Die Gruppenverknüpfung für Kurven in Weierstraßscher Normalform

In der letzten Vorlesung haben wir gesehen, daß man die Punkte einer elliptischen Kurve zu einer Gruppe machen kann durch die Bedingung, daß die Summe dreier Punkte genau dann gleich dem Neutralelement O sein soll, wenn die Punkte auf einer Geraden liegen. Das Neutralelement O mußte dazu als Wendepunkt gewählt werden.

Die Gruppenstruktur ist wesentlich für die Anwendung elliptischer Kurven in der Kryptographie, für Primzahltests, für die Faktorisierung ganzer Zahlen und vieles Anderes; es ist daher wichtig, daß wir die Summe zweier Punkte einfach und effizient berechnen können.

Dazu sollte insbesondere die Gleichung der Kurve möglichst einfach sein; wir beschränken uns daher auf Körper k, deren Charakteristik von zwei und drei verschieden ist und auf Kurven E, die als Nullstellenmenge eines WEIERSTRASS-Polynoms

$$Y^2Z = X^3 + aXZ^2 + bZ^3 \qquad \text{mit} \qquad a, b \in k, \quad 4a^3 + 27b^2 \neq 0$$

dargestellt werden können. Auf der durch das Verschwinden der homogenen Koordinate Z gegebenen Geraden liegt dann nur der Punkt $O = (0 : 1 : 0)$, von dem wir wissen, daß er ein Wendepunkt ist. Diesen Punkt nehmen wir als Neutralelement.

Für das praktische Rechnen sind affine Koordinaten natürlich bequemer und effizienter als homogene; da es nur einen einzigen unendlichfernen Punkt gibt, empfiehlt es sich daher, die Fälle, in denen dieser als Summand oder Ergebnis auftritt, gesondert zu behandeln, und in allen anderen Fällen affin zu rechnen. Wir betrachten somit den Punkt O sowie Punkte $(x, y) \in k^2$ mit $y^2 = x^3 + ax + b$. Letztere bezeichnen wir kurz, aber schlampig, als *affine Punkte.* Tatsächlich ist natürlich *jeder* Punkt der projektiven Ebene ein nulldimensionaler affiner (und projektiver) Raum, aber die gewählte Sprechweise ist bequem und für den Umgang mit elliptischen Kurven in WEIERSTRASS-Normalform auch nützlich.

Da wir O zum Neutralelement gemacht haben, ist $P + O = O + P = P$ für alle Punkte P, und da O als Neutralelement sein eigenes Inverses ist, ist $P + Q = O$ genau dann, wenn P, Q und O auf einer Geraden

liegen. Die Geraden durch O sind genau die zur y-Achse des affinen Koordinatensystems parallelen Geraden; somit ist $P + Q = O$ für zwei verschiedene Punkte P, Q genau dann, wenn P und Q die gleiche x-Koordinate, aber verschiedene y-Koordinaten haben. $2P = O$ gilt einerseits für $P = O$; für einen affinen Punkt $P = (x, y)$ gilt es genau dann, wenn die Tangente im Punkt P parallel zur y-Achse ist, und das ist genau dann der Fall, wenn die y-Koordinate verschwindet. Für zwei affine Punkte $P = (x_1, y_1)$ und $Q = (x_2, y_2)$ ist also $P + Q = O$ genau dann, wenn entweder $x_1 = x_2$ und $y_1 \neq y_2$ ist, oder $x_1 = x_2$ und $y_1 = y_2 = 0$. In allen anderen Fällen ist auch das Ergebnis ein affiner Punkt.

Ist $x_1 = x_2$ und $y_1 \neq y_2$, muß wegen $y^2 = x^3 + ax + b$ natürlich $y_2 = -y_1$ sein. Wir wir gerade gesehen haben, ist dann die Summe der beiden Punkte gleich O, d.h. sie sind invers zueinander. Dies zeigt insbesondere, daß sich Inverse auf einer Kurve in WEIERSTRASS-Normalform sehr einfach berechnen lassen: Für $P = (x, y)$ ist $-P = (x, -y)$. Dies gilt auch für $y = 0$, denn wie wir auch gesehen haben, ist ein Punkt mit Koordinaten $(x, 0)$ zu sich selbst invers.

Seien nun $P = (x_1, y_1)$ und $Q = (x_2, y_2)$ zwei beliebige, aber verschiedene affine Punkte der Kurve. Wir wollen die Koordinaten von $P + Q$ berechnen.

Falls $x_1 = x_2$ ist, muß wegen der Verschiedenheit der Punkte $y_1 \neq y_2$ sein, und für diesen Fall kennen wir bereits das Ergebnis $P + Q = O$.

Für $x_1 \neq x_2$ bestimmen wir zunächst die Gerade durch P und Q. Sie hat die Steigung $m = (y_2 - y_1)/(x_2 - x_1)$, und da P auf der Geraden liegt, hat sie die Gleichung

$$y = m(x - x_1) + y_1 = mx + (y_1 - mx_1) \qquad \text{mit} \qquad m = \frac{y_2 - y_1}{x_2 - x_1}\,.$$

Diese Gleichung setzen wir ein in die WEIERSTRASS-Gleichung

$$y^2 = x^3 + ax + b$$

und erhalten $\big(mx + (y_1 - mx_1)\big)^2 = x^3 + ax + b$ oder

$$x^3 - m^2x^2 + \big(a - 2m(y_1 - mx_1)\big)x + b - (y_1 - mx_1)^2 = 0\,.$$

Das ist eine kubische Gleichung für die x-Koordinaten der drei Schnittpunkte der Geraden mit der elliptischen Kurve, und sie sieht nicht sehr angenehm aus. Zum Glück kennen wir aber bereits die beiden Lösungen x_1 und x_2, denn P und Q sind natürlich Schnittpunkte. Wir brauchen nur noch die x-Koordinate x_3 des dritten Schnittpunkts. Nach dem Wurzelsatz von VIÉTE (oder indem man beachtet, daß die linke Seite das Produkt $(x-x_1)(x-x_2)(x-x_3)$ ist) folgt, daß $x_1+x_2+x_3 = m^2$ sein muß, d.h.

$$x_3 = m^2 - x_1 - x_2 \,.$$

Die y-Koordinate des dritten Schnittpunkts können wir über die Geradengleichung berechnen, allerdings interessiert uns ja nicht dieser Schnittpunkt, sondern sein Inverses, bei dem die y-Koordinate das entgegengesetzte Vorzeichen hat. Der Punkt $P+Q$ hat somit die Koordinaten (x_3, y_3) mit

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad m = \frac{y_2 - y_1}{x_2 - x_1} \,.$$

Bleibt noch der Fall $P = Q = (x_1, y_1)$. Hier müssen wir die Tangente im Punkt P betrachten. Im Falle $y_1 = 0$ ist diese parallel zur y-Achse und $P + P = O$; andernfalls können wir ihre Steigung durch Ableiten der WEIERSTRASS-Gleichung bestimmen:

$$2yy' = 3x^2 + a \Longrightarrow y' = \frac{3x^2 + a}{2y} \,.$$

Im Punkt P ist die Steigung der Tangente somit

$$m = \frac{3x_1^2 + a}{2y_1} \,,$$

und sie hat die Gleichung $y = m(x - x_1) + y_1 = mx + (y_1 - mx_1)$.

Einsetzen in die WEIERSTRASS-Gleichung ergibt

$$\big(mx + (y_1 - mx_1)\big)^2 = x^3 + ax + b$$

oder

$$x^3 - m^2x^2 + \big(a - 2m(y_1 - mx_1)\big)x + (y_1 - mx_1)^2 = 0 \,.$$

Hier wissen wir, daß x_1 eine doppelte Nullstelle ist, also ist die dritte Nullstelle $m^2 - 2x_1$. Somit ist $P + P = (x_3, y_3)$ mit

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad m = \frac{3x_1^2 + a}{2y_1}\,.$$

Der vollständige Algorithmus für die Addition zweier Punkte P und Q sieht also folgendermaßen aus:

Ist $P = O$, so ist $P + Q = Q$; ist $Q = O$, so ist $P + Q = P$.

Sind $P = (x_1, y_1)$ und $Q = (x_2, y_2)$ beide sowohl von O als auch voneinander verschieden, so ist im Falle $x_1 = x_2$ die Summe $P+Q = O$; andernfalls ist $P + Q = (x_3, y_3)$ mit

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad m = \frac{y_2 - y_1}{x_2 - x_1}\,.$$

Ist $P = Q \neq O$, so ist im Falle $y_1 = 0$ die Summe $P+Q = O$; andernfalls ist $P + Q = (x_3, y_3)$ mit

$$x_3 = m^2 - 2x_1, \quad y_3 = y_3 = m(x_1 - x_3) - y_1, \quad m = \frac{3x_1^2 + a}{2y_1}\,.$$

Das inverse Element $-P$ zu einem Punkt P ist im Falle $P = O$ der Punkt selbst; andernfalls ist für $P = (x_1, y_1)$ der Punkt $-P = (x_1, -y_1)$.

Wie man sieht, ist das Rechnen in dieser Gruppe für Kurven in WEIERSTRASS-Normalform in der Tat recht einfach, und auch die Anzahl der Rechenoperationen ist relativ gering.

Zum Schluß wollen wir uns noch die Punkte P mit $2P = O$ genauer anschauen. Einen solchen Punkt gibt es im Falle einer Kurve mit WEIERSTRASS-Gleichung immer, nämlich den Punkt O selbst. Wie im Falle der Punkte mit $3P = O$, die wir am Schluß der letzten Vorlesung betrachtet haben, ist wieder klar, daß auch die Punkte mit $2P = O$ eine Untergruppe bilden. Für einen Punkt $P \neq O$ mit $2P = O$ ist die Tangente im Punkt P parallel zur y-Achse, und wie wir gerade bei der Berechnung von $P + P$ gesehen haben, ist das genau dann der Fall, wenn die y-Koordinate verschwindet. Die Punkte $P \neq O$ mit $2P = O$ sind also genau die Punkte

$(x, 0)$ mit $x^3 + ax + b = 0$. Über einem algebraisch abgeschlossenen Körper hat diese Gleichung drei Lösungen; die Punkte mit $2P = O$ bilden also eine Gruppe mit vier Elementen. Ist k nicht algebraisch abgeschlossen, so können wir einen Erweiterungskörper K finden, in dem die Gleichung drei Lösungen hat, so daß die Punkte aus $E(K)$ mit $2P = O$ eine Gruppe der Ordnung vier bilden. $E(k)$ ist eine Untergruppe davon, hat also die Elementanzahl eins, zwei oder vier. In der Tat hat eine kubische Gleichung in einem Körper k entweder keine oder eine oder drei Lösungen; genau zwei Lösungen sind nicht möglich, denn die Summe aller drei Lösungen ist Null (es gibt keinen x^2-Term), so daß im Falle zweier Lösungen aus k auch die dritte dort liegen muß.

Als Beispiel wollen wir auf der Kurve $y^2z = x^3 + z^3$ in $\mathbb{P}^2(\mathbb{F}_5)$ die Vielfachen des Punkts $(2 : 2 : 1)$ bestimmen. In affinen Koordinaten ist das der Punkt $P = (2, 2)$, und in der affinen WEIERSTRASS-Gleichung $y^2 = x^3 + 1$ ist $a = 0$ und $b = 1$. Für die Berechnung von $2P = P + P$ brauchen wir die Steigung

$$m = \frac{3x_1^2 + a}{2y_1} = \frac{2}{4} = 3$$

der Tangente in P; nach obigen Formeln hat $2P$ die x-Koordinate $m^2 - 2x_1 = 4 - 4 = 0$ und y-Koordinate $0 - (2 - 3 \cdot 2) = 4$, d.h. $2P = (0, 4)$.

Den Punkt $3P$ berechnen wir als $2P + P$, d.h. $x_1 = y_1 = 2$, $x_2 = 0$ und $y_2 = 4$. Die Steigung der Geraden durch die beiden Punkte ist

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{4 - 2}{0 - 2} = -1 = 4\,;$$

also ist $x_3 = m^2 - x_1 - x_2 = 4$ und $y_3 = m(x_1 - x_3) - y_1 = 4 \cdot (-2) - 2 = 0$, d.h. $3P = (4, 0)$. Da die y-Koordinate dieses Punkts verschwindet, ist $6P = 3P + 3P = O$, und damit können wir nun ohne weitere Rechnung auch $4P$ und $5P$ bestimmen:

$$4P = 6P - 2P = O - 2P = -(0, 4) = (0, -4) = (0, 1)$$

und

$$5P = 6P - P = O - P = -P = (2, -2) = (2, 3)\,.$$

P erzeugt also eine zyklische Gruppe der Ordnung sechs, und wie wir bei Aufgabe 2*b)* des sechsten Übungsblatts gesehen haben, sind die sechs berechneten Punkte die sämtlichen Punkte auf der Kurve. Als abstrakte Gruppe ist diese Kurve somit isomorph zur zyklischen Gruppe $\mathbb{Z}/6$.

Die Wendepunkte sind die Punkte, deren Dreifaches gleich O ist; dies sind außer O selbst die Punkte $2P = (0, 4)$ und $4P = (0, 1)$. Der einzige Punkt $Q \neq O$ mit $2Q = O$ ist $Q = 3P = (4, 0)$, was natürlich auch daraus folgt, daß es der einzige Punkt mit verschwindender y-Koordinate ist.