All exercise numbers from the textbook refer to the **second edition**.

1. Exercise 2.30. Show complete details for each argument, clearly indicating which axioms or previously-proved statements you are using.
2. Exercise 2.32.
3. Exercise 2.33.
4. Exercise 2.35, part (d) only.
5. Exercise 2.36, part (d) only.
6. Consider the following variant of EC Diffie-Hellman key exhange, in which Alice and Bob only exchange individual numbers, rather than both coordinates of a point on an elliptic curve.

   - **Public parameter creation:** same as in table 6.5.
   - **Private computations:** same as in table 6.5.
   - **Public exchange of values:** Alice sends *the x-coordinate* of Q_A to Bob; Bob sends *the x-coordinate* of Q_B to Alice.
   - **Further private computations**: Both Alice and Bob determine the *x-coordinate* of $(n_A \cdot n_B)P$. This is their shared secret value.

   (a) Prove that if Q, Q' are two points on an elliptic curve with the same x-coordinate, and n is any integer, then nQ and nQ' also have the same x-coordinate.

   (b) Describe how Alice is able to (efficiently) determine the shared secret, using only the information that she knows. You may assume that Alice has an efficient algorithm to determine square roots modulo p.

   (c) What advantages, if any, does this system have over the usual ECDH system described in table 6.5?

   Note. You will implement a function to perform the task Alice and Bob must perform in the last programming problem.
7. Exercise 7.1.

Programming problems

Full formulation and submission: `https://www.hackerrank.com/m158-2016-pset-10`

8. Implement functions to add and multiply elements of the polynomial ring $\mathbf{F}_p[x]$.
9. Implement a function to perform division with remainder in $\mathbf{F}_p[x]$. That is, given two polynomials $a, b \in \mathbf{F}_p[x]$, you must determine polynomials k, r (the quotient and the remainder) such that $a = k \cdot b + r$ and $\deg r < \deg b$.
10. Implement the extended Euclidean algorithm for $\mathbf{F}_p[x]$. You will be given polynomials a, b of different degrees[1], and must find polynomials u, v, g such that $au + bv = g$, and g is the greatest common divisor of a and b. You should return a choice of u, v, g such that g is *monic* (i.e. the higest-degree coefficient is 1) and u, v have the smallest possible degree.

[1] It is not essential to assume that the degrees are different, but it may simplify some analysis.

11. Given an elliptic curve over $\mathbf{F}_p$, where $p \equiv 3 \pmod 4$, a positive integer n, and *the x-coordinate of* a point P on the curve, determine the x-coordinate of $n \cdot P$. Such a function could be used to do the variant of EC Diffie-Hellman mentioned in problem 6. You will want to use a fact mentioned in Proposition 2.26 in order to do part of this computation.

12. (Extra credit) Do the same task as the previous problem, in the case $p \equiv 1 \pmod 4$. You will need to do some research to find an efficient algorithm to compute square roots modulo p.