Elliptic Curves - List 2

Task 1 (3 pts) The task is composed of the following steps:

(a) Install `SageMath` (`https://www.sagemath.org/`)

(b) Download `ec-prime-order.sage` script from the webpage of the course.

(c) Run `sage` and load the script with the following sage command:

```
load("ec-prime-order.sage")
```

(d) Generate two elliptic curves and corresponding basepoints with the calls

```
generateDomainParameters(bitLength)
```

succesively for `bitLength` equal to 40 and 60. The normalized projective coordinates of the base point generated means that the first two coordinates are equal to the affine coordinates of the point.

Task 2 (5 pts) Implement the elliptic curve group operation in affine coordinates: addition of two different points, and doubling a point.

Task 3 (7 pts) Modify your implementation of the Pollard-ρ method to solve DLP on elliptic curves (use the arithmetic implemented in Task 2). Run the modification on both instances generated in Task 1.