321). See Blackboard "Example: A linear homogeneous recursion" • #14 uses Theorem 5.8.5 (pg 325) because the characteristic equation as only 1 root. See the solution to Problem 5.8.13 in the text.	
(9)	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 also based on §4.1.)	

Row	§	Homework from the textbook or written out below.	Due
(10)	4.1	12, 27, 36, 50	
(11)	4.2	2, 7, 20, 28	
(12)	4.3	3, 5, 21, 41	
(13)	4.4	6, 17, 21, 35, 42, 44 [#35 & #42 are like #4.4.43 on BlackBoard.]	
(14)	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.]	
(15)	4.8	Find GCD(98741, 247021).	
(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. Also, mimic "Examples of Factoring By Factoring the Difference of Two Squares" on Blackboard.	
(17)	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 if you try using formulas on the Internet. Epp defines the Fibonacci sequence starting with $F_0=1$, $F_1=1$ while some others (like Wikipedia) have $F_1=1$, $F_2=1$.	
(18)	2.1	15, 33, 43. Hints: For #43, see 2.1.41 on BlackBoard. For #33, use logical manipulations like in the example in "Symbolic Logic Compared to Set Theory" on BlackBoard.	
(19)	2.2	4, 15, 27 Problem 2.2.8 is a truth-table example on BB. <u>Hint</u>: For 2.2.4, see the equivalences in Table 3 in the pdf "Truth Tables, Arguments Forms & Syllogisms" on Blackboard. We reviewed those equivalences in class on 10/10/2018.]	
(20)	2.3	10, 11	
(21)	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 below. Then complete your answer with a proof if your answer is A or B; or with an explanation if your answer is C: **(A)** Prove s is true; **(B)** Prove s is not true; <u>or</u> **(C)** Explain why (A) and (B) are impossible.	
(22)	3.1	12, 17(b), 18(c)-(d), 28(a)&(c), 32(b)&(d) (pages 106-108)	

Row	§	Homework from the textbook or written out below.	Due
(23)	3.2	10, 17, 25(b)-(c), 38 (pages 116-117). (In #38, "Discrete Mathematics" refers to the phrase "Discrete Mathematics," not to the subject of Discrete Mathematics.)	
(24)	3.3	#41 (page 130).	
(25)	1.2	4; 7(b),(e)&(f); 12 (Section 1.2 fits with Ch. 6 on Set Theory.)	
(26)	6.1	7b; 12(a),(b),(g)&(j); 13; 18, ~~33~~	
(27)	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?	
(28)	6.2	10, 14, 32	
(29)	6.3	2, ~~4, 7,~~ 20, 21. [Is-an-element-of proofs work for verifying a "for-all-sets" identity. We may instead verify or find a counterexample by calculating with numbered Venn-Diagram regions. However, NO solution based on Venn-Diagram shading will be accepted - shading alone is usually confusing & unconvincing.	
(30)	6.3	Prove or disprove each of the following 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).	
(31)	1.3	15(c),(d),&(e); 17. These little problems fit with Ch. 7 on Functions.	
(32)	7.1	2; 5; ~~14;~~ 51(d),(e),&(f)	
(33)	7.2	8, 13(b), 17	
(34)	7.3	2, 4, 11, 17	
(35)	8.3	#10 [#12 is similar and solved on BlackBoard.]	
(36)	8.4	2, 4, 8, 17, 18	
(37)	8.4	Calculate 2^{373} (mod 367). [Hint: If it matters, 2, 367, and 373 are all prime numbers.]	
(38)	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.]	
(39)	8.4	Solve for x: 1014*x ≡ 7 (mod 4,157), 0 ≤ x ≤ 4,156.	

Row	§	Homework from the textbook or written out below.	Due
(40)	8.4	#20, 21, 23, 27, 32, 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..	
(41)	8.4	Under RSA: p = 13, q = 17, n = 221, & e = 37 is the encryption exponent. Find d = decryption exponent. [Hint: See Blackboard, "Example calculating RSA Encryption-Decryption Pairs."	
(42)	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 shows multiple square roots exist under a composite modulus, like is used in RSA. Multiple square roots allow factoring the RSA modulus as in Row (16) above. The textbook attack on RSA is: Find multiple square roots modulo the public modulus n, factor n=pq, solve $e=d^{-1}$ (mod (p-1)(q-1)).	
(43)	8.4	What integer x satisfies: (a) $1 \le x \le$ 2,622,187; (b) x = 510 (mod 661); and (c) x = 479 (mod 3967)? Here, 661*3967 = 2,622,187.	
(44)	10.1	4, 19, 20, 29, 34 (pages 639-640)	
(45)	10.2	8(b),(c)&(d); 9; 10 (pages 657-658)	
(46)	10.5	15, 16, 17, 18, 19	
(47)	10.6	15, 16, 17, 18	
(48)	9.1	10, 12(b)(ii)-(iii), 14(b)-(c), 20	
(49)	9.2	7, 12(b), 17(a),(b)&(d), 22, 33, 40	
(50)	9.5	7(a)-(b), 12, 14. See the solutions on BlackBoard.	