Please write your hackerrank username somewhere on your problem set.
Written problems are due at the beginning of class on Friday, November 6. Programming problems must be electronically submitted by 10:50am according to the instructions on problem set 1. The submission page for the programming questions is the following.

`https://www.hackerrank.com/math158-problem-set-7/`

You should use a calculator or computer for the arithmetic in several of the written problems.

Written problems

1. Textbook exercise 4.5.
2. Textbook exercise 4.6.
3. Textbook exercise 4.9.
4. Textbook exercise 4.10.
5. Textbook exercise 4.8.
6. (a) Let $f(n)$ denote the probability that two numbers chosen uniformly at random from the first n positive integers are relatively prime. Calculate $f(100k)$ for $k = 1, 2, \cdots, 10$. What appears to be the long-term behavior of the function $f(n)$?
   (b) Calculate the product of $(1 - \frac{1}{p^2})$, where p ranges over all primes up to 100. Give an informal explanation why the result appears to resemble the numbers you computed in part (a).
7. Textbook exercise 5.5.
8. Textbook exercise 5.6.
9. Textbook exercise 5.7.

Programming problems

10. Write a program that verifies whether or not a given DSA signature is valid. You will be given the public parameters and public key, and a document with a purported signature.
11. Problem 5 showed that a pair of ElGamal signatures using the same ephemeral key can accidentally give away the signer's private key. The same is true in DSA – write a program which take public paramters and a public key for DSA, along with two signed documents that have been signed with the same ephemeral key, and computes the signer's private key from this information.
12. Suppose that a fair coin is flipped n times, where $n \leq 500$. Write a program which computes the probability that the number of heads shown is between a and b inclusive, where a, b are two given integers. You should print the answer as the numerator and the denominator of a reduced fraction.