Problems

9.1. Show that the condition $4a^3 + 27b^2 \neq 0 \bmod p$ is fulfilled for the curve

$$y^2 \equiv x^3 + 2x + 2 \bmod 17 \tag{9.3}$$

9.2. Perform the additions

1. $(2,7) + (5,2)$
2. $(3,6) + (3,6)$

in the group of the curve $y^2 \equiv x^3 + 2x + 2 \bmod 17$. Use only a pocket calculator.

9.3. In this chapter the elliptic curve $y^2 \equiv x^3 + 2x + 2 \bmod 17$ is given with $\#E = 19$. Verify Hasse's theorem for this curve.

9.4. Let us again consider the elliptic curve $y^2 \equiv x^3 + 2x + 2 \bmod 17$. Why are *all* points primitive elements?

Note: In general it is not true that all elements of an elliptic curve are primitive.

9.5. Let E be an elliptic curve defined over $\mathbb{Z}_7$:

$$E : y^2 = x^3 + 3x + 2.$$

1. Compute all points on E over $\mathbb{Z}_7$.
2. What is the order of the group? (Hint: Do not miss the neutral element $\mathcal{O}$.)
3. Given the element $\alpha = (0,3)$, determine the order of α. Is α a primitive element?

9.6. In practice, a and k are both in the range $p \approx 2^{150} \cdots 2^{250}$, and computing $T = a \cdot P$ and $y_0 = k \cdot P$ is done using the Double-and-Add algorithm as shown in Sect. 9.2.

1. Illustrate how the algorithm works for $a = 19$ and for $a = 160$. Do *not* perform elliptic curve operations, but keep P a variable.
2. How many (i) point additions and (ii) point doublings are required on average for one "multiplication"? Assume that all integers have $n = \lceil \log_2 p \rceil$ bit.
3. Assume that all integers have $n = 160$ bit, i.e., p is a 160-bit prime. Assume one group operation (addition or doubling) requires 20 μsec. What is the time for one double-and-add operation?

9.7. Given an elliptic curve E over $\mathbb{Z}_{29}$ and the base point $P = (8,10)$:

$$E : y^2 = x^3 + 4x + 20 \bmod 29.$$

Calculate the following point multiplication $k \cdot P$ using the Double-and-Add algorithm. Provide the intermediate results after each step.

1. $k = 9$
2. $k = 20$

9.8. Given is the same curve as in 9.7. The order of this curve is known to be $\#E = 37$. Furthermore, an additional point $Q = 15 \cdot P = (14, 23)$ on this curve is given. Determine the result of the following point multiplications by using as few group operations as possible, i.e., make smart use of the known point Q. Specify *how* you simplified the calculation each time.

Hint: In addition to using Q, use the fact that it is easy to compute $-P$.

1. $16 \cdot P$
2. $38 \cdot P$
3. $53 \cdot P$
4. $14 \cdot P + 4 \cdot Q$
5. $23 \cdot P + 11 \cdot Q$

You should be able to perform the scalar multiplications with considerably fewer steps than a straightforward application of the double-and-add algorithm would allow.

9.9. Your task is to compute a session key in a DHKE protocol based on elliptic curves. Your private key is $a = 6$. You receive Bob's public key $B = (5, 9)$. The elliptic curve being used is defined by

$$y^2 \equiv x^3 + x + 6 \bmod 11.$$

9.10. An example for an elliptic curve DHKE is given in Sect. 9.3. Verify the two scalar multiplications that Alice performs. Show the intermediate results within the group operation.

9.11. After the DHKE, Alice and Bob possess a mutual secret point $R = (x, y)$. The modulus of the used elliptic curve is a 64-bit prime. Now, we want to derive a session key for a 128-bit block cipher. The session key is calculated as follows:

$$K_{\text{AB}} = h(x||y)$$

Describe an *efficient* brute-force attack against the symmetric cipher. How many of the key bits are truly random in this case? (Hint: You do not need to describe the mathematical details. Provide a list of the necessary steps. Assume you have a function that computes square roots modulo p.)

9.12. Derive the formula for addition on elliptic curves. That is, given the coordinates for P and Q, find the coordinates for $R = (x_3, y_3)$.

Hint: First, find the equation of a line through the two points. Insert this equation in the elliptic curve equation. At some point you have to find the roots of a cubic polynomial $x^3 + a_2x^2 + a_1x + a_0$. If the three roots are denoted by x_0, x_1, x_2, you can use the fact that $x_0 + x_1 + x_2 = -a_2$.