Sommersemester 2025 Blatt 6

1. Questions

(1) Write down a parametrisation of the rational sphere
$$S = \{(x, y, z) \in \mathbb{Q} \colon x^2 + y^2 + z^2 = 1\}$$

(2) (Fermat's Little Theorem.) Let p be a prime number. Show that for any $a \in \{1, \ldots, p-1\}$, we have
$$a^{p-1} \equiv 1 \mod p.$$

(3) Consider the cubic equation
$$y^2 = x^3 - 4x + 1$$
over $\mathbb{Q}$ and set
$$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 \colon y^2 = x^3 - 4x + 1\}.$$

(a) Construct a recursive procedure generating (not necessarily all) points on $E(\mathbb{Q})$ using the secant method (see the comments).

(b) Starting with $(x_1, y_1) = (4, 7)$, compute the next two points (x_2, y_2) and (x_3, y_3).

2. Comments

(1) (a) Describe a line L passing through, say $(0, 0, 1) \in S$ in terms of two linear equations in variables x, y, z.

(b) Find and describe the points contained in S and L.

(2) (a) Start with showing that $(x + y)^p = x^p + y^p$ modulo p.

(b) The proof will be by induction on a.

(c) You will first show that $a^p \equiv a \mod p$. Then, since $a \not\equiv 0 \mod p$, you will be able to divide.

(3) Here is how the secant method will work:

(a) Set $(x_0, y_0) = (0, 1) \in E(\mathbb{Q})$. You should first check that we actually have $(0, 1) \in E(\mathbb{Q})$.

(b) Set (x_1, y_1) to be a point in $E(\mathbb{Q})$ which is different than $(0, 1)$. Construct the line between L_1 through (x_0, y_0) and (x_1, y_1). Show that this line L_1 intersects $E(\mathbb{Q})$. How many points are there in the intersection? In your computation, you are going to get an x-value. Call that value x_2. Then plug it in the equation for L_1 to obtain the y-value y_2^*. So, now you have created a point (x_2, y_2^*) on $E(\mathbb{Q})$. Is this different than (x_1, y_1)? Is it different than (x_0, y_0)?

(c) In order to make sense of the above item, try to find a point $(x_1, y_1) = (X, Y)$ on $E(\mathbb{Q})$ which is different than $(0, 1)$ and $(4, 7)$ and actually construct $(U, V) = (x_2, y_2^*)$. Then, do the same procedure by letting $(x_1, y_1) = (U, V)$. Check that in this case, you will get $(x_2, y_2^*) = (X, Y)$.

(d) Show that what you observed in (c) holds more generally. That is, if you construct the line through (x_0, y_0) and (x_2, y_2^*) and intersect with $E(\mathbb{Q})$, you will get (x_1, y_1).

(e) In order to make this a recursive procedure which keeps generating new points, put $y_2 = -y_2^*$ and show that (x_2, y_2) lies on $E(\mathbb{Q})$. Then, continue with (x_2, y_2) to generate new points (x_3, y_3^*) and (x_3, y_3) as above.

(f) You should now write down the general rule for this procedure.