Extra credit

Very small amount of extra credit will be available for some extra problems subject to the below rules. Note the amount is very small, so don't look at these unless you are comfortable with the core material of the class. That is, except the book errors category, that should be tried by all.

Note that this document may (and will) change throughout, problems will be added, typos fixed, etc...

Rules:

There are three categories of extra credit.

(1) **Puzzles.** The first person to submit a certain puzzle will get 0.25% extra credit. However, one person can get credit for only one puzzle.

(2) **Book errors.** This is my sneaky way of getting you guys to read the book. For every actual mathematical error in the book, the first person to point it out will get $\frac{0.25}{n}\%$ for the nth submission. So you first get 0.25% for the first submission, 0.125% for the second, 0.0833% for the third submission, etc... It must be an actual mathematical error, not a grammar or style problem, and only the first person to reported gets credit. It can be in any part of the book, but it must be the 7th edition. No worries, there are mistakes to catch.

(3) **Corewars tournament.** Given enough submissions, we will run a tournament and the winner can get 0.25% extra credit. See below for more info.

Submission should be to my email: `lebl@math.wisc.edu` . You should make sure to put something like "Extra credit submission" in the subject so that I can categorize and respond properly. Submissions should come before the date of the final.

Puzzles

Note: some are harder, some are easier. New puzzles may be added later.

(1) (Logic Puzzle) **(Note: this was solved already)** You are before the grand council of the island of Foobar, composed of three members: True, False, and Argblarg. Unfortunately, you do not know which one is which, which is a pity, as you have been given to understand that this is vital information. Fortunately, you do know some information: True always tells the truth, False always lies, and Argblarg... well, Argblarg says whatever he wants. The rules of the grand council of the island of Foobar are as follows: Anyone going before the council gets to ask exactly three yes/no questions, each one directed to exactly one of the members of the council, who will then answer the question. One may base later questions on the answers to earlier ones, and one may direct multiple questions to the same council member. Unfortunately, though all the members of the grand council understand English, ceremonial rules require that they only speak the secret tongue of Foobarian. The words for "yes" and "no" in Foobarian are "foo" and "bar", in some order – but you don't know which is which. How can you, through your three questions and the three answers given by the grand council of the island of Foobar, determine which council member is True, which one is False, and which one is Argblarg?

(2) (Number Theory) Let a and m be (arbitrary) positive integers. Define a sequence a_n recursively as follows: $a_1 = a$, and $a_{n+1} = a^{a_n}$ for $n \geq 1$. Then, define the sequence b_n by $b_n = a_n \bmod m$. Prove that the sequence b_n is eventually constant.

(3) (Programming / Number Theory) Diana sends the same message to each of Alice, Bob, and Charles, using their RSA keys.

Alice's public key is

$n_1 = 8\ 863\ 311\ 460\ 481\ 781\ 141\ 746\ 416\ 676\ 937\ 941\ 075\ 153\ 709\ 659\ 930\ 434\ 578\ 989\ 576\ 454\ 853\ 657\ 824\ 757\ 125\ 219\ 971\ 944\ 776\ 154\ 496\ 375\ 261\ 537\ 574\ 471\ 193\ 394\ 889\ 882\ 989\ 089\ 525\ 667\ 336\ 788\ 696\ 489\ 143\ 321\ 703\ 785\ 633\ 024\ 846\ 473\ 739\ 853\ 542\ 155\ 131\ 471\ 765\ 883\ 950\ 963\ 709\ 458\ 425\ 003\ 103\ 527\ 483\ 331\ 918\ 530\ 627\ 858\ 660\ 949\ 272\ 208\ 501\ 136\ 880\ 181\ 401\ 361\ 437\ 034\ 621,$

$e_1 = 3.$

Bob's is

$n_2 = 8\ 863\ 311\ 460\ 481\ 781\ 141\ 746\ 416\ 676\ 937\ 941\ 075\ 153\ 709\ 659\ 930\ 434\ 578\ 989\ 576\ 454\ 853\ 657\ 824\ 757\ 125\ 219\ 971\ 944\ 776\ 154\ 496\ 375\ 261\ 537\ 574\ 471\ 193\ 391\ 387\ 559\ 088\ 717\ 587\ 680\ 322\ 284\ 863\ 076\ 552\ 503\ 650\ 556\ 227\ 344\ 117\ 936\ 523\ 740\ 217\ 549\ 860\ 922\ 144\ 393\ 964\ 978\ 935\ 696\ 177\ 238\ 190\ 245\ 580\ 706\ 063\ 128\ 502\ 771\ 258\ 186\ 465\ 823\ 214\ 390\ 003\ 235\ 691\ 996\ 303\ 304\ 527,$

$e_2 = 3.$

Charles's is

$n_3 = 8\ 863\ 311\ 460\ 481\ 781\ 141\ 746\ 416\ 676\ 937\ 941\ 075\ 153\ 709\ 659\ 930\ 434\ 578\ 989\ 576\ 454\ 853\ 657\ 824\ 757\ 125\ 219\ 971\ 944\ 776\ 154\ 496\ 375\ 261\ 537\ 574\ 471\ 193\ 391\ 385\ 407\ 891\ 698\ 062\ 317\ 496\ 575\ 205\ 108\ 824\ 871\ 544\ 510\ 374\ 815\ 234\ 856\ 205\ 738\ 766\ 004\ 136\ 828\ 520\ 805\ 419\ 335\ 875\ 843\ 560\ 760\ 813\ 014\ 018\ 735\ 860\ 250\ 929\ 031\ 609\ 054\ 577\ 089\ 970\ 896\ 036\ 106\ 983\ 556\ 531\ 583\ 303,$

$e_3 = 3.$

The keys are given as modulus n and encryption exponent e. You, Eve the evil eavesdropper, snoop in and discover that the ciphertext sent to Alice is:

$4\ 577\ 680\ 065\ 415\ 368\ 161\ 648\ 540\ 884\ 550\ 232\ 673\ 528\ 863\ 129\ 874\ 614\ 143\ 903\ 085\ 721\ 197\ 264\ 729\ 467\ 287\ 391\ 728\ 239\ 488\ 766\ 293\ 702\ 878\ 779\ 569\ 458\ 876\ 181\ 042\ 624\ 925\ 557\ 540\ 071\ 289\ 584\ 555\ 692\ 433\ 528\ 201\ 730\ 360\ 701\ 157\ 483\ 100\ 163\ 799\ 951\ 165\ 081\ 143\ 270\ 882\ 917\ 025\ 409\ 619\ 990\ 398\ 953\ 861\ 880\ 538\ 175\ 231\ 585\ 652\ 010\ 025\ 281\ 079\ 755\ 920\ 991\ 602\ 465\ 584\ 286\ 718,$

that sent to Bob is:

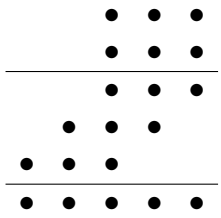
$2\ 940\ 124\ 463\ 515\ 328\ 311\ 271\ 793\ 477\ 152\ 822\ 171\ 601\ 128\ 905\ 910\ 679\ 917\ 132\ 860\ 419\ 093\ 728\ 196\ 677\ 381\ 616\ 596\ 595\ 963\ 049\ 224\ 436\ 649\ 008\ 655\ 484\ 870\ 188\ 073\ 648\ 668\ 140\ 168\ 657\ 423\ 122\ 181\ 636\ 806\ 974\ 474\ 782\ 033\ 479\ 946\ 998\ 431\ 756\ 340\ 802\ 758\ 166\ 088\ 718\ 503\ 769\ 194\ 836\ 550\ 239\ 068\ 162\ 754\ 375\ 749\ 734\ 632\ 251\ 720\ 740\ 530\ 843\ 335\ 647\ 009\ 097\ 024\ 868\ 877\ 766\ 216,$

and that sent to Charles is:

$1\ 944\ 990\ 884\ 872\ 864\ 570\ 293\ 582\ 284\ 852\ 287\ 219\ 644\ 000\ 554\ 796\ 598\ 757\ 253\ 502\ 734\ 697\ 193\ 299\ 590\ 620\ 296\ 722\ 550\ 094\ 514\ 493\ 330\ 603\ 278\ 084\ 907\ 134\ 325\ 657\ 042\ 465\ 763\ 074\ 210\ 737\ 354\ 537\ 277\ 376\ 595\ 314\ 254\ 301\ 885\ 328\ 228\ 128\ 811\ 484\ 849\ 142\ 598\ 263\ 733\ 960\ 309\ 950\ 893\ 225\ 645\ 530\ 668\ 131\ 875\ 931\ 580\ 139\ 812\ 579\ 408\ 862\ 698\ 979\ 500\ 298\ 119\ 315\ 275\ 949\ 230\ 573$

Given that all of these are encryptions of the same message, what is that message? Note that the format of the message is $2^{700} + a_1 + 256a_2 + 256^2a_3 + \cdots$, where a_j is the jth letter in ASCII.

(4) **(Note: this was solved already)** Fill in the dots with decimal digits to make into a correct multiplication algorithm and such that each digit appears at most twice.



(5) (Encryption) You intercept a message given as numbers: 168, 238, 102, 202, 124, 87, 156, 77, 186, 120, 120, 129, 243, 5, 70, 204, 182, 36, 8, 166, 224, 194, 164, 137, 79, 188, 133, 205, 240, 251, 238, 150, 3, 63, 184, 59, 117, 25. You know that the message starts with "Attack at dawn!" (without the quotation marks of course). But the rest of the message is important, find it.

Corewars

Corewars is a game in which you write a simple program (warrior) that battles another warrior in memory. It is very easy to get started and is an excellent way to learn about programming.

See `www.corewars.org` for links to lots of documentation and (free) software. The rules of the tournament will be '88 rules (simpler), the core size will be 800 (quite small), and the limit on number of instructions will be 15 (your warrior must fit within that).

I will seed some very simple stupid warriors into the tournament so that your warrior has to be at least as good enough to beat very simple strategies. If one of these very bad warriors wins, nobody gets credit.