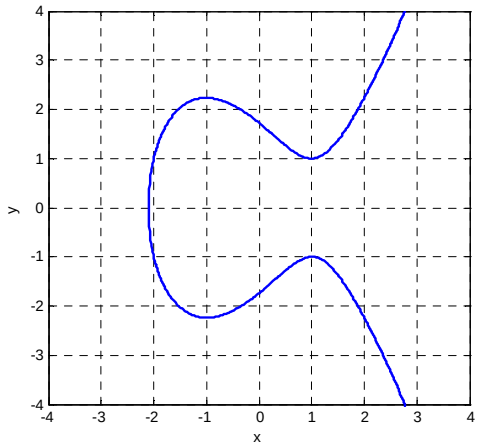

Figur 139: Beispiel einer elliptischen Kurve.

Die Berechnung des Schnittpunkts zwischen einer beliebigen Gerade

$$g : y = mx + b$$

und der elliptischen Kurve

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

führt auf kubische Gleichungen:

$$(mx + b)^2 + a_1x(mx + b) + a_3(mx + b) = x^3 + a_2x^2 + a_4x + a_6$$
$$\vdots$$
$$x^3 + x^2(a_2 - m^2 - a_1m) + x(a_4 - 2mb - a_1b - a_3m) + a_6 - b^2 - a_3b = 0\,.$$

welche entweder eine oder drei reelle Lösungen besitzen. Eine Gerade durch zwei Punkte der elliptischen Kurve muss diese also in einem dritten Punkt schneiden.

24.3.1 Addition von Punkten

Auf elliptischen Kurven wird die Addition[44] von zwei Punkten wie folgt definiert.

[44] Dass wir die beschriebene Verknüpfung als Addition bezeichnen, ist ziemlich willkürlich. Ebenso gut könnte man sie als Multiplikation bezeichnen.