EINE ARITHMETISCHE EIGENSCHAFT DER KUBISCHEN BINÄRFORMEN

von

KURT MAHLER

in Groningen.

Es wird folgender Satz bewiesen: „*Sei* $F(x, y)$ *eine kubische Binärform mit ganzen rationalen Koeffizienten und nichtverschwindender Diskriminante. Dann gibt es nur endlichviele natürliche kubusfreie Zahlen* k, *so dass die Gleichung*

$$F(x, y) = k$$

zwar mindestens eine, aber höchstens endlichviele Lösungen in rationalen Zahlen x, y *besitzt.*" Für alle anderen natürlichen kubusfreien k hat diese Gleichung also entweder gar keine oder unendlichviele Lösungen in rationalen Zahlen.

Aus diesem Satz ergibt sich ein sehr einfacher Beweis dafür, dass es *zu jeder natürlichen Zahl* t *eine ganze rationale Zahl* $k \neq 0$ *gibt, so dass die Gleichung*

$$F(x, y) = k$$

mindestens t *Lösungen in ganzen rationalen Zahlen besitzt.*

Die Methode dieser Note kann auch für andere Klassen von Diophantischen Gleichungen benutzt werden, wie Herr PAYNTER, Manchester, in seiner demnächst erscheinenden These zeigen wird. Ich bin ihm sehr zu Dank verpflichtet für seine Mitarbeit bei der Durchrechnung einiger numerischen Beispiele.

I.

1). Sei

$$F(x, y) = a_0x^3 + a_1x^2y + a_2xy^2 + a_3y^3$$

eine kubische Binärform mit ganzen rationalen Koeffizienten

und nichtverschwindender Diskriminante, ferner zur Abkürzung

$$F_x(x, y) = \frac{\partial F(x, y)}{\partial x}, \qquad F_y(x, y) = \frac{\partial F(x, y)}{\partial y}.$$

Ist $k \neq 0$ beliebig, so definiert die Gleichung

$$F(x, y) = k$$

eine Kurve dritter Ordnung $C(k)$ vom Geschlecht 1. Die Gleichung ihrer Tangente in einem gegebenen Punkt (x, y) lautet

$$X\mathfrak{x} + Y\mathfrak{y} = Xx + Yy,$$

wobei

$$X = F_x(x, y), \qquad Y = F_y(x, y)$$

gesetzt wurde; nach dem Eulerschen Satz über homogene Funktionen ist

$$Xx + Yy = 3F(x, y) = 3k.$$

Die Tangente schneidet die Kurve noch in einem Punkte $(\mathfrak{x}, \mathfrak{y})$, den wir den Tangentialpunkt von (x, y) nennen wollen; eine einfache Rechnung ergibt für seine Koordinaten die Werte

$$\mathfrak{x} = -2x - \frac{3kF_y(Y, -X)}{F(Y, -X)},$$

$$\mathfrak{y} = -2y + \frac{3kF_x(Y, -X)}{F(Y, -X)}.$$

Da nun $F(Y, -X)$ durch $F(x, y)$ ohne Rest teilbar ist, wie eine einfache Rechnung zeigt, so ergibt sich ein Formelpaar

$$\mathfrak{x} = \frac{P(x, y)}{R(x, y)}, \qquad \mathfrak{y} = \frac{Q(x, y)}{R(x, y)},$$

wobei

$$R(x, y) = \frac{F(Y, -X)}{F(x, y)}$$

eine Binärform dritter Ordnung, und

$$P(x, y) = -2xR(x, y) - 3F_y(Y, -X),$$

$$Q(x, y) = -2yR(x, y) + 3F_x(Y, -X)$$

zwei Binärformen vierter Ordnung bedeuten; diese drei Formen besitzen ganze rationale Koeffizienten. Die beiden Formen $P(x, y)$ und $Q(x, y)$ haben eine nichtverschwindende Resultante $r \neq 0$; man beweist dies am einfachsten durch direkte Ausrechnung, indem man $F(x, y)$ in der kanonischen Form als Summe der Kuben von zwei Linearformen voraussetzt.

2). Jedem Punkt (x, y) mit reellen Koordinaten auf $C(k)$ entspricht eine reelle Zahl

$$t = \frac{y}{x},$$

und umgekehrt bestimmt diese Zahl t den Punkt (x, y) wieder eindeutig; denn jede gerade Linie durch den Ursprung schneidet $C(k)$ in nur einem reellen Punkt. Ist $(\mathfrak{x}, \mathfrak{y})$ der Tangentialpunkt von (x, y) und

$$\mathfrak{t} = \frac{\mathfrak{x}}{\mathfrak{y}},$$

so wird nach den Formeln in 1.)

$$\mathfrak{t} = \frac{Q(1, t)}{P(1, t)},$$

also $\mathfrak{t}$ eine rationale Funktion von t mit ganzen rationalen Koeffizienten.

Im folgenden nehmen wir immer an, dass der Parameter k rational ist, und wir betrachten allein Punkte (x, y) auf $C(k)$, die rationale Koordinaten haben. Dann ist also auch t eine rationale Zahl, unter Umständen $t = \infty$, und eindeutig durch den Punkt (x, y) bestimmt. Umgekehrt, wenn t gegeben und rational oder gleich ∞ ist, so wird

$$x = \lambda, \quad y = \lambda t, \qquad k = \lambda^3 F(1, t),$$

bzw. für $t = \infty$

$$x = 0, \quad y = \lambda, \quad k = \lambda^3 F(0, 1),$$

und zwar darf hier λ eine beliebige rationale Zahl $\neq 0$ sein. Insbesondere ist also der Parameter k bis auf einen multiplikativen Faktor λ^3 bestimmt.

Für die folgenden Überlegungen ist es deshalb zweckmässig, irgend zwei rationale Werte des Parameters $k \neq 0$, die sich nur um einen solchen Faktor λ^3 unterscheiden, als äquivalent zu betrachten, ferner alle äquivalenten Parameterwerte k in eine Klasse K zusammenzufassen. Als Repräsentant dieser Klasse kann alsdann die einzige in ihr vorkommende kubusfreie natürliche Zahl genommen werden. Eine Klasse K ist offenbar eindeutig bestimmt, wenn wir einen Parameterwert k aus ihr, oder die entsprechende Kurve $C(k)$, oder einen rationalen Punkt (x, y) auf dieser Kurve, oder endlich die entsprechende Zahl $t = \frac{y}{x}$ kennen. Derselben Klasse K, der $t = \frac{y}{x}$ zugeordnet ist, entspricht auch der Wert $\mathfrak{t} = \frac{\mathfrak{y}}{\mathfrak{x}}$ des Tangentialpunktes. Zur Abkürzung nennen wir $\mathfrak{t}$ das Tangential von t; das bedeutet also, dass

$$\mathfrak{t} = \frac{Q(1, t)}{P(1, t)}$$

ist.

3). Bedeute für eine beliebige rationale Zahl $k \neq 0$ das Zeichen $a(k)$ die Anzahl der Punkte (x, y) mit endlichen rationalen Koordinaten auf der Kurve

$$C(k): \qquad F(x, y) = k.$$

Dann hat offenbar $a(k)$ für alle k aus derselben Klasse K denselben Wert, und wir können also hierfür $a(K)$ schreiben. Die Zahl $a(K)$ kann gleich Null, gleich Unendlich, oder gleich einer endlichen natürlichen Zahl sein. Im letzteren Fall, wenn also $a(K)$ zwar endlich, aber nicht gleich Null ist, heisse K eine singuläre Klasse; ebenso heisse ein Parameter k aus dieser Klasse, die entsprechende Kurve $C(k)$, ein rationaler Punkt (x, y) auf dieser Kurve, und der zugehörige Zahlwert t singulär.

In den nächsten Paragraphen soll der folgende Satz bewiesen werden:

Satz 1: *Es gibt nur endlichviele verschiedene singuläre Klassen.*

Mit diesem Satz gleichbedeutend ist die Aussage:

Satz 1*a*: *Es gibt höchstens endlichviele kubusfreie natürliche Zahlen k, so dass die Gleichung*

$$F(x, y) = k$$

eine zwar endliche, aber nichtverschwindende Anzahl von Lösungen in endlichen rationalen Zahlen x, y hat.

4). Zum Beweise schreiben wir t als Quotienten zweier teilerfremden ganzen rationalen Zahlen p und q:

$$t = \frac{q}{p}, \quad (p, q) = 1,$$

insbesondere

$$0 = \frac{0}{1}, \quad \infty = \frac{1}{0}.$$

Entsprechenderweise ist das Tangential $\mathfrak{t}$ von t gleich dem Quotienten zweier teilerfremden ganzen rationalen Zahlen $\mathfrak{p}$ und $\mathfrak{q}$:

$$\mathfrak{t} = \frac{\mathfrak{q}}{\mathfrak{p}}, \quad (\mathfrak{p}, \mathfrak{q}) = 1.$$

Es ist

$$\mathfrak{p} : \mathfrak{q} = P(p, q) : Q(p, q),$$

also

$$\mathfrak{p} = \frac{P(p, q)}{\delta}, \quad \mathfrak{q} = \frac{Q(p, q)}{\delta},$$

wo δ den größten gemeinsamen Teiler

$$\delta = (P(p, q),\ Q(p, q))$$

bedeutet.

Die beiden Binärformen vierten Grades $P(x, y)$ und $Q(x, y)$ haben nun aber ganze rationale Koeffizienten, und ihre Resultante r ist nicht Null. Nach bekannten algebraischen Sätzen gibt es also vier Binärformen

$$P_1(x, y), \quad Q_1(x, y), \quad P_2(x, y), \quad Q_2(x, y)$$

mit ganzen rationalen Koeffizienten und vom dritten Grade, so dass

$$P(x, y)P_1(x, y) + Q(x, y)Q_1(x, y) = rx^7,$$

$$P(x, y)P_2(x, y) + Q(x, y)Q_2(x, y) = ry^7$$

ist. Für $x = p,\ y = q$ folgt hieraus

$$\delta = (\mathrm{P}(p, q), \mathrm{Q}(p, q)) \mid (rp^7, rq^7) = r(p, q)^7,$$

und wegen $(p, q) = 1$ muss also δ ein Teiler von r sein. Also gibt es eine feste natürliche Zahl d, etwa $d = |r|$, so dass für alle teilerfremden ganzen rationalen p und q die Zahl

$$\delta = (\mathrm{P}(p, q),\ \mathrm{Q}(p, q))$$

in d aufgeht.

Da für $x^2 + y^2 > 0$ die beiden Formen $\mathrm{P}(x, y)$ und $\mathrm{Q}(x, y)$ nie gleichzeitig verschwinden, so ist weiterhin klar, dass die Funktion

$$\mathrm{S}(x, y) = \max (|\ \mathrm{P}(x, y)\ |,\ |\ \mathrm{Q}(x, y)\ |)$$

auf dem Quadratrand

$$\max (|\ x\ |,\ |\ y\ |) = 1$$

ein absolutes Minimum $c > 0$ besitzt; wegen

$$\mathrm{S}(ux, uy) = u^4 \mathrm{S}(x, y)$$

für jede positive Zahl u besteht demnach die Ungleichung

$$\max (|\ \mathrm{P}(x, y)\ |,\ |\ \mathrm{Q}(x, y)\ |) \geqq c\ (\max (|\ x\ |,\ |\ y\ |))^4$$

für alle reellen Zahlen x und y.

Wegen

$$\mathfrak{p} = \frac{\mathrm{P}(p, q)}{\delta}, \qquad \mathfrak{q} = \frac{\mathrm{Q}(p, q)}{\delta}, \qquad \delta \mid d$$

genügen also die beiden Ausdrücke

$$\alpha(t) = \max (|\ p\ |, |\ q\ |), \quad \alpha(\mathfrak{t}) = \max (|\ \mathfrak{p}\ |, |\ \mathfrak{q}\ |)$$

der Ungleichung

$$\alpha(\mathfrak{t}) \geqq \frac{c}{d}\ \alpha(t)^4.$$

5). Wir wenden die letzte Ungleichung auf eine rationale Zahl t, die der Klasse K zugeordnet ist, und auf ihre iterierten Tangentiale

$$t_1 = \frac{\mathrm{Q}(1, t)}{\mathrm{P}(1, t)}, \qquad t_2 = \frac{\mathrm{Q}(1, t_1)}{\mathrm{P}(1, t_1)}, \qquad t_3 = \frac{\mathrm{Q}(1, t_2)}{\mathrm{P}(1, t_2)}, \ \ldots$$

an. Dann wird

$$\alpha(t_1) \geqq \frac{c}{d}\alpha(t)^4, \quad \alpha(t_2) \geqq \frac{c}{d}\alpha(t_1)^4, \quad \alpha(t_3) \geqq \frac{c}{d}\alpha(t_2)^4, \ldots$$

und speziell, wenn

$$\alpha(t) > \left(\frac{d}{c}\right)^{1/3}$$

vorausgesetzt wird, bekommen wir

$$\left(\frac{d}{c}\right)^{1/3} < \alpha(t) < \alpha(t_1) < \alpha(t_2) < \alpha(t_3) < \ldots,$$

und somit müssen alle Zahlen

$$t,\ t_1,\ t_2,\ t_3,\ \ldots$$

verschieden sein, da ihre Darstellungen als gekürzte Brüche nicht übereinstimmen. Also liegen auf der Kurve der Klasse K unendlichviele Punkte mit rationalen Koordinaten, und diese Klasse ist nicht singulär.

Umgekehrt folgt, dass die Klasse K nur singulär sein kann, wenn auf einer ihrer Kurven $C(k)$ ein rationaler Punkt (x, y) mit einem solchen Zahlwert

$$t = \frac{y}{x} = \frac{q}{p}, \quad (p, q) = 1,$$

liegt, so dass

$$\alpha(t) = \max\left(|\, p\,|,\ |\, q\,|\right) \leqq \left(\frac{d}{c}\right)^{1/3}$$

ist. Da diese Ungleichung nur endlichviele Lösungen p, q, d.h. t hat, so kann es auch nur höchstens endlichviele singuläre Klassen geben, und das sollte gerade bewiesen werden.

Da sich für jede Form $F(x, y)$ die beiden Zahlen c und d wirklich bestimmen lassen, so gibt der Beweis übrigens ein Mittel zur expliziten Bestimmung der etwaigen singulären Klassen. Einige Ergebnisse dieser Art sind auf Tabelle I zusammengestellt.

Tabelle I.

Form	Singuläre Klassen	Anzahl der rationalen Lösungen
$x(x^2+y^2)$	$k = 1$	1 Lösung
$x(x^2-y^2)$	$k = 1$	3 Lösungen
$xy(x+y)$	$k = 2$	3 Lösungen
$x(3x^2+y^2)$	$k = 3$	1 Lösung
	$k = 12$	2 Lösungen
$x(2x^2-y^2)$	Keine	
x^3+y^3	$k = 1$	2 Lösungen
	$k = 2$	1 Lösung
$6x^3+y^3$	$k = 6$	1 Lösung

Weitere speziellen Fälle wurden von Herrn PAYNTER untersucht.

II.

6). Die Ergebnisse des letzten Kapitels führen zu einem neuen Beweis des folgenden Satzes, den ich bereits früher, aber auf umständlichere Weise bewiesen hatte:

Satz 2: *Wenn die kubische Binärform $F(x, y)$ ganze rationale Koeffizienten und nichtverschwindende Diskriminante hat, so gibt es zu jeder natürlichen Zahl t eine ganze rationale Zahl $k \neq 0$, so dass die Gleichung*

$$F(x, y) = k$$

mindestens t verschiedene Lösungen in ganzen rationalen Zahlen hat.

Beweis: Seien c und d dieselben Zahlen wie in 4) und p und q irgend zwei ganze rationale teilerfremde Zahlen mit

$$\alpha\left(\frac{q}{p}\right) = \max\left(|p|, |q|\right) > \left(\frac{d}{c}\right)^{1/3},$$

ferner

$$F(p, q) = k^*.$$

Auf der Kurve

$$F(x, y) = k^*$$

liegen dann nach 5) mindestens t verschiedene Punkte

$$(x_1, y_1), \quad (x_2, y_2), \quad \ldots, \quad (x_t, y_t)$$

mit rationalen Koordinaten (es gibt ja sogar unendlich viele!). Sei nun Z der Generalnenner der $2t$ Zahlen

$$x_1, y_1, \quad x_2, y_2, \quad \ldots, \quad x_t, y_t.$$

Dann ist klar, dass auf der Kurve

$$F(x, y) = k = k^* Z^3$$

mindestens t Gitterpunkte liegen, und das war zu zeigen.

7). Die Beweismethode dieser Arbeit kann auch auf andere und allgemeinere Klassen von Kurven des Geschlechtes 1 angewandt werden; auf diese Weise lässt sich insbesondere der folgende Satz beweisen:

Satz 3: *Sei $f(x)$ ein Polynom dritten oder vierten Grades mit ganzen rationalen Koeffizienten und nichtverschwindender Diskriminante. Dann gibt es höchstens endlichviele ganze rationale quadratfreie Zahlen k, so dass die Gleichung*

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

genau eine endliche, aber nichtverschwindende Anzahl von Lösungen in rationalen Zahlen x, y mit $y \neq 0$ besitzt.

Die Durchführung des Beweises wird Herr PAYNTER zusammen mit einer Anzahl durchgerechneter numerischer Fälle in seiner These veröffentlichen.

Frühjahr 1934.