**Please write your hackerrank username somewhere on your problem set.**
Written problems are due at the beginning of class on Friday, October 30. 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-6/`

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

### Written problems

1. Textbook exercise 3.12.
2. Prove that if $N = pq$, where $p, q$ are distinct *odd* prime numbers, then the congruence $x^2 \equiv 1 \pmod{N}$ has exactly *four* distinct solutions (modulo $N$).

   *Hint.* Use the Chinese remainder theorem.
3. For each number $n$ between $100,000$ and $100,019$ (inclusive), determine how many numbers $a \in \{1, 2, \cdots, n-1\}$ are Miller-Rabin witnesses (you should write some code to do this; briefly summarize how your code works and simply copy out the resulting numbers). Which of these numbers are prime? Which number has the lowest proportion of witnesses, and what it this portion?
4. Divide the integers from 1 to $1,000,000$ into ten equal intervals. For each interval, determine how many primes are in that interval. Also determine how many of these primes are congruent to $1 \pmod 4$ and how many are congruent to $3 \pmod 4$. Which of these tends to be a larger number?

   *Note.* You can use the Miller-Rabin test for this problem, but you are free to use any other method you prefer. For example, the Sieve of Eratosthenes may be faster for this particular problem.
5. Textbook exercise 3.19.
6. Textbook exercise 3.20, parts (a), (b) and (c).
7. Textbook exercise 3.21.
8. Textbook exercise 4.1.
9. Textbook exercise 4.2.

### Programming problems

10. Write a program to decipher an RSA message sent to you using your public key. You will be given your public key, as well as the two prime numbers that you used to create it, and a cipher text $c$.

11. Write a program that determines whether a given integer (up to 1024 bit in size) is prime or not.

12. Write a program that generates three numbers $p, q, g$ with the following properties.

    - $p$ and $q$ are primes of specified length in bits.
    - $p \equiv 1 \pmod{q}$
    - $g \in \mathbf{Z}/p$ has order $q$ modulo $p$.

    Your program will receive the desired lengths (number of bits) for $p$ and $q$, and should print $p, q$ and $g$.

    *Hint.* See the solution to problems 5 and 6 on problem set 3; these should help you see how to construct the number $g$ once you have chosen $p$ and $q$.