Refer to the second page of the Course Survey for instructions on submitting written work on Gradescope.

Written problems

1. Throughout this course, we will say that an integer a is an "n-bit (nonnegative) integer" if $0 \leq a < 2^n$ (I will also sometimes use the phrase "exactly n bits long" to mean that $2^{n-1} \leq a < 2^n$, i.e. that a is an n-bit integer but not an $(n-1)$-bit integer).

   The *Data Encryption Standard* (DES) is a private-key encryption algorithm that was a government standard from 1977 to 2002. DES uses 56-bit secret keys. Suppose that Eve attempts a brute-force attack on DES by trying to decrypt an intercepted cipher text with every possible 56-bit key until she finds something that looks like English text. If Eve's system can try 1 billion keys per second, how long would it take her to try all of the keys (and thus be sure to break the encryption)?

   (By 1999, a distributed system was able to break DES encryption in less than 24 hours. DES was replaced in 2002 by a new standard, called AES, which uses keys of at least 128 bits. For "top secret" communication, the government uses AES with 256 bit keys.)

2. Textbook exercise 1.6.

3. Textbook exercise 1.9. Use a calculator/computer for the arithmetic, but show the steps.

4. Textbook exercise 1.11.

5. This problem is meant to allow you to think about how the sizes of an input to a program influence its runtime (and also to practice reading Python code), in a concrete setting. The purpose is for you to try to make some educated guesses for now; you do not need to be correct to receive full points. This problem will also be a chance for you to try out the Gradescope code submission system with some mock submissions that will not count towards your grade.

   (a) Consider the following function. It takes a positive integer n, and returns the number of divisors of n. Read the code and make sure you understand how it works.

   ```
   def numdivs(n):
       count = 0
       for d in range(1,n+1):
           if n%d == 0:
               count += 1
       return count
   ```

   Make a rough guess for how many bits long n can be before this function takes at least 1 second to finish running, and explain your reasoning. You will receive points for this problem as long as your explanation is reasonable.

   (b) On Gradescope, I've created a mock programming problem called "DEMO counting divisors" that will test this function on integers of various sizes (up to 100 bits), with a time limit of 1 second for each test case. (Any "assignment" labeled "DEMO" does not count to your grade in any way; it mereley served as a demonstration.) Use this mock problem to test your answer from part (a), as follows: copy out the code above into a file called `soln1.py`, and submit it to Gradescope. From the autograder output, how many bits could this function in fact handle in 1 second? Compare to your guess from part (a).

(c) Now consider the following alternative implementation. Briefly explain why this also correctly calculates the number of divisors of n.

```
def numdivs(n):
    count = 0
    d = 1
    while d*d < n:
        if n%d == 0:
            count += 2
        d += 1
    if d*d == n:
        count += 1
    return count
```

(d) Predict how many bits long n must be before the code in part (c) cannot finish in less than 1 second, and explain your reasoning. Then copy the code out to a file `soln2.py`, submit it to Gradescope, and see how accurate your guess was. Again, you will receive points for this problem as long as your reasoning makes sense.

Comment: You might enjoy trying to implement a more efficient solution to this problem, and testing it with the Gradesope autograder. This is certainly not in any way a required part of the course, but I'd be interested to here about any interesting ideas you have, and how many testcases you're able to solve.

Programming problems

1. The first part of this week's programming assignment is to work on an excellent Python tutorial that covers almost all of the basics that we will need for the programming in this course. Friday's class (2/1) will be devoted to giving you time to work on the tutorial while I am on hand to help you and answer questions. **You will receive full points for this part as long as you make a good-faith effort to complete the prescribed exercises by the end of next week. Please let me know if you are having difficulty or think you will require more time.** Please let me know if and where you are having trouble. I will be able to monitor your progress from my account, and see which exercises you've completed, so **you do not need to submit anything for this problem.**

   (a) Go to `https://cscircles.cemc.uwaterloo.ca/`, and create a free account. Please use your college (.edu) email address for you account, so that I can match accounts with the class list from acdata.

   (b) After making your account, go to your profile and enter `npflueger` as your "Guru's Username."

   (c) Read the tutorial and complete the exercises from the following sections:

   - Sections 0 through 10, except 2X, 6D, 7A, and 8.
   - Section 13.
   - After doing the rest, go back and work through section 6D (on debugging).

   The whole tutorial is excellent, of course, so you would benefit from doing the other sections as well. The list above identifies the parts that will be most important for our programming assignments.

If you have a lot of previous experience and complete these sections quickly, you might enjoy trying section 15C, which relates to the toy cryptosystem (Caesar cipher) we discussed on the first day.

The remaining two problems will be submitted electronically on Gradescope, and automatically graded. They will be due Friday 2/8. Here are some details/suggestions. I will demonstrate all of this in class on Monday.

- You can develop and test your code without installing anything on your computer, by going to

  `jupyter.amherst.edu`

  and logging in with your Amherst credentials (5-College students should use the same AC account they use to access Moodle). I'll show a bit about how to use Jupyter in Monday's class.
- Go to the following link to find starter code for each problem, as well as a notebook with sample cases.

  `https://www.dropbox.com/sh/jrp6f9mk08ewqnf/AABFGBvYxGr_PWkAMkEnpWNHa?dl=0`
- To use the tester notebook: on Jupyter, upload both files from the problem's folder above. Open the `.ipynb` file to see the sample test cases. Write your code into the `.py` file. To test it, run the first cell in the notebook, then run the cells with the test cases you want to check. The answer to each case is provided in a comment.
- When you want to submit your code, open the `.py` file with your code, and download it to your computer. Then find the problem on Gradescope, and upload the `.py` file to have it graded.
- The autograder will run immediately, and report your score on the problem. **You can resubmit as many times as you like,** so you do not need to wait until your code is final to try submitting.
- Please let me know of any bugs or technical difficulties!

2. Write a function `factor(n)` which takes a composite integer n (in fact, your may assume that n is a product of two prime numbers) and returns two proper factors p, q with $p, q > 1$ and $pq = n$. Your function should be efficient enough to finish in less that one second when n is 40 bits long or less. Half of the test cases will consist of integers 20 bits long or less, so you will receive at least half credit if your implementation can factor these in less than a second each. Submit your solution to the Gradescope assignment "PSet 1 factor."

3. Write a function `gcdList(ls)` which takes a list of positive integers, whose sizes may be as large as 1024 bits, and returns the greatest common divisor of the entire list. Half of the test cases will consists of lists of exactly two elements, so you can begin by writing a function to efficiently compute the gcd of two numbers, which will receive at least half of the points. Submit your solution to the Gradescope assignment "PSet 1 gcdList."