

curve over K is the set of points (x, y) with $x, y \in K$ which satisfy the equation

$$y^2 = x^3 + ax + b, \quad (1)$$

together with a single element denoted O and called the “point at infinity” (about which more will be said below).

If K is a field of characteristic 2, then an *elliptic curve over K* is the set of points satisfying an equation of type either

$$y^2 + cy = x^3 + ax + b \quad (2a)$$

or else

$$y^2 + xy = x^3 + ax^2 + b \quad (2b)$$

(here we do not care whether or not the cubic on the right has multiple roots) together with a “point at infinity” O .

If K is a field of characteristic 3, then an *elliptic curve over K* is the set of points satisfying the equation

$$y^2 = x^3 + ax^2 + bx + c \quad (3)$$

(where the cubic on the right has no multiple roots) together with a “point at infinity” O .

Remarks. 1. There’s a general form of the equation of an ellipse which applies to any field: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, which when $\text{char } K \neq 2$ can be transformed to $y^2 = x^3 + ax^2 + bx + c$ (and to the form $y^2 = x^3 + bx + c$ if $\text{char } K > 3$). In the case when the field K has characteristic 2, this equation can be transformed either to (2a) or (2b).

2. If we let $F(x, y) = 0$ be the implicit equation for y as a function of x in (1) (or (2), (3)), i.e., $F(x, y) = y^2 - x^3 - ax - b$ (or $F(x, y) = y^2 + cy + x^3 + ax + b$, $y^2 + xy + x^3 + ax + b$, $y^2 - x^3 - ax^2 - bx - c$), then a point (x, y) on the curve is said to be *non-singular* (or a *smooth* point) if at least one of the partial derivatives $\partial F / \partial x$, $\partial F / \partial y$ is nonzero at the point. (Derivatives of polynomials can be defined by the usual formulas over any field; see paragraph 5 at the beginning of Chapter II.) It is not hard to show that the condition that the cubic on the right in (1) and (3) not have multiple roots is equivalent to requiring that all points on the curve be nonsingular.

Elliptic curves over the reals. Before discussing some specific examples of elliptic curves over various fields, we shall introduce a centrally important fact about the set of points on an elliptic curve: they form an abelian group. In order to explain how this works visually, for the moment we shall assume that $K = \mathbf{R}$, i.e., the elliptic curve is an ordinary curve in the plane (plus one other point O “at infinity”).

Definition. Let E be an elliptic curve over the real numbers, and let P and Q be two points on E . We define the negative of P and the sum $P + Q$ according to the following rules: