DIOPHANTISCHE GLEICHUNGEN

Teilnehmer:
Inka Eschke (Andreas-Oberschule)
Klaus Gülzow (Heinrich-Hertz-Oberschule)
Lena Kalleske (Heinrich-Hertz-Oberschule)
Thomas Lindner (Heinrich-Hertz-Oberschule)
Valentin Mahrwald (Herder-Oberschule)
Nguyet Nguyen (Andreas-Oberschule)

Gruppenleiter:
Jürg Kramer (Humboldt-Universität)

Die Gruppe beschäftigte sich zunächst mit der allgemeinen Frage nach den Lösungen polynomialer Gleichungen in rationalen Zahlen. Dabei beschränkte man sich der Einfachheit halber auf Polynome in zwei Variablen und von kleinem Grad. Nach dem Studium besagter Problematik wurde man auf den Hauptgegenstand, das Studium rationaler Punkte auf elliptischen Kurven, geführt.
Eine Untergruppe studierte dazu die Herkunft des Begriffs *elliptische Kurve*: Es wurde dazu gezeigt, dass die kubischen Polynome, welche elliptische Kurven definieren, bei der Berechnung des Ellipsenumfangs im Rahmen der sogenannten *elliptischen Integrale* auftreten.
Eine zweite Untergruppe beschäftigte sich mit der Untersuchung rationaler Punkte auf elliptischen Kurven und stellte dazu eine abelsche Gruppenstruktur fest, welche sie mit den entsprechenden expliziten Formeln beschrieb. Dabei wurde auch die nicht-triviale Frage nach der Assoziativität der Gruppenstruktur untersucht.
Die dritte Untergruppe untersuchte die Lösbarkeit des *Kongruenzzahlproblems*, d.h. die Suche nach rechtwinkligen Dreiecken mit rationalen Seiten und vorgegebenem *ganzzahligen* Flächeninhalt. Dabei wurde die Lösbarkeit des Kongruenzzahlproblems auf die Existenz gewisser rationaler Punkte auf bestimmten elliptischen Kurven zurückgeführt.

1. Ellipsenumfang

Im ersten Teil beschäftigten wir uns mit der Herkunft des Begriffs *elliptische Kurve* bzw. *elliptisches Integral*. Dazu betrachten wir eine beliebige Ellipse E, die in Koordinatenform bzw. Parameterform gegeben ist durch (hierbei ist α die große und β die kleine Halbachse):

$$\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} = 1$$

$$0 < \beta \leq \alpha$$

$$x = \alpha \cdot \mathrm{COS}(\varphi)$$

$$y = \beta \cdot \mathrm{SIN}(\varphi)$$

Der Umfang einer solchen Ellipse E berechnet sich wie folgt:

$$u = 4 \cdot \int_0^{\pi/2} \sqrt{(x' \cdot \varphi^2 + y' \cdot \varphi^2)}\, d\varphi$$

$$u = 4 \cdot \int_0^{\pi/2} \sqrt{(\alpha^2 \cdot \mathrm{SIN}(\varphi)^2 + \beta^2 \cdot \mathrm{COS}(\varphi)^2)}\, d\varphi$$

Anwendung des trigonometrischen Pythagoras ergibt:

$$u = 4 \cdot \alpha \cdot \int_0^{\pi/2} \sqrt{\left(1 - \mathrm{COS}(\varphi)^2 + \frac{\beta^2 \cdot \mathrm{COS}(\varphi)^2}{\alpha^2}\right)}\, d\varphi$$

$$u = 4 \cdot \alpha \cdot \int_0^{\pi/2} \sqrt{\left(1 - \frac{\alpha^2 - \beta^2}{\alpha^2} \cdot \mathrm{COS}(\varphi)^2\right)}\, d\varphi$$

$$u = 4 \cdot \alpha \cdot \int_0^{\pi/2} \sqrt{(1 - k^2 \cdot \mathrm{COS}(\varphi)^2)}\, d\varphi$$

mit

$$k^2 = \frac{\alpha^2 - \beta^2}{\alpha^2}$$

Es folgt nun eine Substitution mit

$$t = \cos(\varphi)$$

wobei sich neue Integrationsgrenzen ergeben ($\cos(0)=1, \cos(\pi/2)=0$). Damit folgt

$$u = 4\cdot\alpha\cdot\int_1^0 \frac{\sqrt{(1 - k^2\cdot t^2)}}{-\sin(\varphi)}\,dt$$

$$u = 4\cdot\alpha\cdot\int_0^1 \frac{\sqrt{(1 - k^2\cdot t^2)}}{\sqrt{(1 - t^2)}}\,dt$$

$$u = 4\cdot\alpha\cdot\int_0^1 \frac{1 - k^2\cdot t^2}{\sqrt{((1 - t^2)\cdot(1 - k^2\cdot t^2))}}\,dt$$

Allgemein lässt sich zeigen, dass sich eine Gleichung der Form

$$u^2 = (1 - t^2)\cdot(1 - k^2\cdot t^2)$$

durch die Koordinatentransformation

$$x = \frac{b}{t - a}$$

$$y = x^2\cdot u$$

(wobei a eine Nullstelle obigen Polynoms und b>0 ist) in eine Gleichung der Form

$$y^2 = f(x)$$

bringen lässt, wobei f(x) ein kubisches Polynom ist.

Diese Transformation wenden wir bei obigem Integral durch Substitution an. Im Folgenden wird der Vorfaktor 4α vernachlässigt. Es ergibt sich folgendes Integral:

$$\int_{b}^{b/2} \frac{\left(1 - k^2 \cdot \left(\frac{b}{x} + a\right)^2\right) \cdot \left(-\frac{b}{x^2}\right)}{\sqrt{\left(\left(1 - \left(\frac{b}{x} + a\right)^2\right) \cdot \left(1 - k^2 \cdot \left(\frac{b}{x} + a\right)^2\right)\right)}}\, dx$$

Durch Umformung des Integranden ergibt sich:

$$\frac{b \cdot (x^2 \cdot (a^2 \cdot k^2 - 1) + 2 \cdot a \cdot b \cdot k^2 \cdot x + b^2 \cdot k^2)}{x^2 \cdot \sqrt{(x^4 \cdot (a^4 \cdot k^2 - a^2 \cdot (k^2 + 1) + 1) + 2 \cdot a \cdot b \cdot x^3 \cdot (2 \cdot a^2 \cdot k^2 - k^2 - 1) + b^2 \cdot x^2 \cdot (6 \cdot a^2 \cdot k^2 - k^2 - 1) + 4 \cdot a \cdot b^3 \cdot k^2 \cdot x + b^4 \cdot k^2)}}$$

Da a als Nullstelle obigen Polynoms gewählt wurde, d.h.

$$a^4 \cdot k^2 - a^2 \cdot (k^2 + 1) + 1 = 0$$

folgt mit der Nullstelle a = -1 für den Integranden:

$$\frac{b \cdot \left((k^2 - 1) - \frac{2 \cdot b \cdot k^2}{x} + \frac{b^2 \cdot k^2}{x^2}\right)}{\sqrt{(2 \cdot b \cdot (1 - k^2) \cdot x^3 + b^2 \cdot (5 \cdot k^2 - 1) \cdot x^2 - 4 \cdot b^3 \cdot k^2 \cdot x + b^4 \cdot k^2)}}$$

Insgesamt ergibt sich das folgende sogenannte elliptische Integral, das durch das Auftreten einer Quadratwurzel eines kubischen Polynoms gekennzeichnet ist:

$$\int_{b}^{b/2} \frac{b \cdot \left((k^2 - 1) - \frac{2 \cdot b \cdot k^2}{x} + \frac{b^2 \cdot k^2}{x^2}\right)}{\sqrt{(2 \cdot b \cdot (1 - k^2) \cdot x^3 + b^2 \cdot (5 \cdot k^2 - 1) \cdot x^2 - 4 \cdot b^3 \cdot k^2 \cdot x + b^4 \cdot k^2)}}\, dx$$

Beispielrechnungen:
Exemplarisch berechnen wir den Ellipsenumfang bis auf den Vorfaktor 4α mit k = 0.5:

$$b := 10$$

$$\int_{10}^{5} \frac{\sqrt{(-b\cdot(2\cdot x^3\cdot(k^2-1)+b\cdot x^2\cdot(1-5\cdot k^2)+4\cdot b^2\cdot k^2\cdot x-b^3\cdot k^2))}}{x^2\cdot(b-2\cdot x)}\,dx$$

$$1.46369$$

Dass die Wahl von b tatsächlich beliebig ist, belegt folgendes Beispiel, wobei anstelle von b = 10 beispielsweise b = 20 gewählt wurde:

$$b := 20$$

$$\int_{20}^{10} \frac{\sqrt{(-b\cdot(2\cdot x^3\cdot(k^2-1)+b\cdot x^2\cdot(1-5\cdot k^2)+4\cdot b^2\cdot k^2\cdot x-b^3\cdot k^2))}}{x^2\cdot(b-2\cdot x)}\,dx$$

$$1.46368$$

Zur Überprüfung wurde auch das Integral

$$\int_{0}^{1} \frac{1-k^2\cdot t^2}{\sqrt{((1-t^2)\cdot(1-k^2\cdot t^2))}}\,dt$$

berechnet; es ergibt sich (approximiert) derselbe Wert.

2. Elliptische Kurven

Definition:
Eine kubische Kurve C, die durch die Gleichung

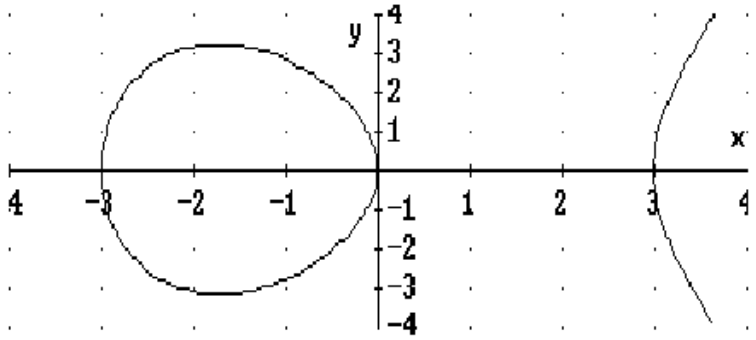
$$y^2 = x^3 + a\cdot x^2 + b\cdot x + c$$

festgelegt ist, heißt *elliptische Kurve*, falls das kubische Polynom auf der rechten Seite drei verschiedene Nullstellen hat (zwei dieser Nullstellen können auch komplex sein).

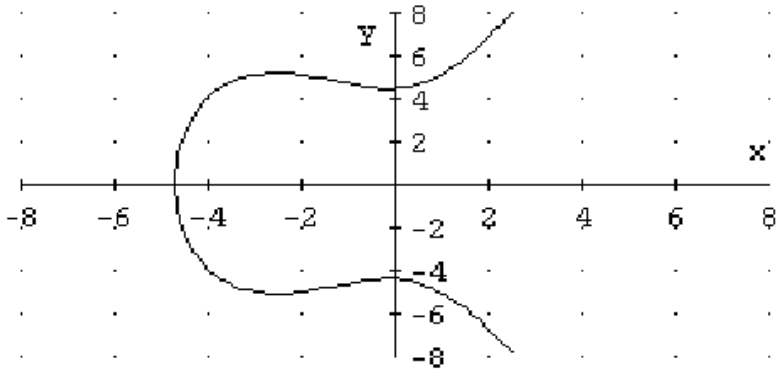
Falls die Koeffizienten a,b,c rationale Zahlen sind, sagen wir, dass die elliptische Kurve C über den rationalen Zahlen definiert ist.

Beispiele:

$$y^2 = x^3 - 9 \cdot x$$



$$y^2 = x^3 + 4 \cdot x^2 + x + 20$$



3. Strukturbetrachtungen der Menge der rationalen Punkte einer elliptischen Kurve

Die Besonderheit der Menge der rationalen Punkte auf einer elliptischen Kurve liegt in der Existenz einer additiven Struktur, wodurch diese Menge zu einer abelschen Gruppe wird.

Die Menge der rationalen Punkte einer elliptischen Kurve C

$$Y^2 = f(X) = X^3 + aX^2 + bX + c \quad (1)$$

(a,b,c$\in$ **Q**) ist gegeben durch

$$C(\mathbf{Q})=\{(x,y) \in \mathbf{Q}^2 \mid y^2 = x^3 + ax^2 + bx + c\}$$

Hat man einen Kandidaten für die Definition einer additiven Verknüpfung + der rationalen Punkte auf einer elliptischen Kurve bestimmt, so muss man (C(**Q**),+) auf die Eigenschaften einer abelschen Gruppe untersuchen, d.h. die Abgeschlossenheit, die Assoziativität, die Kommutativität, sowie die Existenz des neutralen Elements Ȯ und die Existenz des inversen Elements (-P) zu jedem beliebigen Punkt P∈C(**Q**) mit P + (-P) = Ȯ muss nachgewiesen werden.

Um die Addition zweier Punkte $P_1=(x_1,y_1)$ und $P_2=(x_2,y_2)$ zu definieren, wird als erstes eine Gerade an diese beiden Punkte angelegt:

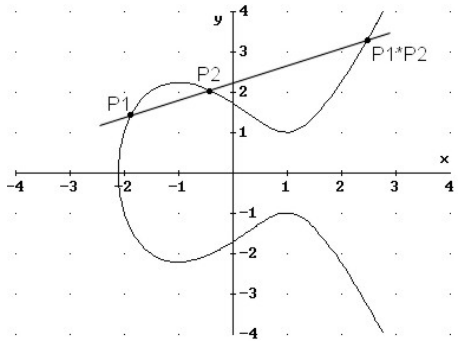


Fig. 1

Es entsteht ein dritter Schnittpunkt mit der elliptischen Kurve; bei diesem handelt es sich um die Verknüpfung $P_1 * P_2$. Die Summe von P_1 und P_2 erhält man geometrisch erst, wenn der erhaltene Punkt $P_1 * P_2 = (x_3,y_3)$ an der X-Achse gespiegelt wird, so dass die Koordinaten von $P_1 + P_2 = (x_3,-y_3)$ lauten:

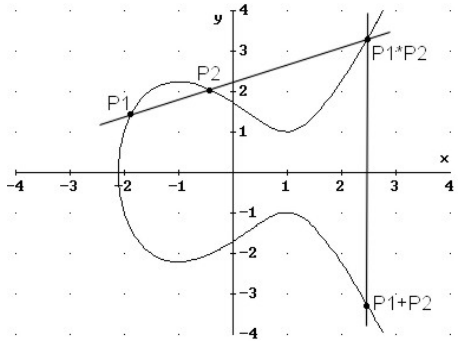


Fig. 2

Rechnerisch muss, um auf die Koordinaten des Punktes $P_1 * P_2$ zu kommen, die Steigung der Geraden berechnet werden, die durch

$$y = \lambda x + \nu \qquad (2)$$

definiert ist. Da zwei Punkte auf der Geraden gegeben sind, kann man die Steigung mit

$$\lambda = (y_2 - y_1) / (x_2 - x_1)$$

und den Achsenabschnitt ν mit

$$\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$$

berechnen.

Nun setzt man die Gerade mit der elliptischen Kurve gleich; es ergibt sich eine Polynomgleichung vom Grad 3, welche x_1 und x_2 als Nullstellen besitzt. Mit Hilfe des Vietaschen Wurzelsatzes lässt sich dann x_3 berechnen. Wir setzen also (2) in (1) ein und erhalten:

$$y^2 = (\lambda x + \nu)^2 = x^3 + ax^2 + bx + c$$
$$0 = x^3 + (a-\lambda^2)x^2 + (b-2\lambda)x + (c-\nu^2)$$

Der Vietasche Wurzelsatz für kubische Kurven besagt, dass die Summe der drei Nullstellen gleich (-1) mal der Koeffizient des quadratischen Terms ist, d.h.:

$$x_1 + x_2 + x_3 = -(a-\lambda^2)$$
$$x_3 = \lambda^2 - a - x_1 - x_2 \qquad (3)$$

Die X-Koordinate von $P_1 * P_2$ ist nun errechnet. Wenn man sie in die Gleichung (2) einsetzt, erhält man für y_3:

$$y_3 = \lambda x_3 + \nu$$

Nach der Spiegelung an der X-Achse hat der Punkt $P_1 + P_2$ die Koordinaten $(x_3,-y_3)$.

Beispiel:

$Y^2 = X^3 + 17$,
$P_1 = (-1,4)$ und $P_2 = (2,5)$.

Gerade: $Y = 1/3X + 13/3$,
$x_3 = -8/9$ und $y_3 = 109/27$.

$P_1 + P_2 = (x_3,-y_3) = (-8/9,-109/27)$.

Dass nicht nur bei diesem Beispiel, sondern auch bei der Addition zweier beliebiger Punkte aus der Menge der rationalen Punkte einer elliptischen Kurve, die Summe wieder durch einen rationalen Punkt repräsentiert wird, ist aus der Gleichung (3) des Vietaschen Wurzelsatzes ersichtlich:
Da sowohl die Steigung λ, der Koeffizient vor dem quadratischen Teil, sowie die X-Koordinaten der Punkte P_1 und P_2 rational sind, muss x_3 auch rational sein. Daraus folgt, dass auch y_3 bzw. $-y_3$ rational sind und es sich bei der Summe um einen rationalen Punkt handelt.

Somit ist (C(**Q**),+) abgeschlossen.

Wie aus Fig. 1 ersichtlich ist, gilt auch das Kommutativgesetz für (C(**Q**),+), da es irrelevant ist, ob man $P_1 + P_2$ oder $P_2 + P_1$ berechnet.

Einen Spezialfall stellt die Addition eines Punktes P mit sich selbst, also die Verdoppelung dar, weil hierbei eine Tangente in P angelegt wird, deren zweiter Schnittpunkt mit der elliptischen Kurve P*P ist. Wenn man auch diesen erhaltenen Punkt spiegelt, ergibt sich die Summe:

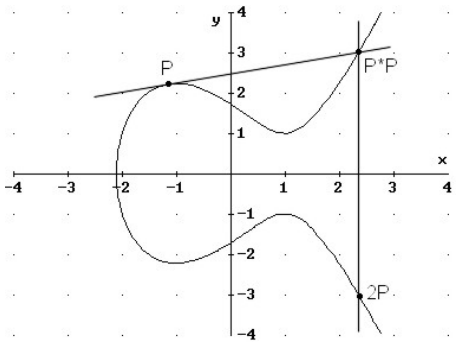


Fig.3: P + P = 2P

Bei der Berechnung wird die Steigung der Tangente durch

$$dY/dX \mid_{(X,Y)=(x,y)} = f'(x)/2y$$

dargestellt, wobei x und y die Koordinaten von P sind.

Die Assoziativität ist nicht so einfach nachzuweisen. Wir haben uns dafür die Differenz der jeweiligen X- bzw. der Y-Koordinate folgender Terme für die Punkte $P_1 = (x_1,y_1)$, $P_2 = (x_2,y_2)$ und $P_3 = (x_3,y_3)$ angeschaut:

$$(P_1 + P_2) + P_3 \text{ bzw. } P_1 + (P_2 + P_3).$$

Am Beispiel der X-Koordinaten dieser beiden Punkte, haben wir mit Hilfe von *Maple* verifiziert, dass diese beiden X-Werte identisch sind. Damit haben wir auch die Assoziativität bestätigt.

Als Nächstes beschäftigten wir uns mit dem neutralen Element. Dabei stellte sich der unendlich ferne Punkt Ȯ als neutrales Element heraus. Denn durch Addieren von Ȯ mit einem Punkt P schneidet die nun zur Y-Achse parallele Gerade die elliptische Kurve im Spiegelpunkt von P und ergibt nach weiterer erforderlicher Spiegelung wieder den Punkt P.

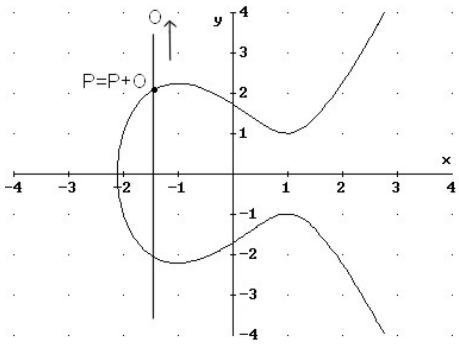


Fig. 4: P + Ȯ = P

Außerdem hat jeder Punkt P = (x,y) einen inversen Punkt –P = (x,-y), so dass gilt:

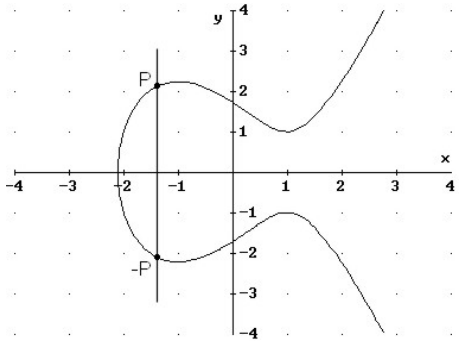


Fig. 5: P + (-P) = Ȯ

Feinere Struktur von C(Q):

(C(**Q**),+) ist sogar eine *endlich erzeugte* abelsche Gruppe, d.h. es gibt endlich viele Punkte $P_1,...,P_r$, so dass alle anderen Punkte aus der Menge C(**Q**) durch Kombination von obigen Tangenten und Sekantenkonstruktionen gewonnen werden können.
Dabei gibt es zwei verschiedene Konfigurationsmöglichkeiten:

1. Die entsprechende Konfiguration schließt sich, d.h.

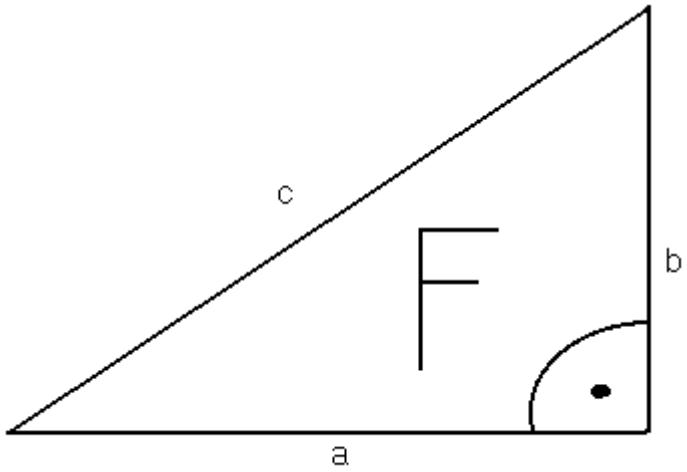
$$|C(\mathbf{Q})| < \infty,$$

   man kommt also nach endlich vielen Schritten zum Ausgangspunkt zurück.

2. Die Konfiguration schließt sich nicht, d.h.

$$|C(\mathbf{Q})| = \infty.$$

4. Kongruenzzahlproblem



Gegeben: F∈ ℚ>0
Frage: Ist F Kongruenzzahl?

F ist Kongruenzzahl, falls $P_F \neq \emptyset$, wobei
$P_F:=\{a, b, c \in \mathbb{Q}_{>0} \mid a^2+b^2=c^2, ab=2F\}$

Man betrachtet die elliptische Kurve

$$C_F : Y^2= X^3- F^2X = X (X-F) (X+F).$$

Wir definieren:

$$C_F (\mathbb{Q})=\{(x, y)\mid x, y \in \mathbb{Q} ; y^2= x^3- F^2x \},$$

$$C_F^* =\{(x, y) \in C_F (\mathbb{Q})\mid x<0 , y>0\}.$$

Man konstruiert aus dem rationalen Punkt $(x, y) \in C_F^*$ der Kurve ein rechtwinkliges Dreieck mit dem Flächeninhalt F, indem man setzt:

$$a=(F^2 - x^2)/y , \; b = -2Fx/y , \; c = (F^2+x^2)/y.$$

Wir prüfen $(a,b,c) \in P_F$, d.h. die Eigenschaften $a^2+b^2=c^2$, $ab=2F$:

$$a^2 + b^2 = (F^2-x^2)^2/y^2 + (-2Fx/y)^2 =[(F^2-x^2)^2+ 4F^2x^2]/y^2 =$$

$$(F^4+2F^2x^2+ x^4)/y^2 = (F^2+x^2)^2/y^2 =c^2$$

und

$$ab =[(F^2 - x^2)/y](-2Fx/y) = 2(-F^3x+ Fx^3)/y^2 =$$

$$2xF(x^2-F^2)/[x(x^2-F^2)]=2F,$$

also gilt $(a,b,c) \in P_F$.

Man betrachte nun ein Zahlentripel $(a,b,c) \in P_F$. Nun kann man umgekehrt einen Punkt $P=(x,y) \in C_F^*$ konstruieren, indem man

$$x= -Fb/(a+c)\ ,\ \ y = 2F^2/(a+c)$$

setzt.

Wir prüfen $(x,y) \in C_F^*$, d.h. die Eigenschaften $x,y \in Ð$, $x<0$, $y>0$,

$$y^2 = x^3 - F^2x = x(x^2 - F^2).$$

Die beiden ersten Eigenschaften sind klar; weiter berechnen wir:

$$x^3 - F^2x = (- Fb/(a+c))^3 + F^2Fb/(a+c) = [F^3b/(a+c)][1-b^2/(a+c)^2] = [F^3b][(a+c)^2-b^2]/(a+c)^3 = [F^3b/(a+c)^3](a^2+2ac+c^2-b^2);$$

wegen $a^2+b^2=c^2$ folgt

$$x^3-F^2x = [F^3b/(a+c)^3](a^2+2ac+a^2) =$$

$$[F^3b/(a+c)^3]2a(a+c) = 2abF^3/(a+c)^2;$$

mit $ab=2F$ folgt schließlich

$$x^3-F^2x = F^34F/(a+c)^2 = [2F^2/(a+c)]^2 = y^2.$$

Damit haben wir die Äquivalenz:

$$P_F \int « \ \ ‹ \ \ C_F^* \int «.$$

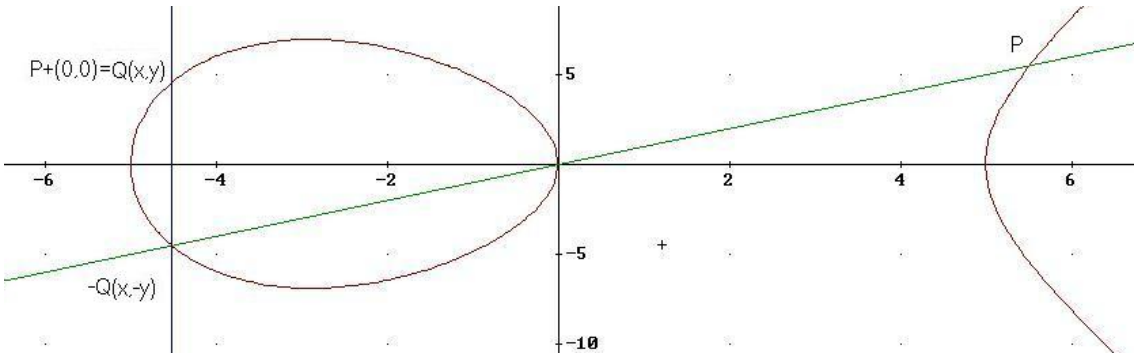


Fig.1 Elliptische Kurve C_F : $Y^2 = X^3 - 25X$

Wie man Fig. 1 entnimmt, kann man aus einem beliebigen Punkt P∈ C_F (Ð) durch Addition von (0,0) (vgl. Abschnitt 3) und gegebenenfalls durch anschließende Spiegelung an der X-Achse einen Punkt Q=(x,y) ∈ C_F (Ð) mit x<0 und y>0 konstruieren.

Damit haben wir folgenden Satz bewiesen:

Satz: F ist genau dann Kongruenzzahl, falls auf der elliptischen Kurve C_F ein rationaler Punkt (x,y) mit y≠0 existiert, d.h. es besteht die Äquivalenz

$$P_F \neq \emptyset \Leftrightarrow \{(x,y) \in C_F(Ð) \mid y \neq 0\} \neq \emptyset.$$

Beispiele:

F = 1,2,3 ⇒ $P_F=\emptyset$.

F=5 : (-5/9,100/27) ∈ C_F(Ð) ⇒ (20/3, 3/2, 41/6) ∈ P_F.

F=6 : (-3,9) ∈ C_F(Ð) ⇒ (3,4,5) ∈ P_F.

Bemerkung: Man erkennt sofort, dass die Menge {(x,y) ∈ C_F(Ð) | y=0} aus den Punkten
{(-F,0), (0,0), (F,0)}besteht; dies sind Punkte P der Ordnung 2, d.h. 2·P=O.

Es lässt sich nachweisen, dass dies die einzigen Punkte endlicher Ordnung in C_F(Ð) sind. Damit haben wir die weitere Äquivalenz

$$P_F \neq \emptyset \Leftrightarrow |C_F(Ð)| = ¶ .$$