Let $\Bbbk$ be a field of characteristic not 2 and $A, B \in \Bbbk$ such that $4A^3 + 27B^2 \neq 0$. An elliptic curve is an equation $E : y^2 = x^3 + Ax + B$ (or, more accurately, the corresponding projective curve).

Let $P, Q \in E(\Bbbk)$. The group operation "$P + Q$" on E is as follows: Draw the line between P and Q; let R be the third point of intersection, draw a vertical line through R (officially, a line between ∞ and R); let S be the third point of intersection; then $P + Q = S$.

Algebraic formulae for group operation: Let $P, Q \in E(\Bbbk)$.

- If $P = \infty$ then return Q.
- If $Q = \infty$ then return P.
- Write $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$.
- If $x_P = x_Q$ and $y_P = -y_Q$ then return ∞.
- If $x_P = x_Q$ and $y_P = y_Q$ then set
$$\lambda = (3x_P^2 + A)/(2y_P),$$
else set
$$\lambda = (y_Q - y_P)/(x_Q - x_P).$$
- The line between P and Q is $y = \lambda(x - x_P) + y_P$.
- Compute $x_S = \lambda^2 - x_P - x_Q$ and $y_S = \lambda(x_S - x_P) + y_P$.
- Return $(x_S, -y_S)$.

Theorem 25.1. The operation defined above is a group operation. More specifically:

- There is an identity element, namely ∞, so $P + \infty = \infty + P = P$ for all points $P \in E(\Bbbk)$.
- If $P = (x_P, y_P)$ then define $-P = (x_P, -y_P)$. Then $P + (-P) = \infty$.
- $P + (Q + R) = (P + Q) + R$ and so the operation is associative.
- $P + Q = Q + P$, and so the operation is commutative.

Example 25.2. Let $E : y^2 = x^3 + x + 3$ and $P = (2, 3)$. Then $P + P = (0, 1)$ and $P + (0, 1) = (-1, 0)$.

Definition 25.3. For $n \in \mathbb{N}$ define $[n]P = P + \cdots + P$ (n times). The **order** of P is the smallest positive integer (if it exists) such that $[n]P = \infty$.

Exercise 25.4. Let $E : y^2 = x^3 + x + 3$ and $P = (-1, 1)$. Compute $[2]P$ and $[3]P$.

Exercise 25.5. Prove that the doubling and addition cases can be unified using the formula $\lambda = (x_P^2 + x_P x_Q + x_Q^2 + A)/(y_P + y_Q)$.

Lemma 25.6. $P = (x_p, y_P) \in E(\Bbbk)$ has order 2 if and only if $y_P = 0$. (An alternative criterion: $x_P^3 + Ax_p + B = 0$.)

Corollary 25.7. There are at most three points of order equal to 2 on an elliptic curve.

Exercise 25.8. Prove that $[3](x_P, y_P) = \infty$ if and only if
$$3x_P^4 + 6Ax_P^2 + 12Bx_P - A^2 = 0.$$
Hence deduce that there are at most 8 points of order equal to 3 on an elliptic curve.

Theorem 25.9. Let l be a prime. There are at most $l^2 - 1$ points of order l on an elliptic curve.