1.) Let

$$\mathbb{F}_{2^{128}} \;=\; \left\{ \sum_{i=0}^{127} a_i x^i \;\middle|\; a_i \in \mathbb{F}_2 \right\}$$

with multiplication defined by reduction with respect to the irreducible polynomial:

$$p(x) \;:=\; 1 + x + x^2 + x^7 + x^{128}$$

Show that the product of two elements $a(x) = \sum_{i=0}^{127} a_i x^i$ and $b(x) = \sum_{i=0}^{127} b_i x^i$ of $\mathbb{F}_{2^{128}}$ can be calculated with the following algorithm:

(1) Let $\mathbf{z} = (z_0, \ldots, z_{127})$ and $\mathbf{v} = (v_0, \ldots, v_{127})$ be variables to store elements of ${\mathbb{F}_2}^{128}$.

(2) Initialize all entries of $\mathbf{z}$ with 0 and $\mathbf{v}$ with the coefficients of $b(x)$:

$$\mathbf{z} \;:=\; (0, \ldots, 0)$$

$$\mathbf{v} \;:=\; (b_0, b_1, \ldots, b_{127})$$

(3) For $i = 0$ to 127 do:

$$\mathbf{z} \;=\; \begin{cases} \mathbf{z} & \text{if } \; a_i = 0 \\ \mathbf{z} + \mathbf{v} & \text{if } \; a_i = 1 \end{cases}$$

$$\mathbf{v} \;=\; \begin{cases} (0, v_0, v_1, \ldots, v_{126}) & \text{if } \; v_{127} = 0 \\ (1, v_0 + 1, v_1 + 1, v_2, v_3, v_4, v_5, v_6 + 1, v_7 \ldots, v_{126}) & \text{if } \; v_{127} = 1 \end{cases}$$

(4) Return the values stored in $\mathbf{z} = (z_0, \ldots, z_{127})$, which are the coefficients of the product of $a(x)$ and $b(x)$ in $\mathbb{F}_{2^{128}}$, i. e.:

$$a(x) \cdot b(x) \bmod p(x) \;=\; \sum_{i=0}^{127} z_i x^i$$

(See also section 6.3 of NIST Special Publication 800-38D.)

2.) Use the AES implementation of your JRE to validate the test cases 4, 11 and 18 of the original publication The Galois/Counter Mode of Operation (GCM) of D. A. McGrew and J. Viega.

Hint: An example that shows how to supply the input data (in particular the "additional data") to a `Cipher` instance in order to run AES in GCM mode can be found in the description of the `Cipher` class in the Security Developer's Guide, Sec. 2 - Java Cryptography Architecture (JCA) Reference Guide, Core Classes and Interfaces, The Cipher Class.

3.) Let p be a prime and g be a primitive element of $\mathbb{Z}_p^*$. Furthermore, let $\mathcal{S}$ denote the set of all squares in $\mathbb{Z}_p$:

$$\mathcal{S} \;:=\; \{a^2 \mid a \in \mathbb{Z}_p\}$$

(i) List all $i \in \{0, 1, 2, \ldots, p-2\}$ with $g^i \in \mathcal{S}$.

(ii) Determine $|\mathcal{S}|$.

(iii) Show:

$$a^{\frac{p-1}{2}} \;=\; \begin{cases} 1 & \text{if } \; a \in \mathbb{Z}_p^* \cap \mathcal{S} \\ -1 & \text{if } \; a \in \mathbb{Z}_p^* \setminus \mathcal{S} \end{cases}$$

4.) Let p be a prime with

$$p \bmod 4 = 3$$

and let $a \in \mathbb{Z}_p^*$ be a square.

Show that the square roots of a are given by $\pm a^{\frac{p+1}{4}}$.

5.) Let $G = E(\mathbb{F}_q)$ denote the group of points of an elliptic curve. (Or just any finite abelian group G.) Proof the following:

(i) For every $P \in G$ there exits some $k \in \mathbb{N}$ such that $k \cdot P = \mathcal{O}$. The smallest $k \in \mathbb{N}$ with $k \cdot P = \mathcal{O}$ is called the order of P and denoted by:

$$o(P) \;:=\; \min\{k \in \mathbb{N} \mid k \cdot P = \mathcal{O}\}$$

(ii) The cyclic subgroup generated by $P \in G$

$$\langle P \rangle \;:=\; \{k \cdot P \mid k \in \mathbb{N}\}$$

contains exactly $o(P)$ many elements, namely:

$$P, \quad 2 \cdot P, \quad 3 \cdot P, \ldots, \quad (o(P)-1) \cdot P, \quad o(P) \cdot P = \mathcal{O}$$

(iii) If $k \cdot P = \mathcal{O}$ then $o(P) \mid k$.

(iv) If $Q \in \langle P \rangle$ then $o(Q) \mid o(P)$.

(v) If $\gcd(k, o(P)) = 1$ then $o(k \cdot P) = o(P)$ and $\langle k \cdot P \rangle = \langle P \rangle$.

(vi) If $\gcd(o(P), o(Q)) = 1$ then $P, Q \in \langle P + Q \rangle$ and $o(P + Q) = o(P) \cdot o(Q)$.

6.) Let $E(\mathbb{F}_{11})$ denote the set of points of the elliptic curve defined by

$$y^2 \;=\; x^3 + 1$$

over $\mathbb{F}_{11}$.

(i) Enumerate all points of $E(\mathbb{F}_{11})$.

(ii) Let $P, Q \in E(\mathbb{F}_{11})$ with $P = (0, 1)$ and $Q = (5, 4)$. Show: $o(P) = 3$ and $o(Q) = 4$.

(iii) Calculate $R = P + Q$ and justify that R is a generator of $E(\mathbb{F}_{11})$, i. e. $\langle R \rangle = E(\mathbb{F}_{11})$.

7.) Complete the implementations of the methods `add()` and `doublePt()` in the provided Java class file `EC.java`.

Check your implementation with the tests provided in the method `EC.test_01()`.

8.) The provided Java class file `EC.java` contains the implementation of a method `multiply()`, which can be used to efficiently compute positive multiples $k \cdot P$ of a point P of an elliptic curve.

Analyse and explain the algorithm used in the implementation.

Given the bit length $l = l_2(k) := \lfloor \log_2(k) \rfloor + 1$ of k, how many of the basic elliptic curve operations `add()` and `doublePt()` have to be performed at most?