All exercise numbers from the textbook refer to the **second edition**.
Problems 8, 9, and 12 refer to material we will not discuss until Monday (§2.4 of the text).

Written problems

1. Textbook exercise 1.35.

   Remark. A prime p such that $q = \frac{1}{2}(p-1)$ is also prime is called a *safe prime,* because the discrete logarithm problem modulo p is particularly difficult, for reasons we'll see soon. The corresponding prime q is called a *Sophie Germain prime*. Germaine originally studied these primes in the 19th century in connection with work on Fermat's last theorem.

2. Textbook exercise 2.3.

3. Textbook exercise 2.11.

4. Textbook exercise 2.12.

5. Consider the set $\mathbf{N}$ of positive integers, equipped with the following operation.

   $$x \star y = \max(x, y)$$

   Show that $(\mathbf{N}, \star)$ satisfies all of the conditions in the definition of a group (as on page 74 of the textbook) except one. Which condition does not hold?

6. (a) Consider the set M consisting of all 2×2 matrices with integer entries, with the operation $\cdot$ being ordinary matrix multiplication. Show that $(M, \cdot)$ is *not* a group.
   (b) Let G denote the subset of M consisting of those matrices with determinant ± 1. Show that $(G, \cdot)$ *is* a group. (This group is usually denoted $\mathrm{GL}_2(\mathrm{Z})$ and is called the *general linear group of degree* 2 *over* $\boldsymbol{Z}$).
   (c) Show that $(G, \cdot)$ is not a *commutative* group.

7. Let $(G, \star)$ be a group, and assume that $|G|$ is a prime number p. For $e \geq 0$, denote by $g^{\star e}$ the element $g \star g \star \cdots \star g$, where g appears e times. Prove that if e is a positive integer not divisible by p, then the function $f : G \to G$ given by $f(g) = g^{\star e}$ is a one-to-one function.

8. Textbook exercise 2.8.

9. Textbook exercise 2.10.

Programming problems

Full formulation and submission: `https://www.hackerrank.com/m158-2016-pset-3`

10. Write a program that breaks Diffie-Hellman for 16-bit primes. That is, you will receive as input the paramters g, p (where $p < 2^{16}$ and elements A, B, and you must determine the shared secret S. (16-bit primes are small enough that a fairly naive approach will work).

11. Given an integer m and the four entries of a 2×2 matrix A, and a *positive* integer e (up to 1024 bits long), determine the result of reducing all entries of the matrix A^e modulo m. (You will want to reduce the entries of matrices "along the way;" it will not be feasible to compute the entries of the matrix A^e in full).

12. Write a program which deciphers a message enciphered to you with Elgamal encryption, given the parameters p, g and your private key. The length of the prime p will be up to 1024 bits.