2 Elliptiske kurver over endelige legemer

Vi skal i dette kapitel undersøge elliptiske kurver over endelige legemer. Lad $\mathbb{F}$ være et endeligt legeme og lad E være en elliptisk kurve på formen

$$y^2 = x^3 + Ax + B,$$

som er defineret over $\mathbb{F}$. Da er gruppen $E(\mathbb{F})$ endelig, da der kun findes endeligt mange talpar (x, y) hvor $x, y \in \mathbb{F}$. Disse elliptiske kurver viser sig, at have flere praktiske anvendelser og vi vil i kapitel 3 vise, hvordan de kan anvendes til faktorisering.