ÜBER RATIONALE PUNKTE AUF KURVEN $y^2=x(x^2-c^2)$.

VON

A. WIMAN

in LUND.

1.

1. In einer im letzten Jahre erschienenen Abhandlung[1] habe ich die rationalen Punkte auf Kurven

$$y^2=x(x+a)(x+b) \tag{1}$$

untersucht, wo a und b ganze rationale Zahlen bedeuten. In der ersten Abteilung dieser Arbeit beschränkte ich mich auf den speziellen Fall, wo (1) sich in der Gestalt

$$y^2=x(x^2-c^2) \tag{2}$$

schreiben lässt. Es wurden dabei verschiedene Kurven (2) vom Range vier in Betracht gezogen. Es gelang mir auch eine Kurve (2), aber nur eine einzige, vom Range fünf zu entdecken. In der zweiten Abteilung der besprochenen Arbeit wurde der allgemeine Fall behandelt. Als Hauptresultat ergab sich, dass man Kurven (1) in unbegrenzter Anzahl sowohl vom Range fünf als vom Range sechs bestimmen kann.

Die vorliegende Arbeit, welche sich nahe an die erste Abteilung der zitierten Abhandlung anschliesst, zerfällt in drei Abschnitte. Im ersten Abschnitt wird eine Methode entwickelt, durch welche in vielen Fällen sich beweisen lässt, dass die bereits bekannte untere Grenze des Ranges einer Kurve den richtigen Rang der Kurve darstellt. Im zweiten Abschnitt werden Fälle behandelt, wo c eine Primzahl p oder das doppelte einer Primzahl bedeutet. Es werden einige Kurven

[1] »*Über den Rang von Kurven* $y^2=x(x+a)(x+b)$», Acta mathematica 76 (1944). Diese Schrift wird hier kurz »*Rang von Kurven*» benannt.

bestimmt, für welche der Maximalrang vier hier erreicht wird. Im dritten Abschnitt wird nachgewiesen, wie sich unbegrenzt viele Kurven (2) nicht nur vom Range vier sondern auch vom Range fünf bestimmen lassen. Wir werden finden, dass sogar der Rang sechs, wenn auch nur durch ein einziges Beispiel, unter den Kurven (2) vertreten wird.

2. In »*Rang von Kurven*» haben wir unter Zugrundelegung des Beispiels $c = 210$ auseinandergesetzt, wie man die rationalen Punkte auf einer Kurve (2) in Klassen verteilt. Hier benutzen wir zu dem gleichen Zwecke das ganz analoge Beispiel

$$c = 330 = 2.3.5.11. \tag{3}$$

Auf dieser Kurve finden wir unmittelbar die beiden rationalen Punkte

$$x - c = 66, \quad x = 396, \quad x + c = 726;$$
$$x - c = 550, \quad x = 880, \quad x + c = 1210,$$

für welche wir der leichteren Übersichtlichkeit wegen die Bezeichnungen

$$(P_1) \qquad (1, 6, 11)\ 66;$$
$$(P_2) \qquad (5, 8, 11)\ 110$$

einführen. Wie man hier für die entsprechenden y-Werte das Zeichen + oder — wählt, ist gleichgültig. Ohne weiteres ist ersichtlich, dass als gemeinsame Faktoren für $x-c$, x und $x+c$ bei einem rationalen Punkt nur die Teiler von c, also in diesem Falle 2, 3, 5 und 11, auftreten können. Ein solcher Faktor muss in zwei von den drei Grössen in ungerader Potenz und in der dritten in gerader Potenz enthalten sein. Wenn wir die Primzahl für diese dritte Grösse charakteristisch sein lassen, so finden wir, dass die beiden Punkte zu zwei Klassen mit den Charakteren

$$(K_1) \qquad 1, 2.3, 11;$$
$$(K_2) \qquad 5, 2, 11.$$

gehören. Die Klasse des dritten Schnittpunktes $P_{1,2}$ der Kurve mit der Verbindungsgeraden von P_1 und P_2 entsteht durch Komposition von K_1 und K_2. Die Charaktere für diese Klasse $K_{1,2}$ erhält man, indem man beachtet, dass durch Komposition der drei Klassen K_1, K_2 und $K_{1,2}$ sich die Einheitsklasse ergeben soll. Wenn man also für die drei Klassen die entsprechenden Charaktere mit einander multipliziert, so sollen für die drei Stellen gleiche Resultate heraus-

kommen, wenn etwa auftretende Quadrate ausgeschieden werden. Im vorliegenden Falle bekommen wir

$(K_{1,2})$ 5, 3, 1,

und in

$(P_{1,2})$ (5, 27, 49) 15

haben wir einen zu dieser Klasse gehörenden rationalen Punkt. Man findet auch leicht, dass hier die Punkte P_1, P_2 und $P_{1,2}$ in gerader Linie liegen, wenn man für sämtliche drei y-Werte entweder das Zeichen + oder das Zeichen — nimmt.

Den rationalen Punkten auf der Achse $y = 0$ geben wir die Bezeichnungen:

(P_3) (0, 330, 660);
(P_4) (— 330, 0, 330);
$(P_{3,4})$ (— 660, — 330, 0).

Wir ziehen die neun Verbindungslinien zwischen den Punkten P_1, P_2 und $P_{1,2}$ einerseits und P_3, P_4 und $P_{3,4}$ andererseits. Den dritten Punkt, der je aus der Kurve ausgeschnitten wird, findet man am bequemsten, indem man für eine Gerade durch P_3, P_4 oder $P_{3,4}$ die Relation zwischen den x-Werten für die beiden übrigen Schnittpunkte bestimmt. Hierfür ergibt sich bzw.:

(4) $$(x_1 - c)(x_2 - c) = 2c^2; \quad x_1 x_2 = -c^2; \quad (x_1 + c)(x_2 + c) = 2c^2.$$

In leicht verständlicher Bezeichnung erhalten wir jetzt:

$(P_{1,3})$ (10, 11, 12) 330;
$(P_{2,3})$ (6, 11, 16) 66;
$(P_{1,2,3})$ (44, 49, 54) 66;
$(P_{1,4})$ (— 11, — 5, 1) 55;
$(P_{2,4})$ (— 11, — 3, 5) $\frac{165}{4}$;
$(P_{1,2,4})$ (— 49, — 22, 5) $\frac{110}{9}$;
$(P_{1,3,4})$ (— 12, — 1, 10) 30;
$(P_{2,3,4})$ (— 16, — 5, 6) 30;
$(P_{1,2,3,4})$ (— 54, — 5, 44) $\frac{880}{49}$.

In diesen Punkten haben wir Repräsentanten für die folgenden neun Klassen:

$(K_{1,3})$ 2.5, 11, 3;
$(K_{2,3})$ 2.3, 11, 1;
$(K_{1,2,3})$ 11, 1, 2.3;

$(K_{1,4})$ $\quad -11, -5, 1;$
$(K_{2,4})$ $\quad -11, -3, 5;$
$(K_{1,2,4})$ $\quad -1, -2.11, 5;$
$(K_{1,3,4})$ $\quad -3, -1, 2.5;$
$(K_{2,3,4})$ $\quad -1, -5, 2.3;$
$(K_{1,2,3,4})$ $\quad -2.3, -5, 11.$

Die Charaktere der Klassen, für welche die Punkte auf der Achse Repräsentanten sind, lassen sich jetzt durch Komposition bestimmen, und wir erhalten:

(K_3) $\quad 3.5.11, 1, 2;$
(K_4) $\quad -1, -2.3.5.11, 1;$
$(K_{3,4})$ $\quad -2, -1, 3.5.11.$

Man beachte, wie die Primzahl 2 hier in anderer Weise als die ungeraden Primzahlen auftritt. Nach Hinzunahme der Einheitsklasse haben wir jetzt sechszehn Klassen, welche sich mit einander wie eine Abelsche Gruppe vom Typus (2, 2, 2, 2) komponieren. Als erzeugende Elemente dieser Gruppe können wir K_1, K_2, K_3 und K_4 nehmen. Die Kurve (3) kann also von keinem niedrigeren Range als vier sein. Es bleibt übrig zu beweisen, dass der Rang auch nicht höher als vier sein kann.

Wir betrachten noch einen Fall, in welchem c eine ungerade Zahl ist, und zwar setzen wir

$$c = 15.$$

Ein erster rationaler Punkt ist hier

(P_1) $\quad (2, 5, 8)\ 5.$

Hierzu kommen die drei Punkte auf der Achse:

(P_2) $\quad (0, 15, 30);$
(P_3) $\quad (-15, 0, 15);$
$(P_{2,3})$ $\quad (-30, -15, 0).$

Die Verbindungslinien von P_1 mit P_2, P_3 und $P_{2,3}$ gehen bzw. durch die Punkte:

$(P_{1,2})$ $\quad (3, 4, 5)\ 15;$
$(P_{1,3})$ $\quad (-5, -1, 3)\ \frac{15}{4};$
$(P_{1,2,3})$ $\quad (-8, -3, 2)\ 3.$

Für die zugehörigen Klassen haben wir die Charaktere:

(K_1) 1, 2.5, 1;
$(K_{1,2})$ 3, 1, 5;
$(K_{1,3})$ -5, -1, 3;
$(K_{1,2,3})$ -1, -2.3, 1.

In Übereinstimmung hiermit bekommen wir für die Punkte auf der Achse:

(K_2) 3.5, 2, 1;
(K_3) -1, -3.5, 1;
$(K_{2,3})$ -1, -2, 3.5.

Zu bemerken ist, dass die Primzahl 2, ohne Faktor von c zu sein, hier unter den Charakteren auftritt. In solchen Fällen haben $x-c$ und $x+c$ 2 als Faktor in ungerader Potenz, und der Platz für 2 als Charakter ist nach unseren Verabredungen an der mittleren Stelle. Man beachte in diesem Zusammenhange noch, dass, wie aus den angeführten Beispielen hervorgeht, die Primzahl 2 für die Punkte auf der Achse in anderer Weise bei geraden und ungeraden Werten von c als Charakter auftritt.

3. Es sei c Produkt von r verschiedenen Primzahlen. Zunächst nehmen wir an, dass 2 unter diesen Primzahlen auftritt. Unabhängig davon, ob entsprechende rationale Punkte auf der Kurve existieren, suchen wir einen Überblick über die Charaktere, welche vermittelst dieser Primzahlen sich aufstellen lassen. Zu dem Ende genügt es die erzeugende Elemente für die Gruppe der Charaktere zu bestimmen. Für eine beliebige in c eingehende Primzahl p bekommen wir deren zwei, etwa p, 1, 1 und 1, 1, p; durch die Komposition von diesen Charakteren ergibt sich ja 1, p, 1. Zu den in solcher Weise erhaltenen $2r$ erzeugenden Elementen kommt noch -1, -1, 1, so dass als Gesamtzahl $2r+1$ herauskommt. In $2r+1$ haben wir also offensichtlich eine obere Grenze für den Rang der Kurve.

Gehört 2 nicht zu den Faktoren von c, so kommt, wie aus dem letzten Beispiel in der vorhergehenden Nummer verständlich sein dürfte, noch das erzeugende Element 1, 2, 1 hinzu. In diesem Falle bekommen wir somit $2r+2$ als obere Grenze des Ranges der Kurve[1]. Diese obere Grenze wird auch, wie

[1] Nach diesem Gedankengange hat G. BILLING in seiner Abhandlung, »*Beiträge zur arithmetischen Theorie der ebenen kubischen Kurven vom Geschlechte eins*» (Königl. Sozietät der Wissenschaften zu Uppsala, 1938), eine obere Grenze des Ranges nicht nur für diesen Fall, sondern für die kubischen Kurven im allgemeinen hergeleitet.

wir im nächsten Abschnitt sehen werden, für $r = 1$ erreicht. Dort werden wir auch finden, dass, falls r die Anzahl der in c eingehenden *ungeraden* Primzahlen bedeutet, man ganz allgemein $2r+2$ als obere Grenze des Ranges annehmen kann, unabhängig davon, ob 2 als Faktor eingeht oder nicht.

4. Für $c = 330$ haben wir in der 2. Nummer vier als untere Grenze des Ranges erhalten. Dass in diesem Falle vier auch eine obere Grenze des Ranges und also den wahren Rang bezeichnet, wird als Resultat von dieser Nummer hervorgehen. Nach der vorhergehenden Nummer wissen wir, dass die Gruppe der Charaktere, in denen nur die Primzahlen 2, 3, 5 und 11 auftreten, neun erzeugende Elemente besitzt, und wir wissen, dass zu den Elementen einer Untergruppe mit vier erzeugenden Elementen rationale Punkte auf der Kurve existieren. Für den Beweis genügt es dann offensichtlich, wenn sich eine andere Untergruppe mit fünf erzeugenden Elementen von der Art aufsuchen lässt, dass nur zu dem Einheitselemente rationale Punkte der Kurve gehören. Dies ist möglich in vielerlei Weisen. Für die vier ersten erzeugenden Elemente nehmen wir:

$$1,\ 2,\ 1;\quad 1,\ 3,\ 1;\quad 1,\ 5,\ 1;\quad 1,\ 11,\ 1.$$

Es gilt also nachzuweisen, dass, wenn $k = 1$ ausgenommen wird, zu keinem der Charaktere $1, k, 1$, wo k die Teiler von 330 durchläuft, rationale Punkte auf der Kurve (3) vorkommen. Für einen rationalen Punkt, der etwa zu einem gewissen k-Wert gehört, gibt es für $x - c$, x und $x + c$ Ausdrücke von der Gestalt

$$\frac{u^2}{t^2},\quad \frac{kv^2}{t^2},\quad \frac{w^2}{t^2}, \tag{5}$$

wo der den drei Gliedern gemeinsame Faktor k weggelassen wird, und für u, v, w und t ganze rationale Zahlen ohne einen gemeinsamen Faktor genommen werden können. Es gilt dann

$$kv^2 - u^2 = w^2 - kv^2 = k_1 t^2, \tag{6}$$

wo k und k_1 komplementäre Faktoren von c, das heisst hier 330, bedeuten. Aus (6) ergibt sich

$$u^2 + w^2 - 2kv^2 = 0. \tag{7}$$

Das linke Glied von (7) soll also eine Nullform bedeuten, und k darf keine von den Faktoren 3 und 11 enthalten. Enthält andererseits k nur die Faktoren 2 oder 5 so hat (7) Lösungen. Hieraus folgt aber nicht, dass unter diesen Lösungen

auch solche existieren, die zu dem gegebenen k-Wert gehören. Hierfür ist nach (6) noch erforderlich, dass

$$w^2 - k v^2 - k_1 t^2 \tag{8}$$

eine Nullform sein soll. Die Bedingungen, welche hierin liegen, nämlich, dass k und k_1 quadratische Reste zu einander sind, lassen sich aber nicht erfüllen. Man hat hier die Zusammenstellungen

$$k = 10,\ k_1 = 33; \quad k = 5,\ k_1 = 66; \quad k = 2,\ k_1 = 165.$$

In keinem von diesen Fällen ist aber k quadratischer Rest zu k_1; es ist ja 10 kein Rest zu 11, 5 kein Rest zu 3 und 2 kein Rest zu 3, 5 und 11.

Wir kombinieren jetzt die obige Gruppe von Charakteren 1, k, 1 mit dem Charakter

$$-1, -1, 2.$$

Wir bekommen hierdurch neue Charaktere von der Gestalt $-1, -k, 2$ oder $-2, -k, 1$, wo k die Teiler von 165 durchläuft. Dies führt uns auf die Frage, in wie weit unter den Formen $u^2 - 2w^2 - 2kv^2$ oder $2u^2 - w^2 - 2kv^2$ Nullformen existieren. Bekanntlich wird die Antwort hier auf die entsprechende Frage für die Formen $2u^2 - w^2 - kv^2$ oder $u^2 - 2w^2 - kv^2$ zurückgeführt. Wir erhalten also die Bedingung, dass 2 quadratischer Rest von k sein soll. Da aber 2 Nichtrest zu 3, 5 und 11 ist, so ist dies nur für $k=1$ möglich. Nur für $k=1$ bekommen wir mithin hier Nullformen. Dann bekommen wir aber, in Analogie mit (6), die weiteren Bedingungen

$$u^2 - v^2 = v^2 + 2w^2 = 165\, t^2$$

bzw.

$$2u^2 - v^2 = v^2 + w^2 = 165\, t^2,$$

welche sich nicht erfüllen lassen. Hiermit ist bewiesen, dass die fünf Basiselemente

$$1, 2, 1;\ 1, 3, 1;\ 1, 5, 1;\ 1, 11, 1;\ -1, -1, 2$$

eine Gruppe von Charakteren erzeugen, unter denen nur das Einheitselement durch rationale Punkte auf der Kurve (3) vertreten wird. Der Rang dieser Kurve ist also auch nicht grösser als vier.

Auch in mehreren anderen Fällen, wie z. B. für $c = 210 = 2.3.5.7$, gelingt nach dieser Methode die genaue Bestimmung des Ranges. Doch werden die Überlegungen je weitläufiger, je mehr Primfaktoren c enthält. Als zweites Beispiel betrachten wir $c = 1254 = 2.3.11.19$. Im dritten Abschnitt werden wir fünf als

untere Grenze des Ranges für diesen Fall finden. Wollen wir beweisen, dass fünf auch der richtige Rang ist, so gilt es hier nur eine Gruppe von Charakteren mit vier erzeugenden Elementen zu bestimmen, so dass nur zu dem Einheitselemente rationale Punkte der Kurve gehören. Als solche Elemente nehmen wir

$$1,\ 2,\ 1;\ \ 1,\ 3,\ 1;\ \ 1,\ 11,\ 1;\ \ 1,\ 19,\ 1.$$

Die Gruppe besteht somit aus sämtlichen Charakteren $1,\ k,\ 1$, wo k die Teiler von 1254 durchläuft. Als erste Bedingung für rationale Punkte erhalten wir, dass

$$u^2 + w^2 - 2kv^2 = 0$$

rationale Lösungen besitzen soll. Unter den Faktoren 3, 11 und 19 darf mithin keiner in k enthalten sein. Nur der Fall $k = 2$ bleibt noch übrig zu behandeln. Hier hat man, in Übereinstimmung mit (6), noch die Bedingung, dass

$$2v^2 - u^2 = w^2 - 2v^2 = 627\,t^2$$

rationale Lösungen besitzen soll. Dies ist jedoch unmöglich, da 2 zu keiner der Primzahlen 3, 11 und 19 quadratischer Rest ist.

II.

5. Es sei jetzt c eine Primzahl p. Hier mag zunächst erwähnt werden, dass Billing in den Tabellen am Ende der zitierten Abhandlung die Resultate für $c = 2,\ 3,\ 5,\ 7$ mitgeteilt hat, und zwar hat die Kurve für $c = 2,\ 3$ den Rang zwei und für $c = 5,\ 7$ den Rang drei. Es ist weiter bekannt, dass für $p = 8k + 3$ der Rang nur zwei ist. Der niedrigste Rang, der bei den von uns behandelten Kurven vorkommen kann, ist zwei, da ja die drei Punkte auf der Achse zusammen mit dem unendlich entfernten Punkte ein System von diesem Range bilden. In diesen vier Punkten haben wir Repräsentanten für die Einheitsklasse und für die Klassen mit den Charakteren

$$p,\ 2,\ 1;\ \ -1,\ -p,\ 1;\ \ -1,\ -2,\ p. \tag{9}$$

Wenn es auf der Kurve noch andere rationale Punkte gibt, so lässt sich zeigen, dass der Rang höher als zwei ist. Gibt es nun auf der Kurve rationale Punkte, die zu anderen Klassen gehören, so lassen sich offensichtlich diese Klassen durch Komposition mit den oben angeführten auf solche reduzieren, für welche p nicht in den Charakteren eingeht. Derartige Charaktere gibt es ausser dem Einheitscharakter nur drei, nämlich

$$-1,\ -1,\ 1;\ \ 1,\ 2,\ 1;\ \ -1,\ -2,\ 1. \tag{10}$$

Die Frage nach dem Range ist also beantwortet, wenn man kennt, welche von den Klassen mit den Charakteren (10) durch rationale Punkte vertreten sind. *Je nachdem die Antwort auf keine, eine oder drei lautet, hat die Kurve den Rang zwei, drei oder vier.* Für $p = 2$ geht (9) in

$$(9_1) \qquad 1,\ 1,\ 2;\ -1,\ -2,\ 1;\ -2,\ -1,\ 1$$

über, und in (10) bleibt nur der erste Charakter $-1,\ -1,\ 1$ übrig.

Bei den Ausdrücken für $x - c$, x und $x + c$ in einem rationalen Punkt, die wir hier geben wollen, lassen wir die als Nenner auftretenden Quadrate t^2 fort. Dies bedeutet ja nur, dass in den Differenzen entsprechende Quadrate zu c hinzugefügt werden. Für den Charakter $-1,\ -1,\ 1$ erhalten dann die Ausdrücke der drei Grössen die Gestalt

$$(11) \qquad -u^2,\ -v^2,\ w^2.$$

Hieraus ergibt sich

$$(12) \qquad c \equiv u^2 - v^2 = w^2 + v^2.$$

Gibt es auf der Kurve rationale Punkte, die zu dieser Klasse gehören, so kann also c keine Primfaktoren $4k + 3$ enthalten. In entsprechender Weise erhalten wir für die nächstfolgende Klasse die Zusammenstellung:

$$(11_1) \qquad 2u^2,\ v^2,\ 2w^2;$$

$$(12_1) \qquad c \equiv v^2 - 2u^2 = 2w^2 - v^2.$$

In diesem Falle dürfen also in c keine Primfaktoren $8k + 3$ oder $8k + 5$ vorkommen. Für die letzte hier in Rede stehende Klasse $-1, -2, 1$ bekommen wir:

$$(11_2) \qquad -2u^2,\ -v^2,\ 2w^2;$$

$$(12_2) \qquad c \equiv 2u^2 - v^2 = 2w^2 + v^2.$$

Hier sind für c die Faktoren $8k + 3$, $8k + 5$ und $8k + 7$ ausgeschlossen.

Diese Ergebnisse bestätigen für den Fall, dass c eine Primzahl p bezeichnet, den Satz, dass für $p = 8k + 3$ der Rang nur zwei sein kann. *Wir finden auch, dass für $p = 8k + 5$ und $8k + 7$ der Maximalwert des Ranges drei ist. Nur für $p = 8k + 1$ gibt es eine Möglichkeit von einem Range vier.*

6. Es ist hier leicht einfache explizite Ausdrücke für c herzustellen. Leider enthalten diese Ausdrücke gewöhnlich überflüssige quadratische Faktoren. Aus (12) ergibt sich

$$u^2 - w^2 = 2v^2. \tag{13}$$

Es wird angenommen, dass u, v und w keine gemeinsame Faktoren besitzen. Nach (13) sind dann u und w ungerade Zahlen und v^2 teilbar durch vier. Man erhält aus (13)

$$u \pm w = 2m^2; \quad u \mp w = 4n^2.$$

Also haben wir

$$u = m^2 + 2n^2; \quad w = \pm (m^2 - 2n^2); \quad v = 2mn. \tag{14}$$

Als Ausdruck für c bekommen wir jetzt:

$$c \equiv (u+v)(u-v) = (m^2 + 2mn + 2n^2)(m^2 - 2mn + 2n^2) = \\ = ((m+n)^2 + n^2)((m-n)^2 + n^2) = m^4 + 4n^4 = f(m,n). \tag{15}$$

Hier sind m und n teilerfremde ganze Zahlen. Für m ist immer eine ungerade Zahl zu setzen. Je nachdem n gerade oder ungerade ist, hat man $c \equiv 1$ oder $\equiv 5$ (mod. 8). Da c also hier den Faktor 2 nicht enthalten kann, so gibt es, wenn c eine gerade Zahl ist, niemals auf der Kurve rationale Punkte mit dem Charakter $-1, -1, 1$. Hieraus folgt die Richtigkeit der Bemerkung in Nr. 3, nach welcher $2r+2$ die Maximalzahl des Ranges bezeichnet, wenn c r *ungerade* Faktoren enthält.

Nach (12_1) hat man

$$v^2 = u^2 + w^2. \tag{13$_1$}$$

Zwei Möglichkeiten gibt es hier für die Ausdrücke von u, v und w, nämlich:

$$\begin{aligned} &v = m^2 + n^2; \quad u = 2mn; \qquad w = m^2 - n^2. \\ &v = m^2 + n^2; \quad u = m^2 - n^2; \quad w = 2mn. \end{aligned} \tag{14$_1$}$$

Es gilt der obere oder untere Fall, je nachdem

$$m^2 - n^2 - 2mn \gtrless 0.$$

Wir erhalten jetzt

$$\begin{aligned} c &\equiv (w+u)(w-u) = \\ &= \pm (m^2 - n^2 + 2mn)(m^2 - n^2 - 2mn) = \pm [(m^2 - n^2)^2 - 4m^2n^2] = \\ &= \pm ((m+n)^2 - 2n^2)((m-n)^2 - 2n^2) = \pm [m^4 + n^4 - 6m^2n^2] = \\ &= \pm [(m^2 + n^2)^2 - 8m^2n^2] = \pm g(m,n). \end{aligned} \tag{15$_1$}$$

Es ist hier eine von den Zahlen m und n gerade und die andere ungerade. Auch hier kann c die Primzahl 2 nicht enthalten.

Zuletzt erhält man nach (12_2)

$$u^2 = v^2 + w^2. \tag{13_2}$$

Hier hat man als erste Möglichkeit

$$u = m^2 + n^2; \quad v = m^2 - n^2; \quad w = 2mn. \tag{14_2}$$

Es ergibt sich hieraus nach (12_2)

$$c \equiv (m^2 - n^2)^2 + 8m^2n^2 = (m^2 + n^2)^2 + 4m^2n^2 = m^4 + n^4 + 6m^2n^2 = h(m,n). \tag{15_2}$$

Auch hier muss c eine ungerade Zahl sein.

Bei der zweiten Möglichkeit haben wir

$$u = m^2 + n^2; \quad v = 2mn; \quad w = m^2 - n^2. \tag{16}$$

Hieraus folgt nach (12_2)

$$c \equiv 2(m^2 + n^2)^2 - 4m^2n^2 = 2(m^4 + n^4) = h_1(m,n). \tag{17}$$

Sämtliche vier Formen $f(m,n)$, $g(m,n)$, $h(m,n)$ und $h_1(m,n)$ übereinstimmen darin, dass sie harmonisch sind, und dass die äquianharmonische Invariante den Wert 4 hat. Für $h(m,n)$ und $h_1(m,n)$ soll eine von den Zahlen m und n gerade und die andere ungerade sein. Sind beide diese Zahlen ungerade, so ersetzt man dieselben durch $\frac{m+n}{2}$ und $\frac{m-n}{2}$ und kommt, nach Ausscheidung des Faktors 4, in die andere Form über. Durch $h_1(m,n)$ werden also nur gerade und durch die drei übrigen Formen nur ungerade c-Werte dargestellt; die etwa in den Formen eingehenden quadratischen Faktoren denken wir uns dabei ausgeschieden. Auf Grund der Komposition der Klassen gilt hier die bemerkenswerte Eigenschaft, dass *eine Zahl, welche durch zwei von den Formen $f(m,n)$, $g(m,n)$ und $h(m,n)$ ausgedrückt wird, sich auch durch die dritte Form ausdrücken lässt.* Man beachte noch, dass durch diese Formen keine Quadrate dargestellt werden können.

7. Wir betrachten zuerst die Form $h(m,n)$, welche nur Primfaktoren $8k+1$ enthalten kann. Es sei m eine gerade und n eine ungerade Zahl. Wenn man m und n variieren lässt, so bekommt man die verschiedenen rationalen Punkte mit dem Charakter -1, -2, 1. Die Kurve, zu welcher ein solcher Punkt gehört, wird durch den c-Wert bestimmt, der nach Wegschaffung der quadratischen Faktoren übrig bleibt. Wir geben hier einige Beispiele.

1) $m = 2,\ n = 1;\ c = 41.$
2) $m = 2,\ n = 3;\ c = 313.$
3) $m = 2,\ n = 5;\ c = 1241 = 17.73.$
4) $m = 4,\ n = 1;\ c = 353.$
5) $m = 4,\ n = 3;\ c = 1201.$
6) $m = 4,\ n = 5;\ c = 3281 = 17.193.$
7) $m = 6,\ n = 1;\ c = 1513 = 17.89.$
8) $m = 14,\ n = 1;\ c = 137 \equiv 137.289.$

Dass in dem letzten Beispiel 137 nicht ohne Hinzufügung eines quadratischen Faktors in der Gestalt $h(m, n)$ geschrieben werden kann, sieht man leicht, und der kleinste quadratische Faktor, der hier auftreten kann, ist ja $289 = 17^2$. Hier stellt sich die Frage auf, wie sich zu einem gegebenen c-Wert ein Quadrat K^2 bestimmen lässt, sodass das Produkt cK^2 bei geigneter Wahl von m und n sich in der Gestalt $h(m, n)$ schreiben lässt; dabei dürfen offenbar c und K nur Primfaktoren $8k + 1$ enthalten. In

$$c = a^2 + b^2, \qquad K = \xi^2 + \eta^2$$

denken wir uns Darstellungen von c und K als Summe von zwei Quadraten. Man hat dann

$$K^2 = (\xi^2 - \eta^2)^2 + 4\,\xi^2\eta^2.$$

Für das Produkt cK^2 erhalten wir jetzt

$$(a(\xi^2 - \eta^2) + 2\,b\,\xi\eta)^2 + (b(\xi^2 - \eta^2) - 2\,a\,\xi\eta)^2. \tag{18}$$

Aus (15_2) sehen wir, dass $h(m, n)$ sich als Summe der Quadrate zweier Grössen darstellen lässt, die von der Art sind, dass wir für die Summe und die Differenz der Grössen die Quadrate $(m + n)^2$ und $(m - n)^2$ erhalten. Es entsteht so die Frage, wie sich diese Bedingungen für (18) ausdrücken. Man erhält hierzu die Antwort, dass ξ und η so gewählt werden müssen, dass die Formen

$$\begin{aligned} &(a + b)(\xi^2 - \eta^2) - 2(a - b)\,\xi\eta; \\ &(a - b)(\xi^2 - \eta^2) + 2(a + b)\,\xi\eta \end{aligned} \tag{19}$$

Quadrate darstellen, wobei es natürlich erlaubt ist für eine Form (19) das Zeichen zu ändern. Als Diskriminante der beiden Formen (19) bekommt man

$$8(a^2 + b^2) = 8c.$$

Für die Existenz der Begleitformen (19) von c ist es nur notwendig, dass die Primfaktoren von c die Gestalt $4k+1$ haben. Ohne die Verschärfung von $4k+1$ zu $8k+1$ ist es aber nie möglich die obigen Bedingungen für ξ und η zu erfüllen.

Für $c = 137$ haben wir $a = 11$, $b = 4$, und die Formen (19) gehen in

$$15(\xi^2 - \eta^2) - 14\xi\eta; \quad 7(\xi^2 - \eta^2) + 30\xi\eta$$

über. Im Beispiel 8) können wir setzen $\xi = 4$, $\eta = 1$. Nach Einführung dieser Werte in die Formen erhalten wir die Quadrate 169 und 225. Die Ermittlung neuer Lösungen scheint eine recht schwierige Aufgabe zu sein. Wir versuchen mit dem einfachsten Falle $c = 41$. Als Formen (19) erhalten wir hier

$$9(\xi^2 - \eta^2) - 2\xi\eta; \quad \xi^2 - \eta^2 + 18\xi\eta.$$

Der Lösung $\xi = 1$, $\eta = 0$, für welche wir die Quadrate 9 und 1 bekommen, entspricht das oben angegebene Beispiel 1). Es gilt für $c = 41$ einen anderen rationalen Punkt auf der Kurve mit dem Charakter -1, -2, 1 anzugeben. Zu dem Ende können wir von rationalen Punkten der Kurve mit Charakteren -1, -1, 1 und 1, 2, 1 ausgehen, die wir in den folgenden Nummern bestimmen. Wenn wir zwei solche Punkte durch eine gerade Linie verbinden, so gehört ja der dritte Schnittpunkt zum Charakter -1, -2, 1. Je nach der Wahl der y-Werte für die beiden ersten bekommen wir für den dritten Punkt zwei Lösungen für $x - c$, x und $x + c$. Für eine von diesen Lösungen, die uns bereits durch das Beispiel 1) bekannt ist, haben wir $K = 1$. Für die andere erhält man $K =$ der Primzahl 21089.

8. Für die zu dem Charakter -1, -1, 1 gehörenden c-Werte haben wir nach (15)

$$c \equiv [(m+n)^2 + n^2]\,[(m-n)^2 + n^2].$$

Wünscht man hier Primzahlwerte für c, so muss einer von diesen Faktoren eine quadratische Zahl darstellen. Nun sieht man leicht, dass bei einem gegebenen Wert für den einen Faktor der mitfolgende sich in vier verschiedenen Weisen bestimmen lässt. Man hat ja bei der Darstellung des gegebenen Faktors freie Wahl einerseits zwischen geradem und ungeradem n, andererseits zwischen gleichen und verschiedenen Zeichen für m und n, und eine Änderung bei diesen Wahlen hat Einfluss auf den anderen Faktor. Wir nehmen an, der Wert des Faktors $(m+n)^2 + n^2$ sei ein Quadrat. Es gibt dann zwei Möglichkeiten für die Dar-

stellung des anderen Faktors durch zwei Parameter μ und ν. Wenn n ungerade ist, setzen wir

$$n = \mu^2 - \nu^2, \quad m + n = 2\mu\nu, \quad m - n = 2(\mu\nu - \mu^2 + \nu^2).$$

Wir erhalten hieraus

$$(20) \qquad (m-n)^2 + n^2 = 4(\mu\nu - \mu^2 + \nu^2)^2 + (\mu^2 - \nu^2)^2.$$

Bei geradem n werden die Substitutionen für n und $m + n$ vertauscht, und wir bekommen

$$n = 2\mu\nu, \quad m + n = \mu^2 - \nu^2, \quad m - n = \mu^2 - \nu^2 - 4\mu\nu.$$

Es ergibt sich also

$$(20_1) \qquad (m-n)^2 + n^2 = (\mu^2 - \nu^2 - 4\mu\nu)^2 + 4\mu^2\nu^2.$$

Man kann in (20) und (20_1) μ und ν mit gleichen oder verschiedenen Zeichen nehmen. Der Ausdruck für $(m+n)^2+n^2$ wird in allen Fällen $(\mu^2+\nu^2)^2$. Bemerkenswert ist, dass die Formen (20) und (20_1) gleichwertige Invarianten besitzen.

Hier folgen einige Beispiele. Zuerst werden die Werte der Faktoren von $f(m, n)$ und dann c angegeben.

1) $m = 1$, $n = 1$; $c = 5$.
2) $m = 1$, $n = 3$; 13.25; $c = 13$.
3) $m = 7$, $n = 5$; 29.169; $c = 29$.
4) $m = -1$, $n = 21$; 925.841; $c = 37$.
5) $m = 41$, $n = 39$; $1525.7921 = 61.25.89^2$; $c = 61$.
6) $m = -1$, $n = 4$; 41.25; $c = 41$.
7) $m = -7$, $n = 4$; 137.25; $c = 137$.
8) $m = 1$, $n = 20$; 761.841; $c = 761$.

Aus diesen Beispielen sehen wir, dass für $c = 5, 13, 29, 37$ und 61 der Rang der Kurve drei ist. Es gibt nur noch eine einzige Primzahl $8k + 5 < 100$, nämlich 53. Die Frage, ob für $c = 53$ der Rang zwei oder drei ist, lassen wir unbeantwortet. Wichtiger sind hier die resultierenden Primzahlen $8k + 1$, weil unter diesen die Fälle vom Range vier für $c = p$ zu suchen sind. Da nach der vorhergehenden Nummer für $c = 41$ und $c = 137$ auch der Charakter $-1, -2, 1$ durch rationale Punkte auf der Kurve vertreten wird, so folgt daraus bereits, dass *in diesen Fällen der Rang vier ist. Für $c = 761$ verhält es sich ebenso,* wie wir in der folgenden Nummer finden werden. Andere zwei- oder dreiziffrige Primzahlen $8k + 1$ für c als die drei oben angegebenen habe ich bei Fortsetzung

der Untersuchungen nicht finden können. Die Primzahlen $8k + 1$ scheinen also hier viel seltener auftreten als die Primzahlen $8k + 5$. Die vierzifferigen Primzahlwerte $8k + 1$ für c, die ich gefunden habe, sind:

(21) 1217, 1321, 2777, 3881, 4441, 6641, 9281, 9377, 9521, 9601.

Wir geben noch einige Beispiele, wo c Produkt von zwei Primzahlen ist.

9) $m = 7$, $n = 8$; 65.289; $c = 65 = 5.13$.

10) $m = 47$, $n = 12$; $3625.1369 = 125.29.\overline{37}^2$; $c = 145 = 5.29$.

11) $m = 11$, $n = 8$; 425.73; $c = 17.73 = 1241$.

12) $m = 61$, $n = 8$; $4825.2873 = 193.25.17.169$; $c = 17.193$.

Wenn man die Primzahlen 5 und 13 bzw. 5 und 29 auf die beiden Faktoren von $f(m, n)$ verteilt, so bekommt man $c = 65$ und $c = 145$ für $m = 1$, $n = 2$ bzw. $m = 3$, $n = 2$. Die Lösungen $c = 17.73$ und $c = 17.193$ fand ich zuerst bei den Charakteren -1, -2, 1 und 1, 2, 1. Dadurch erhielt ich die Veranlassung zur Aufsuchung dieser Lösungen auch für den Charakter -1, -1, 1.

9. Für den noch zu behandelnden Charakter 1, 2, 1 haben wir nach (15_1)

$$c \equiv \pm [(m + n)^2 - 2n^2][(m - n)^2 - 2n^2].$$

Je nachdem das obere oder untere Zeichen gilt, ist $c \equiv 1$ oder $c \equiv 7 \pmod 8$. Hat man nun für c eine Primzahl p, so muss einer von den obigen Faktoren ein Quadrat sein. Da wir hier die Rollen von m und n wechseln können, so ist es erlaubt für n eine gerade Zahl zu nehmen. Ist jetzt

$$(m + n)^2 - 2n^2 = l^2,$$

so können wir setzen

$$m + n \pm l = 2\mu^2; \quad m + n \mp l = 4\nu^2; \quad n = 2\mu\nu.$$

Hieraus folgt

$$m + n = \mu^2 + 2\nu^2; \quad l = \pm(\mu^2 - 2\nu^2); \quad m - n = \mu^2 + 2\nu^2 - 4\mu\nu.$$

Nach Ausscheidung des quadratischen Faktors $(\mu^2 - 2\nu^2)^2$ bekommt man

(22) $$c \equiv \pm [(\mu^2 + 2\nu^2 - 4\mu\nu)^2 - 8\mu^2\nu^2].$$

Hierzu fügen wir einige Beispiele.

1) $m = 1$, $n = 2$; $c = 7$.

2) $m = 13$, $n = 6$; 289.23; $c = 23$.

3) $m = 5$, $n = 4$; 49.31; $c = 31$.

4) $m = 53$, $n = 36$; $5329.2303 = \overline{73}^2.49.47$; $c = 47$.

5) $m = 6$, $n = 5$; 71.49; $c = 71$.

6) $m = 5$, $n = 2$; $c = 41$.

7) $m = 37$, $n = 14$; $2209.137 = \overline{47}^2.137$; $c = 137$.

8) $m = 41$, $n = 10$; $2401.761 = 7^4.761$; $c = 761$.

9) $m = 13$, $n = 4$; 257.49; $c = 257$.

10) $m = 17$, $n = 6$; 457.49; $c = 457$.

11) $m = 7$, $n = 2$; $c = 17.73$.

12) $m = 11$, $n = 4$; $c = 17.193$.

Für $c = 7$, 23, 31, 47 und 71, also für die fünf ersten Primzahlen $8k + 7$, ist mithin der Rang drei. Ein analoges Verhältniss bemerkten wir in der vorigen Nummer für die Primzahlen $8k + 5$. Primzahlen $8k + 1 < 100$ gibt es fünf, nämlich 17, 41, 73, 89 und 97. Wie wir gesehen haben ist es sehr leicht für $c = 41$ repräsentierende Punkte zu den drei Charakteren -1, -1, 1; 1, 2, 1 und -1, -2, 1 zu finden. Dagegen ist uns dies in keinem Falle für die vier Primzahlen 17, 73, 89 und 97 gelungen. Die Vermutung liegt nahe, dass der Rang in diesen vier Fällen nicht über zwei kommt[1]. Die Primzahlwerte für c, zu denen wir einen Rang vier gefunden haben, sind 41, 137 und 761. Doch haben wir hier für $c = 761$ keine zum Charakter -1, -2, 1 gehörende Lösung gegeben; eine solche lässt sich wohl kaum ohne einen sehr grossen mitfolgenden quadratischen Faktor herstellen. Meine Bestrebungen auch für andere Fälle $c = p$ einen Rang vier nachzuweisen, wie z. B. für eine von den zehn Primzahlen (21), haben zu keinem Resultate geführt. Ich muss also die Frage offen lassen, ob es eine begrenzte oder unbegrenzte Anzahl derartiger Primzahlen $8k + 1$ gibt. Nach unseren Resultaten sind noch zwei andere Kurven, $c = 17.73$ und $c = 17.193$, durch rationale Punkte für sämtliche drei Charaktere vertreten. Auch hier bleibt die Frage unentschieden, in wie weit, wenn c sowohl Primzahl als zusammengesetzte Zahl sein darf, die Anzahl der Werte mit dieser Eigenschaft begrenzt oder unbegrenzt ist.

10. Wir betrachten hier noch den Fall $c = 2p$. Nach Nr. 6 wissen wir, dass, wenn c den Faktor 2 enthält, so kann unter den Charakteren -1, -1, 1; 1, 2, 1 und -1, -2, 1 höchstens der letzte durch rationale Punkte vertreten werden. Hieraus zogen wir die Folgerung, dass für $c = 2p$, wo p eine ungerade Primzahl

[1] Dies folgt in der Tat aus einem Satze, nach welchem für $c = p = a^2 + b^2 \equiv 1 \pmod 8$ mit $a + b \equiv \pm 3 \pmod 8$ der Rang nur zwei ist.

bedeutet, der Rang höchstens vier sein kann. Bei diesem höchsten Rang vier müssen notwendig rationale Punkte mit dem Charakter $-1, -2, 1$ auf der Kurve vorkommen. Nach (17) hat man dann

$$c \equiv 2(m^4 + n^4) = h_1(m, n)$$

wo eine von den Zahlen m und n gerade und die andere ungerade sein soll. Primfaktoren von $m^4 + n^4$ müssen in diesem Falle von der Gestalt $16k + 1$ sein. Dagegen ist bei den drei Fällen $c = p$, nämlich $p = 41$, 137 und 761, für welche wir den Rang vier gefunden haben, stets $p \equiv 9 \pmod{16}$. Der Gedanke liegt nahe, dass dies überhaupt für Primzahlen gilt, die zu dem Range vier führen.

Wir geben zunächst einige Beispiele

1) $m = 1$, $n = 2$; $c = 2.17$.
2) $m = 2$, $n = 3$; $c = 2.97$.
3) $m = 1$, $n = 4$; $c = 2.257$.
4) $m = 3$, $n = 4$; $c = 2.337$.
5) $m = 2$, $n = 5$; $c = 2.641$.
6) $m = 5$, $n = 6$; $c = 2.1921$.
7) $m = 13$, $n = 8$; $c = 2.113$.

Im letzten Falle ist ein Faktor 17^2 von $m^4 + n^4$ ausgeschieden.

Nach Nr. 2, womit man »*Rang von Kurven*», S. 228 vergleichen mag, sind für $c = 2p_1p_2 \ldots p_r$ die Charaktere, welche die Punkte $x = c$, 0, $-c$ auf der Achse als Repräsentanten haben, bzw.

$$(23) \qquad p_1p_2 \ldots p_r,\ 1,\ 2;\ -1,\ -2p_1p_2 \ldots p_r,\ 1;\ -p_1p_2 \ldots p_r,\ -1,\ 2.$$

Die beiden ersten können wir als erzeugende Elemente der Gruppe der Charaktere wählen. Für die Bestimmung des Ranges muss man wissen, wie viele andere erzeugende Elemente noch nötig sind. Dass für $c = 2.17$ der Rang vier ist wird durch die Existenz der Folge

$$(24) \qquad 1,\ 9,\ 17,\ 25$$

klargelegt. Hieraus erhalten wir ja unmittelbar die beiden Punkte, wobei die zugehörigen Charaktere beigefügt werden:

$$(25) \qquad (1,\ 9,\ 17)\ \tfrac{17}{4};\ 1,\ 1,\ 17.$$

$$(25_1) \qquad (9,\ 17,\ 25)\ \tfrac{17}{4};\ 1,\ 17,\ 1.$$

Durch Kombination bekommen wir weiter

(25_2) $\qquad (17, 49, 81)\ \frac{17}{16};\ 17,\ 1,\ 1.$

Da keiner der Charaktere (25), (25_1) und (25_2) mit einem Charakter (23) für $p_1 p_2 \ldots p_r = 17$ zusammenfällt, so muss der Rang vier sein.

Wir geben noch für $c = 34$ Repräsentanten für die übrigen Charaktere. Ohne Mühe findet man

$$(16, 25, 34)\ \tfrac{34}{9};\ 1,\ 1,\ 2.17.$$
$$(64, 81, 98)\ 2;\ 1,\ 1,\ 2.$$
$$(16, 17, 18)\ 34;\ 1,\ 17,\ 2.$$

Indem wir die Relationen (4) benutzen, finden wir leicht die folgenden Punkte, die zu den noch übrigen Charakteren gehören.

$$(-50, -16, 18);\ -1, -2, 1.$$
$$(-36, -2, 32);\ -2, -1, 1.$$
$$(-98, -17, 64)\ \tfrac{34}{81};\ -2, -17, 1.$$
$$(-34, -9, 16)\ \tfrac{34}{25};\ -2.17, -1, 1.$$
$$(-81, -32, 17)\ \tfrac{34}{19};\ -1, -2, 17.$$
$$(-17, -8, 1)\ \tfrac{34}{9};\ -17, -2, 1.$$

Ein anderes Beispiel, wo man leicht sieht, dass der Rang vier ist, haben wir in $c = 2.113$. Ein rationaler Punkt ist hier

$$(49, 81, 113)\ \tfrac{118}{16};\ 1,\ 1,\ 113.$$

Durch Komposition von $-1, -2, 1$ mit $1, 1, 113$ erhält man

$$-1, -2, 113.$$

Da keiner von diesen drei Charakteren mit einem Charakter (23) identisch ist, so ist unsere Behauptung bewiesen. Für diese Kurve geben wir noch die folgenden rationalen Punkte:

$$(64, 113, 162)\ \tfrac{226}{49};\ 1,\ 113,\ 2.$$
$$(56^2, 57^2, 2.41^2)\ 2;\ 1,\ 1,\ 2.$$
$$(113, 41^2, 57^2)\ \tfrac{113}{16.49};\ 113,\ 1,\ 1.$$

Aus diesen Punkten lassen sich vermittelst der Relationen (4) andere herleiten. Zuletzt bemerken wir, dass der Charakter $-2, -1, 1$ durch Komposition von $1, 1, 2$ und $-1, -2, 1$ entsteht. Die Charaktere, in denen p nicht eingeht, sind mithin dieselben für $p = 17$ und $p = 113$.

11. Für $c = 2p$, ebenso wie für $c = p$, können wir mit Hilfe von (23) die vorkommenden Charaktere auf solche reduzieren, in denen p nicht eingeht. Diese bilden eine Gruppe (2, 2, 2), für welche man $-1, -1, 1$; $1, 2, 1$; und $2, 1, 1$ als erzeugende Elemente nehmen kann. Die in dieser Gruppe enthaltenen Charaktere der Kurve können entweder aus einer Vierergruppe, aus einer G_2 oder nur aus der Identität bestehen. Je nachdem dies der Fall ist, hat die Kurve den Rang vier, drei oder zwei. Dabei bezeichnen wir als Charaktere der Kurve diejenigen Charaktere, die auf der Kurve repräsentierende Punkte besitzen. Für den Rang vier kennen wir bereits die Bedingung, dass $-1, -2, 1$ ein Charakter der Kurve sein muss. Dieser Charakter ist Element in drei Vierergruppen. Abgesehen von der Identität, enthalten diese Vierergruppen die Tripel:

(26) $\quad -1, -1, 1;\ -1, -2, 1;\ 1, 2, 1.$

(26_1) $\quad -1, -1, 2;\ -1, -2, 1;\ 2, 1, 1.$

(26_2) $\quad -2, -1, 1;\ -1, -2, 1;\ 1, 1, 2.$

Mit (26) brauchen wir uns hier nicht aufzuhalten, da wir aus Nr. 6 wissen, dass, wenn c eine gerade Zahl ist, $-1, -1, 1$ und $1, 2, 1$ niemals Charaktere der Kurve sind. Betreffend die Elemente in (26_1) werden wir finden, dass dieselben niemals gleichzeitig Charaktere einer Kurve sein können. Im Falle vom Range vier muss also das Tripel (26_2) aus Charakteren der Kurve bestehen. Zwei Beispiele hierzu kennen wir bereits aus der vorhergehenden Nummer.

Bei den folgenden Zusammenstellungen für $x - c$, x und $x + c$ wird der gemeinsame Faktor 2 fortgelassen. Für den Charakter $-1, -1, 2$ erhalten wir

$$-u^2,\ -v^2,\ 2w^2.$$

Setzen wir $c = 2c_1$, so ergibt sich hieraus

(27) $$c_1 \equiv u^2 - v^2 = v^2 + 2w^2.$$

Man hat also

(28) $$u^2 = 2(v^2 + w^2).$$

Aus (28) folgert man, dass u gerade, dagegen v und w ungerade sein müssen. Es ist mithin $c_1 \equiv 3 \pmod 8$. Primfaktoren von c_1 können sowohl $\equiv 1$ als $\equiv 3 \pmod 8$ sein; doch muss die Anzahl von der letzteren Art ungerade sein. Im Falle einer Primzahl c_1 muss also diese hier von der Gestalt $8k + 3$ sein. Da hier für den Charakter $-1, -2, 1$ $c_1 \equiv 1 \pmod{16}$ ist, so sieht man, dass das

Tripel (26_1) niemals Charaktere einer und derselben Kurve sein kann. Hierzu fügen wir einige Beispiele.

1) $u = 2,\ v = w = 1;\ c = 2.3.$
2) $u = 10,\ v = 1,\ w = 7;\ c = 2.11.$
3) $u = 50,\ v = 31,\ w = 17;\ c = 2.19.$
4) $u = 26,\ v = 17,\ w = 7;\ c = 2.43.$

Bei den vier ersten Fällen $c = 2p$ für $p = 8k + 3$ ist demnach der Rang drei. Für $c = 6$ findet man dieses Resultat in den Tabellen am Ende der Ahandlung von BILLING.

In ähnlicher Weise nehmen wir für den Charakter 2, 1, 1 den Ausgangspunkt von

$$2u^2,\ v^2,\ w^2.$$

Man hat also

$$(27_1) \qquad c_1 \equiv v^2 - 2u^2 = w^2 - v^2;$$

$$(28_1) \qquad w^2 = 2(v^2 - u^2).$$

Aus (28_1) ist ersichtlich, dass w teilbar durch 4, u und v dagegen ungerade Zahlen sein müssen. Nach Einführung von zwei Parametern m und n bekommen wir jetzt leicht die folgende Darstellung für u, v und w:

$$(29) \qquad u = \pm(m^2 - 2n^2);\quad v = m^2 + 2n^2;\quad w = 4mn.$$

Hieraus ergibt sich nach (27_1)

$$(30) \qquad c_1 = -(m^2 + 2n^2 + 4mn)(m^2 + 2n^2 - 4mn) = -(m^4 + 4n^4 - 12m^2n^2) =$$
$$= 16m^2n^2 - (m^2 + 2n^2)^2 = 8m^2n^2 - (m^2 - 2n^2)^2.$$

Nehmen wir m und $n > 0$, so gilt hier die Bedingung

$$4mn > m^2 + 2n^2.$$

In (30) soll m eine ungerade Zahl bedeuten; dagegen kann n sowohl gerade als ungerade sein. Die Primfaktoren von c_1 sind von der Gestalt $8k \pm 1$. Da $c_1 \equiv -1 \pmod 8$, so müssen Primfaktoren $8k-1$ in ungerader Anzahl auftreten. Eine Primzahl c_1 muss also von dieser Art sein. Je nach dem Faktor von (30), der Quadrat ist, kann man für c_1 in zwei Weisen eine Primzahl erhalten. Wir schreiben

$$(31) \qquad 4mn - m^2 - 2n^2 = 2n^2 - (m - 2n)^2;$$

$$(31_1) \qquad m^2 + 2n^2 + 4mn = (m + 2n)^2 - 2n^2.$$

Soll nun erstens (31) ein Quadrat bezeichnen, so muss offenbar n eine ungerade Zahl sein. Es ist dann $2n^2 \equiv 2 \pmod{16}$; Hieraus folgt $(m - 2n)^2 \equiv 1 \pmod{16}$. Das Quadrat ist also $\equiv 1 \pmod{16}$. Man sieht hieraus, dass der Ausdruck $(31_1) \equiv -1 + 8mn \equiv 7 \pmod{16}$ sein muss; etwa hierin eingehende quadratische Faktoren sind $\equiv 1 \pmod{16}$. Ist c_1 eine Primzahl, so muss mithin diese $\equiv 7 \pmod{16}$ sein. Zwei Beispiele findet man sofort.

1) $m = n = 1$; $c = 2.7$.
2) $m = 3$, $n = 1$; $c = 2.23$.

Ist andererseits (31_1) ein Quadrat, so muss n eine gerade Zahl sein. Wie man leicht sieht, ist dann der Ausdruck $(30) \equiv -1 \pmod{16}$. Da etwa auftretende quadratische Faktoren $\equiv 1 \pmod{16}$, so ist c_1 hier $\equiv -1 \pmod{16}$, was auch gilt, wenn c_1 eine Primzahl bedeutet.

Hier folgen nun einige weitere Beispiele.

3) $m = 7$, $n = 10$; $c = 2.31$.
4) $m = 7$, $n = 6$; $c = 2.47$.
5) $m = 31$, $n = 10$; $c = 2.79$.
6) $m = 17$, $n = 8$; $c = 2.127$.

Nun sind 7 und 23 die beiden ersten Primzahlen $16k + 7$ und ebenso 31, 47, 79 und 127 die vier ersten Primzahlen $16k - 1$. In allen diesen Fällen ist mithin der Rang drei für $c = 2p$.

12. Wir sind also, um den Rang vier zu erreichen, auf das Tripel (26_2) hingewiesen. Wenn wir hier zunächst den Charakter 1, 1, 2 in Betracht nehmen, so haben wir unseren Ausgangspunkt in der Folge

$$u^2,\ v^2,\ 2w^2.$$

Wir erhalten hieraus

$$c_1 \equiv v^2 - u^2 = 2w^2 - v^2.$$

Es gilt also die Relation

$$u^2 = 2(v^2 - w^2),$$

welche aus (28_1) hervorgeht, wenn man u und w vertauscht. Hieraus folgt, dass man für c_1 dieselbe Parameterdarstellung wie im vorhergehenden Falle erhält, nur mit geändertem Zeichen. Wir bekommen mithin

$$(32) \qquad c_1 \equiv m^4 + 4n^4 - 12m^2n^2 = (m^2 - 2n^2)^2 - 8m^2n^2 =$$
$$= (m^2 + 2n^2)^2 - 16m^2n^2 = [(m + 2n)^2 - 2n^2]\,[(m - 2n)^2 - 2n^2] = \bar{g}(m, n).$$

Hier hat man, wenn m und $n > 0$ genommen werden,

$$m^2 + 2n^2 > 4mn.$$

Ist nun c_1 eine Primzahl, so muss einer von den quadratischen Faktoren ein Quadrat sein. Hierfür hat man die Bedingung, dass n eine gerade Zahl sein muss, und man findet nach derselben Schlussweise wie am Ende der vorigen Nummer, dass eine solche Primzahl $\equiv 1 \pmod{16}$ ist. Auch hier geben wir einige Beispiele.

1) $m = 1,\ n = 2;\ c = 2.17.$
2) $m = 1,\ n = 6;\ c = 2.97.$
3) $m = 7,\ n = 2;\ c = 2.113.$
4) $m = 23,\ n = 42;\ c = 2.193.$
5) $m = 79,\ n = 22;\ c = 2.257.$
6) $m = 49,\ n = 12;\ c = 2.337.$
7) $m = 1,\ n = 30;\ c = 2.1921.$

In sämtlichen diesen sieben Fällen ist der Rang vier. Für sechs Fälle ist dies bereits durch Nr. 10 klargelegt, wo man findet, dass auch $-1, -2, 1$ ein Charakter dieser Kurven ist. Für $c = 2.337$ folgt der Beweis aus den hier bei Betrachtung des Charakters $-2, -1, 1$ folgenden Resultaten. Man beachte, dass unter den sieben ersten Primzahlen $16k+1$, 17, 97, 113, 193, 241, 257 und 337 nur eine, nämlich 241, hier oben fehlt.

Beim übrig bleibenden Charakter $-2, -1, 1$ hat man für die drei Grössen $x - c$, x und $x + c$ die Ausdrücke

$$-2u^2,\ -v^2,\ w^2.$$

Man bekommt also

$$c_1 \equiv 2u^2 - v^2 = v^2 + w^2.$$

Hieraus ergibt sich die Relation

$$w^2 = 2(u^2 - v^2),$$

welche sich von (28_1) nur darin unterscheidet, dass u und v Platz gewechselt haben. Aus den beiden Ausdrücken für c_1 sieht man, dass c_1 hier nur Primfaktoren $8k + 1$ enthalten kann. Man bekommt die Parameterdarstellung

$$u = m^2 + 2n^2,\quad v = \pm(m^2 - 2n^2),\quad w = 4mn.$$

Man erhält

$$(32_1)\qquad c_1 \equiv m^4 + n^4 + 12m^2n^2 = (m^2 + 2n^2)^2 + 8m^2n^2 =$$
$$= (m^2 - 2n^2)^2 + 16m^2n^2 = h(m, n).$$

Wie im vorhergehenden Falle ist $c_1 \equiv 1 \pmod{16}$. Ist c_1 eine Primzahl p, so ist also $p = 16k + 1$. Zuletzt geben wir einige Beispiele.

1) $m = 1$, $n = 1$; $c = 2.17$.
2) $m = 11$, $n = 3$; $c = 2.97$.
3) $m = 1$, $n = 2$; $c = 2.113$.
4) $m = 3$, $n = 1$; $c = 2.193$.
5) $m = 29$, $n = 8$; $c = 2.257$.
6) $m = 27$, $n = 2$; $c = 2.337$.
7) $m = 1$, $n = 3$; $c = 2.433$.
8) $m = 1$, $n = 4$; $c = 2.1217$.

Hierbei sind die folgenden Identitäten benutzt:

$$97.17^2 = 103^2 + 132^2;$$
$$257.73^2 = 713^2 + 928^2;$$
$$337.41^2 = 721^2 + 216^2.$$

Da $c = 2.193$ hier unter den Beispielen vorkommt, so ist es bewiesen, dass der Rang für diesen c-Wert vier ist. Zu $c = 2.193$ muss dann auch der Charakter $-1, -2, 1$ gehören. Dies wird übrigens durch die Identität

$$193.73^2 = 961^2 + 324^2 = 31^4 + 18^4$$

bestätigt.

Für $c = 2c_1$ erhält man beim Charakter $-1, -2, 1$ den Wertvorrat für c_1 durch die Form $m^4 + n^4$, wobei eine von den Zahlen m und n gerade anzunehmen ist. Ersetzt man hier n mit $2n$, so bekommt man die Form

$$(32_2) \qquad m^4 + 16n^4 = \bar{f}(m, n).$$

In $\bar{f}(m, n)$, $\bar{g}(m, n)$ und $\bar{h}(m, n)$ haben wir drei harmonische Formen mit derselben äquianharmonischen Invariante 16. Man bemerke die Analogie mit dem in Nr. 6 auftretenden Formentripel $f(m, n)$, $g(m, n)$ und $h(m, n)$.

Aus den vorangehenden Auseinandersetzungen ist ersichtlich, dass, falls ein Charakter in einem der Tripel (26_1) oder (26_2) auf einer Kurve Repräsentanten hat, so kann c keinen Primfaktor $8k + 5$ enthalten. *Es ist also der Rang nur zwei für $c = 2p$, wenn p eine Primzahl $8k + 5$ bedeutet.* Wir wissen weiter, dass, falls c_1 eine Primzahl p bezeichnet, so hat man für die Charaktere $-1, -1, 2$ und $2, 1, 1$ $p = 8k + 3$ bzw. $8k + 7$ und für die Charaktere $-2, -1, 1$; $-1, -2, 1$ und $1, 1, 2$ $p = 16k + 1$. *Auch wenn p eine Primzahl $16k + 9$ ist, hat mithin*

die Kurve für $c = 2p$ nur den Rang zwei. Hierzu kommt, dass es für $p = 8k+3$ und $p = 8k + 7$ eine Möglichkeit vom Range drei gibt, und dass nur für $p = 16k + 1$ der Rang vier sich erreichen lässt.

III.

13. Wir wollen in dieser Nummer den Fall, wo c ein Produkt von zwei ungeraden Primzahlen darstellt, durch einige Beispiele beleuchten. Es ist uns nicht gelungen die Frage zu entscheiden, ob in diesem Falle der Rang höher als vier sein kann oder nicht. In der Tat kennen wir kein Beispiel von so hohem Range als fünf, wo c nicht ausser den Faktoren 2 und 3 noch wenigstens zwei ungerade Primfaktoren enthält.

Nach Nr. 9 wissen wir, dass für $c = 17.73$ und $c = 17.193$ der Rang nicht <4 ist. Wir wollen hier zeigen, dass in diesen Fällen der Rang auch nicht >4 sein kann. In

$$17,\ 1,\ 1;\ 1,\ 17,\ 1;\ 1,\ 1,\ 17 \tag{33}$$

nebst dem Einheitscharakter haben wir die Elemente einer Vierergruppe. Eine Bedingung dafür, dass wir für $c = 17.73$ einen Charakter der Kurve aus (33) erhalten ist nun, dass wenigstens eine von den Identitäten

$$x^2 - 17y^2 \pm 73z^2 = 0$$

sich befriedigen lässt. Dies ist aber unmöglich, da 17 und 73 zu einander quadratische Nichtreste sind. Da dasselbe für 17 und 193 gilt, so ist es erwiesen, dass für $c = 17.73$ und $c = 17.193$ der Rang vier ist.

Andererseits haben wir in 17 und 137 zwei Primzahlen $8k + 1$, welche von einander quadratische Reste sind. Dass für $c = 17.137$ der Rang $\geqq 4$ ist, sieht man aus der Folge

$$121,\ 137,\ 153,\ 169,$$

welche von einer Art ist, die in der Fortsetzung dieses Abschnitts eine Hauptrolle spielen wird. Die Bedingung hier für einen Rang >4 ist, dass zu mindestens einem von den Charakteren

$$-1,\ -1,\ 1;\ 1,\ 2,\ 1;\ -1,\ -2,\ 1$$

rationale Punkte auf der Kurve gehören. Es ist uns aber nicht gelungen derartige Punkte zu finden.

Zwei andere Beispiele, wo der Rang der Kurve vier ist, haben wir für $c=5.13$ und $c=5.29$. Wir wissen aus Nr. 8, dass in diesen Fällen -1, -1, 1 zu den Charakteren der Kurve gehört. Für $c=5.13$ findet man leicht auf der Kurve den Punkt

$$(5,\ 9,\ 13)\ 65. \tag{34}$$

Es sind also in diesem Falle auch 5, 1, 13 und -5, -1, 13, welche durch Komposition mit -1, -1, 1 entsteht, Charaktere der Kurve. Da keiner von diesen drei Charakteren mit dem Charakter für einen Punkt auf der Achse zusammenfällt, so muss der Rang $\geqq 4$ sein. Dasselbe lässt sich für $c=5.29$ beweisen. Indem wir von dem Punkte

$$(9,\ 29,\ 49)\ 29 \tag{34$_1$}$$

ausgehen, kommen wir ja hier zu dem Charakterentripel

$$-1,\ -1,\ 1;\ 1,\ 29,\ 1;\ -1,\ -29,\ 1.$$

Es besteht ein wesentlicher Unterschied zwischen den Fällen $c=5.13$ und $c=5.29$, indem 5 und 13 quadratische Nichtreste, dagegen 5 und 29 quadratische Reste von einander sind. Hierauf beruht es, dass die Charaktere der Kurven nicht aus einander hervorgehen, indem 13 und 29 vertauscht werden. Es bleibt noch übrig zu beweisen, dass der Rang der beiden Kurven auch nicht >4 sein kann. Für $c=5.13$ haben wir in

$$5,\ 1,\ 1;\ 1,\ 5,\ 1;\ 1,\ 1,\ 5$$

ein mit (33) analoges Tripel von Charakteren, welche auf der Kurve keine Repräsentanten haben. Für $c=5.29$ betrachten wir das Tripel

$$1,\ 5,\ 29;\ 5,\ 29,\ 1;\ 29,\ 1,\ 5.$$

Hier bekommen wir jedesmal für c zwei Ausdrücke. Wenn wir diese identifizieren, so ergibt sich bzw. die Relationen

$$u^2+29w^2-2.5v^2=0;\quad 5u^2+w^2-2.29v^2=0;\quad 29u^2+5w^2-2v^2=0. \tag{35}$$

Die linken Glieder sind aber hier keine Nullformen. Keine von den Relationen (35) lässt sich mithin befriedigen, und rationale Punkte mit einem von den drei in Rede stehenden Charakteren gibt es keine auf der Kurve. Aus den vorangehenden Auseinandersetzungen folgt, dass der Rang für $c=5.13$ und $c=5.29$ genau vier ist.

14. Bei der Abfassung von »*Rang von Kurven*» war mir nur eine einzige Kurve (2) vom Range fünf bekannt, und zwar für

$$c = 2.3.5.7.11.13.17. \tag{36}$$

Diese Kurve wurde auch dort besonders zur Behandlung aufgenommen. Ohne Hilfe der hier folgenden Entwicklungen entdeckte ich später drei neue Fälle, nämlich für

$$c = 2.3.7.17.41,\ 2.3.73.97,\ 2.3.97.193. \tag{36_1}$$

Doch bemerkte ich damals nicht, dass der Rang für $c = 2.3.7.17.41$ sogar sechs ist.

Wir nehmen unseren Ausgangspunkt von zwei Quadraten m^2 und n^2 $(n^2 > m^2)$, wo m und n relative Primzahlen bedeuten. Zwei Fälle sind zu unterscheiden. Im ersten Falle ist weder m noch n teilbar durch 3. Man hat dann in arithmetischer Progression

$$m^2,\ \frac{2m^2+n^2}{3},\ \frac{m^2+2n^2}{3},\ n^2. \tag{37}$$

Im zweiten Falle, wo eine von den Zahlen m und n 3 als Faktor hat, ist (37) durch

$$3m^2,\ 2m^2+n^2,\ m^2+2n^2,\ 3n^2. \tag{37_1}$$

zu ersetzen.

In unseren Untersuchungen haben wir einen rationalen Punkt durch die zugehörigen Werte für $x-c$, x und $x+c$ charakterisiert, ohne den Wert für y besonders anzugeben. Hier führen wir nun eine Verkürzung ein, indem wir die gemeinsamen Faktoren der drei Grössen, welche sich ja leicht bestimmen lassen, nicht niederschreiben. So bedeuten z. B. die Bezeichnungen (8, 13, 18) und (117, 121, 125) bei vollständiger Ausführung (8, 13, 18) 13 bzw. (117, 121, 125) $\frac{65}{4}$.

In (37) haben wir eine Zusammenfassung von zwei rationalen Punkten

$$\left(m^2,\ \frac{2m^2+n^2}{3},\ \frac{m^2+2n^2}{3}\right);\ \left(\frac{2m^2+n^2}{3},\ \frac{m^2+2n^2}{3},\ n^2\right), \tag{38}$$

welche zu derselben Kurve gehören. Für diese Kurve ist

$$c \equiv \frac{n^2-m^2}{3}\cdot\frac{2m^2+n^2}{3}\cdot\frac{m^2+2n^2}{3}, \tag{39}$$

wo quadratische Faktoren auszuschalten sind. In gleicher Weise bekommen wir aus (37_1) die Punkte

$$(38_1) \qquad (3m^2,\ 2m^2 + n^2,\ m^2 + 2n^2);\ (2m^2 + n^2,\ m^2 + 2n^2,\ 3n^2).$$

Hier hat man

$$(39_1) \qquad c \equiv 3(n^2 - m^2)(2m^2 + n^2)(m^2 + 2n^2).$$

Ungerade Primzahlen in den Charakteren der Punkte (38) und (38_1) müssen, wie unmittelbar ersichtlich ist, von der Gestalt $8k + 1$ oder $8k + 3$ sein. Doch kann c auch Primfaktoren $8k+5$ und $8k+7$ enthalten, welche dann vom Faktor $n^2 - m^2$ herrühren. Für $m = 1$, $n = 4$ hat man $c = 2.3.5.11$, und die Punkte (38) gehen in

$$(1,\ 6,\ 11);\ (6,\ 11,\ 16)$$

über. Diese Punkte haben in Nr. 2 die Bezeichnungen P_1 und $P_{2,3}$, und es lässt sich offenbar P_2 als Basispunkt der rationalen Punkte der Kurve durch $P_{2,3}$ ersetzen. *Wie in diesem speziellen Falle kann man auch im allgemeinen die Punkte* (38) *und* (38_1) *nebst zwei Punkten auf der Achse, als Basispunkte für die rationalen Punkte betrachten. Wenn c durch* (39) *oder* (39_1) *definiert wird, hat man also einen Rang* $\geqq 4$ *zu erwarten.* Doch gibt es von dieser Regel, wie wir sehen werden, seltene Ausnahmen.

Es lässt sich ohne Schwierigkeit beweisen, dass in (39_1) c mindestens drei Primfaktoren enthält. Übrigens ist mir hier nur ein einziger Fall mit drei Primfaktoren bekannt, nämlich

$$27,\ 43,\ 59,\ 75;\quad c = 3.43.59.$$

Dagegen gibt es in (39) auch eine Möglichkeit von nur zwei Primfaktoren, wie die folgenden Beispiele zeigen.

$$1,\ 9,\ 17,\ 25;\quad c = 2.17.$$
$$25,\ 73,\ 121,\ 169;\quad c = 3.73.$$
$$121,\ 137,\ 153,\ 169;\quad c = 17.137.$$
$$529,\ 673,\ 817,\ 961;\quad c = 673.817.$$

Andere Fälle mit nur mässig grossen Primzahlen scheinen nicht vorzukommen.

Hierbei wurde von dem einfachsten Falle abgesehen:

$$(40) \qquad 1,\ 2,\ 3,\ 4;\quad c = 2.3.$$

Der Rang ist hier bekanntlich nur drei. Der Grund für diese Erniedrigung des Ranges hat man darin, dass von den drei Charakteren 1, 2, 3; 2, 3, 1; 3, 1, 2, welche aus der Folge (40) hervorgehen, der letzte nach (23) auch den Punkt $x = c$ auf der Achse als Repräsentanten hat. Man kann hier nach anderen der-

artigen Fällen vom Range drei fragen. Ein solcher muss offenbar mit einer arithmetischen Progression

$$u^2,\ 2v^2,\ s,\ 4w^2, \tag{41}$$

wo die Differenz = einem Quadrate t^2 ist, verbunden sein. Man hat dann $c \equiv 2s$. Hier findet man sofort die Bedingungen

$$u^2 + t^2 = 2v^2;\quad v^2 + t^2 = 2w^2. \tag{42}$$

Durch (42) wird eine Raumkurve vierter Ordnung vom Geschlechte eins bestimmt, und die Lösungen unseres Problems sind mit den rationalen Punkten dieser Kurve verbunden. Nun kennen wir bereits den rationalen Punkt 1, 1, 1, 1, und aus diesem Punkte lassen sich andere herleiten. Zunächst suchen wir den vierten Schnittpunkt mit der Schmiegungsebene. Für diese Ebene finden wir die Gleichung

$$u - 6v + 8w - 3t = 0. \tag{43}$$

Mit Hilfe von (42) und (43) lassen sich zwei von den Veränderlichen eliminieren, und man bekommt zwischen den beiden übrigen eine Gleichung vierten Grades, wobei, da man bereits drei Wurzeln 1 : 1 kennt, es nur nötig ist das erste und das letzte Glied zu berechnen. Für den vierten Schnittpunkt findet man so

$$u = 23,\ v = -17,\ w = -13,\ t = 7.$$

Als Resultat findet man mithin

$$529,\ 578,\ 627,\ 676;\quad c = 2.3.11.19. \tag{44}$$

Die erhaltene Kurve ist aber vom Range fünf und also keine Lösung unserer Aufgabe. Doch erhält man ein System rationaler Punkte vom Range drei, wenn man als Basispunkte nur Punkte auf der Achse und durch (44) definierte Punkte benutzt. Die Berechnung anderer rationaler Punkte der Kurve (42) scheint einen ziemlich grossen Aufwand von Rechnungen zu erfordern.

15. Wenn man Kurven vom Range fünf aufzusuchen wünscht, so ist es natürlich vorteilhaft von einem Kurvensystem ausgehen zu können, für welches man bereits weiss, dass der Rang wenigstens vier ist. Es gilt ja dann nur die Bestimmung eines einzigen neuen Basispunktes, der von den schon bekannten unabhängig ist. Wir wollen dies zunächst durch das Beispiel

$$16,\ 51,\ 86,\ 121;\quad c = 2.3.5.7.17.43 \tag{45}$$

beleuchten. Wie unmittelbar ersichtlich ist, liegt auf derselben Kurve noch der Punkt

(46) $\qquad (84, 85, 86).$

Wir kennen also drei Punkte:

$$(16, 51, 86); \quad (51, 86, 121); \quad (84, 85, 86).$$

Die zugehörigen Charaktere sind

(47) $\qquad 1, \ 3.17, \ 2.43; \quad 3.17, \ 2.43, \ 1; \quad 3.7, \ 5.17, \ 2.43.$

Durch Komposition findet man hieraus noch die folgenden Charaktere

$$2.43, \ 1, \ 3.17; \quad 7, \ 5, \ 3; \quad 2.7.43, \ 5, \ 17; \quad 7.17, \ 2.3.5.43, \ 1.$$

Da also die drei Charaktere (47) von einander und von den Charakteren (23) unabhängig sind, so ist der Rang wenigstens fünf.

In völlig analoger Weise verhält es sich mit dem folgenden Beispiel.

(45_1) $\qquad 289, \ 513, \ 737, \ 961; \quad c = 2.3.7.11.19.67.$

Zu diesem c-Werte gehört noch der Punkt

(46_1) $\qquad (132, 133, 134).$

Als Charaktere der drei Punkte

$$(289, 513, 737); \quad (513, 737, 961); \quad (132, 133, 134)$$

hat man

(47_1) $\qquad 1, \ 3.19, \ 11.67; \quad 3.19, \ 11.67, \ 1; \quad 3.11, \ 7.19, \ 2.67.$

Durch Komposition bekommt man hieraus

$$11.67, \ 1, \ 3.19; \quad 1, \ 7.11, \ 2.3; \quad 67, \ 7, \ 2.11.19; \quad 19, \ 3.7.67, \ 2.$$

Wie im vorigen Beispiel sieht man, dass der Rang $\geqq 5$ sein muss.

Insbesondere wird der Rang erhöht, wenn mehr als eine Folge (37) oder (37_1) zu derselben Kurve führt. Hier haben wir als einfaches Beispiel

(48) $\qquad c = 2.3.11.19.$

Es gibt sogar vier Folgen, von denen man zu dieser Kurve gelangt. Diese wollen wir hier zusammenstellen, wobei die drei durch eine Folge definierten Charaktere zu ihr hinzugefügt werden.

(49) 16, 19, 22, 25; 1, 19, 2.11; 19, 2.11, 1; 2.11, 1, 19.

(49_1) 16, 27, 38, 49; 1, 3, 2.19; 3, 2.19, 1; 2.19, 1, 3.

(49_2) 3, 11, 19, 27; 3, 11, 19; 11, 19, 3; 19, 3, 11.

(49_3) 529, 578, 627, 676; 1, 2, 3.11.19; 2, 3.11.19, 1; 3.11.19, 1, 2.

Wir finden, dass für kein Paar von diesen Charakterentripeln ein gemeinsames Element existiert. Hieraus folgt, dass die beiden durch die zugehörigen Folgen definierten Punktpaare Basispunkte für ein System rationaler Punkte vom Range vier sind. Da hierzu noch die rationalen Punkte hinzukommen, bei denen das Zeichen — in den Charakteren auftritt, so muss der Rang fünf sein. Für diesen Schluss ist also nur die Kenntnis von zwei beliebigen der obigen vier Folgen nötig. Aus den übrigen Charakteren mit lauter Zeichen + erhält man, wenn vom Einheitscharakter abgesehen wird, ein mit den obigen völlig analoges Tripel

1, 11, 2.3; 11, 2.3, 1; 2.3, 1, 11.

Doch existiert, so viel ich weiss, keine Folge von vier Zahlen in arithmetischer Progression, von welcher man zu diesem Tripel kommt.

Für acht von den hier oben gegebenen Charakteren erhält man unmittelbar Repräsentanten durch die vier Folgen. Wir vervollständigen dies, indem wir hier noch repräsentierende Punkte für die sechs übrigen angeben[1].

(22, 49, 76); 2.11, 1, 19.
(950, 961, 972); 2.19, 1, 3.
(19, 147, 275); 19, 3, 11.
(256, 275, 294); 1, 11, 2.3.
(11, 486, 961); 11, 2.3, 1.
(6, 25, 44); 2.3, 1, 11.

Die Kurve (48) *ist nur das erste Glied einer Schar von Kurven des Ranges fünf.* Der Zusammenhang zwischen den Folgen (49) und (49_1) ist evident. Für (49) lässt sich mit $u = 4$, $v = 5$ schreiben

$$u^2, \frac{2u^2 + v^2}{3}, \frac{u^2 + 2v^2}{3}, v^2.$$

[1] Für 3, 11, 19, 1, 2 hat man bekanntlich einen Repräsentanten im Punkte $x = c$.

In (49_1) ist dann das dritte Glied $\frac{4u^2 + 2v^2}{3}$ und die Differenz $\frac{u^2 + 2v^2}{6}$. Die Folge (49_1) erhält also die Gestalt

$$u^2, \frac{7u^2 + 2v^2}{6}, \frac{4u^2 + 2v^2}{3}, \frac{3u^2 + 2v^2}{2}.$$

Nun sind in (49_1) noch die Bedingungen

$$(50) \qquad 7u^2 + 2v^2 = 18w^2; \quad 3u^2 + 2v^2 = 2t^2$$

befriedigt. Durch (50) lässt sich eine Raumkurve 4. Ordnung vom Geschlechte eins definieren. Auf dieser Kurve sind erstens die in der Ebene $u = 0$ liegenden Punkte rational; für diese Punkte sind die Schmiegungsebenen stationär. Daneben kennen wir den rationalen Punkt $u = 4$, $v = 5$, $w = 3$, $t = 7$, und durch Zeichenänderungen erhält man hieraus sieben andere rationale Punkte. Indem man von diesen Punkten ausgeht, lässt sich die Bestimmung von rationalen Punkten fortsetzen; dabei benutzt man entweder die Schmiegungsebenen oder Ebenen, welche in einem Punkte berühren und durch einen anderen hindurchgehen. Es lässt sich nicht bezweifeln, dass man in solcher Weise eine unbegrenzte Anzahl von rationalen Punkten erhält. Jeder solchen Lösung u^2, v^2, w^2, t^2 lässt sich nun eine Kurve (2) vom Range fünf zuordnen. Auf einen anderen mässigen c-Wert als (48) scheint man dabei nicht zu stossen.

16. Wir werden jetzt zu einem neuen unendlichen System von Kurven des Ranges vier übergehen, das mit dem vorangehenden die Eigenschaft teilt, dass jedem Paare von relativen Primzahlen eine Kurve zugeordnet wird. Wir nehmen hier m^2 und n^2 mit verschiedenen Zeichen und schreiben so die Folge

$$(51) \qquad -3m^2, \; -2m^2 + n^2, \; -m^2 + 2n^2, \; 3n^2.$$

Da eine Änderung der Zeichen keine Bedeutung hat, so können wir $n^2 > m^2$ annehmen. Es sind zwei Fälle zu unterscheiden. Im ersten Falle hat man $n^2 < 2m^2$. Die beiden durch die Folge definierten Punkte schreiben sich dann

$$(52) \quad (-3m^2, \; -(2m^2 - n^2), \; 2n^2 - m^2); \quad (-3n^2, \; -(2n^2 - m^2), \; 2m^2 - n^2).$$

Im anderen Falle ist $n^2 > 2m^2$, und wir bekommen aus der Folge die Punkte

$$(52_1) \qquad (-(2n^2 - m^2), \; -(n^2 - 2m^2), \; 3m^2); \quad (n^2 - 2m^2, \; 2n^2 - m^2, \; 3n^2).$$

Für c erhalten wir den Ausdruck

$$c \equiv \pm 3(m^2+n^2)(2m^2-n^2)(2n^2-m^2), \tag{53}$$

wo das obere Zeichen für (52) und das untere für (52_1) gilt. Unter den Primfaktoren von c befinden sich hier immer 2 und 3. Der Faktor 2 rührt von m^2+n^2, $2m^2-n^2$ oder $2n^2-m^2$ her, je nachdem m und n beide ungerade, m ungerade und n gerade oder m gerade und n ungerade ist. Wenn von 3 abgesehen wird, gibt es hier keine Primfaktoren $8k+3$ von c; Primfaktoren $8k+5$ können nicht in den Charakteren der Punkte (52) und (52_1), aber wohl in der Differenz m^2+n^2 auftreten. Bei Komposition der Charaktere für die Punkte (52) und (52_1) erhält man bzw.:

$$(2m^2-n^2)(2n^2-m^2),\ 1,\ 1;\quad -1,\ -1,\ (n^2-2m^2)(2n^2-m^2).$$

Etwa in $2m^2-n^2$ und $2n^2-m^2$ auftretende quadratische Faktoren sollen dabei wegfallen.

Für $m=n=1$ erhalten wir die Folge

$$-3,\ -1,\ 1,\ 3;\quad c=2.3.$$

Nur in diesem Falle, der uns bereits wohlbekannt ist, bekommen wir hier einen Rang <4. Als zweites Beispiel nehmen vier

$$-3,\ 2,\ 7,\ 12;\quad c=2.3.5.7.$$

Die erhaltene Kurve wird ausführlich in »*Rang von Kurven*» behandelt. Nur zwei Folgen (51) kenne ich, für welche c ein Produkt von drei Primfaktoren ist:

$$-27,\ -2,\ 23,\ 48;\quad c=2.3.23.$$
$$-147,\ 191,\ 529,\ 867;\quad c=2.3.191.$$

17. Wir haben jetzt grössere Möglichkeiten Kurven vom Range fünf zu entdecken. Als erstes Beispiel nehmen wir

$$c=2.3.7.17.31. \tag{54}$$

Es gibt zwei Folgen, welche zu diesem c-Wert führen, nämlich

$$25,\ 242,\ 459,\ 676;$$
$$-3,\ 14,\ 31,\ 48.$$

Durch diese Folgen werden unmittelbar drei Punkte mit positiven Charakteren bestimmt:

$$(25,\ 242,\ 459);\quad (242,\ 459,\ 676);\quad (14,\ 31,\ 48).$$

Die zugehörigen Charaktere sind

$$1,\ 2,\ 3.17;\quad 2,\ 3.17,\ 1;\quad 2.7,\ 31,\ 3.$$

Durch Komposition erhält man hieraus, ausser dem Einheitscharakter, noch die folgenden Charaktere

$$3.17,\ 1,\ 2;\quad 7,\ 31,\ 2.17;\quad 3.7,\ 17.31,\ 1;\quad 7.17,\ 2.3.31,\ 1.$$

Da keiner von diesen Charakteren mit einem Charakter (23) übereinstimmt, so muss der Rang wenigstens fünf sein. Für den Punkt $(-31, -14, 3)$ ist der Charakter $-31, -2.7, 3$. Da man durch Komposition von $7, 31, 2.17$ mit $-31, -2.7, 3$ auf $-2, -1, 3.7.17.31$, also einen Charakter (23) kommt, so lässt sich auch auf einen höheren Rang als fünf nicht schliessen.

Hierzu fügen wir noch zwei Beispiele, welche sich in völlig gleichartiger Weise behandeln lassen. Doch tritt der Unterschied ein, dass diese neuen Fälle als erste Glieder in zwei Kurvenscharen vom Range fünf auftreten. In dem einen Falle ist

$$c = 2.3.73.97. \tag{55}$$

Zu diesem c-Wert gehören die Folgen

$$49,\ 73,\ 97,\ 121; \tag{56}$$

$$-48,\ 49,\ 146,\ 243. \tag{56_1}$$

Wir erhalten also die rationalen Punkte

$$(49,\ 73,\ 97);\ (73,\ 97,\ 121);\ (49,\ 146,\ 243)$$

mit den Charakteren

$$1,\ 73,\ 97;\ 73,\ 97,\ 1;\ 1,\ 2.73,\ 3.$$

Durch Komposition bekommen wir noch die Charaktere

$$97,\ 1,\ 73;\ 1,\ 2,\ 3.97;\ 1,\ 2.97,\ 3.73;\ 73.97,\ 2,\ 3.$$

Der Schluss, dass der Rang fünf ist, lässt sich jetzt in derselben Weise wie für die Kurve (54) ziehen.

Auch im noch übrigen Falle

$$c = 2.3.97.193 \tag{57}$$

gilt dieselbe Schlussweise. Die Folgen sind hier

$$1,\ 97,\ 193,\ 289; \tag{58}$$

$$-192,\ 97,\ 386,\ 675. \tag{58_1}$$

Wir haben also die rationalen Punkte

$$(1, 97, 193); \quad (97, 193, 289); \quad (97, 386, 675)$$

mit den Charakteren

$$1, 97, 193; \quad 97, 193, 1; \quad 97, 2.193, 3$$

und den aus diesen abgeleiteten Charakteren

$$193, 1, 97; \quad 193, 2, 3.97; \quad 1, 2, 3; \quad 1, 2.97, 3.193.$$

Von hier aus beweist man, wie in den beiden vorhergehenden Fällen, dass der Rang fünf ist.

Die drei Kurven

$$c = 2.3.11.19, \quad 2.3.73.97, \quad 2.3.97.193$$

stimmen darin überein, dass sie Anfangsglieder von Kurvenscharen des Ranges fünf sind. Man überzeugt sich leicht, dass dies nicht ohne Zusammenhang mit dem Umstande ist, dass in allen drei Fällen c ausser den Primzahlen 2 und 3 nur noch zwei Primfaktoren enthält. Es ist (56) ein Spezialfall der Folge

$$u^2, \; u^2 + 24v^2, \; u^2 + 48v^2, \; u^2 + 72v^2.$$

Für (56_1) schreibt sich dann das dritte Glied $= 2(u^2 + 24v^2)$ und die Differenz $= u^2 + 48v^2$. Man bekommt mithin für (56_1) die Gestalt

$$-48v^2, \; u^2, \; 2(u^2 + 24v^2), \; 3(u^2 + 32v^2).$$

Nun kommen noch die Bedingungen für die letzten Glieder hinzu. Für diese haben wir die Ausdrücke

$$(59) \qquad u^2 + 72v^2 = w^2; \quad u^2 + 32v^2 = t^2.$$

Durch (59) wird eine Raumkurve 4. Ordnung vom Geschlechte eins bestimmt. Auf dieser Kurve kennen wir die rationalen Punkte

$$v = 0, \; u = w = t = 1; \quad u = 7, \; v = 1, \; w = 11, \; t = 9,$$

sowie diejenigen, welche man hieraus durch Zeichenänderungen erhält. Mit diesen Punkten als Basispunkten kommt man nach bekannten Methoden zu neuen rationalen Punkten. Für jede Lösung u^2, v^2, w^2, t^2 bekommen wir eine Kurve vom Range fünf.

Auch (58) ist ein Spezialfall der Folge

$$u^2,\ u^2 + 24v^2,\ u^2 + 48v^2,\ u^2 + 72v^2.$$

In (58_1) bekommt man für das zweite Glied $u^2 + 24v^2$ und für das dritte $2(u^2 + 48v^2)$. Für (58_1) erhalten wir hiernach den Ausdruck

$$-48v^2,\ u^2 + 24v^2,\ 2(u^2 + 48v^2),\ 3(u^2 + 56v^2).$$

Hier müssen die letzten Glieder noch die Bedingungen

$$u^2 + 72v^2 = w^2;\quad u^2 + 56v^2 = t^2 \tag{60}$$

befriedigen. Die Kurve 4. Ordnung vom Geschlechte eins, die durch (60) definiert wird, besitzt nun die rationalen Punkte

$$v = 0,\ u = w = t = 1;\quad u = 1,\ v = 2,\ w = 17,\ t = 11$$

sowie die hieraus durch Zeichenänderungen hervorgehenden. Den rationalen Punkten, zu denen man von diesen Punkten als Basispunkten gelangt, sind in derselben Weise wie im vorhergehenden Falle neue Kurven vom Range fünf zugeordnet. Man kann aber nicht sagen, dass die Kurven dieser Systeme vom Range fünf, wenn von den Anfangskurven abgesehen wird, besonders zugänglich sind.

18. Ganz anders verhält es sich in letzterer Hinsicht mit der Schar von Kurven des Ranges fünf, welche wir in dieser Nummer behandeln werden. Meine Aufmerksamkeit auf diese Schar wurde durch die Entdeckung von zwei ihr zugehörigen Kurven gerichtet. Auf eine von diesen Kurven mit

$$c = 2.3.7.17.97.313 \tag{61}$$

führen die Folgen

$$-75,\ 119,\ 313,\ 507; \tag{62}$$

$$-432,\ -119,\ 194,\ 507. \tag{62_1}$$

Für die andere hat man

$$c = 2.3.7.23.257.353, \tag{63}$$

und die entsprechenden Folgen sind

$$-675,\ -161,\ 353,\ 867; \tag{64}$$

$$-192,\ 161,\ 514,\ 867. \tag{64_1}$$

In den beiden Paaren (62), (62_1) und (64), (64_1) ist das letzte Glied gemeinsam, und die Summe der Beträge der ersten Glieder ist gleich dem letzten Glied. Der Zusammenhang mit den Pythagoreischen Relationen

$$25 + 144 = 169; \quad 225 + 64 = 289$$

ist evident, und man erschliesst hieraus unmittelbar ein allgemeines Gesetz.

Sind m und n relative Primzahlen, wobei man etwa m ungerade und n gerade annimmt, so bekommt man allgemein als erste bzw. zweite Folge:

$$(65) \qquad -3(m^2-n^2)^2,\ -(m^4+n^4-6m^2n^2),\ m^4+n^4+6m^2n^2,\ 3(m^2+n^2)^2;$$

$$(65_1) \qquad -12m^2n^2,\ m^4+n^4-6m^2n^2,\ 2(m^4+n^4),\ 3(m^2+n^2)^2.$$

Die Differenz ist in der ersten Folge $2(m^4+n^4)$ und in der zweiten $m^4+n^4+6m^2n^2$. Wir erhalten hieraus

$$(66) \qquad c \equiv \pm 2.3(m^4+n^4-6m^2n^2)(m^4+n^4)(m^4+n^4+6m^2n^2).$$

Es gibt noch eine dritte Folge, welche auf dieselbe Kurve führt, nämlich

$$(65_2) \qquad 12m^2n^2,\ m^4+n^4+6m^2n^2,\ 2(m^4+n^4),\ 3(m^2-n^2)^2.$$

Die Differenz ist hier $m^4+n^4-6m^2n^2$.

Unter den Faktoren von c in (66) befinden sich immer 2 und 3. Sonst hat c keine Primfaktoren $8k+3$ und überhaupt keine Primfaktoren $8k+5$. Der Faktor m^4+n^4 kann nur Primfaktoren $16k+1$, $m^4+n^4+6m^2n^2$ Primfaktoren $8k+1$ und $m^4+n^4-6m^2n^2$ Primfaktoren $8k\pm1$ enthalten. Wir erinnern hier an die in »*Rang von Kurven*» behandelte Kurve vom Range fünf mit

$$c = 2.3.5.7.11.13.17,$$

wo c also ein Produkt der sieben ersten Primzahlen darstellt. Derartige Fälle, wo keine Reste (mod 8) bevorzugt erscheinen, sind hier nicht zu erwarten.

Bei dem jetzt folgenden Beweise, dass der Rang fünf ist oder grösser, benutzen wir die in Nr. 6 gegebenen Verkürzungen $g(m,n)$, $h(m,n)$ und $h_1(m,n)$ für $m^4+n^4-6m^2n^2$, $m^4+n^4+6m^2n^2$ und $2(m^4+n^4)$. Wie leicht zu sehen ist, haben nie zwei von den Zahlen, die von diesen Grössen gebildet werden, gemeinsame Faktoren; es gibt auch unter diesen Zahlen keine Quadrate. Mit g, h und h_1 bezeichnen wir das Produkt der Primzahlen, die bzw. in $\pm g(m,n)$, $h(m,n)$ und $h_1(m,n)$ als Faktoren in ungerader Potenz auftreten.

Zunächst nehmen wir an, es sei $m^4+n^4>6m^2n^2$. Wir erhalten dann folgende Charaktere.

Aus der Folge (65): $-3, -g, h;\ -3, -h, g;\ g.h,\ 1,\ 1.$

Aus der Folge (65_1): $-h_1, -g, 3;\ g, h_1, 3;\ -1, -1, g.h_1.$

Aus der Folge (65_2): $3, h, h_1;\ h, h_1, 3;\ h_1, 3, h.$

Wie man sieht, sind je zwei von diesen Charakterentripeln von einander unabhängig. Dagegen lässt sich jedes Tripel aus den beiden anderen herleiten. So z. B. ist $3, h, h_1$ das Produkt von $-3, -h, g$ und $-1, -1, g.h_1$; $h, h_1, 3$ das Produkt von $g.h, 1, 1$ und $g, h_1, 3$; $h_1, 3, h$ das Produkt von $-3, -g, h$ und $-h_1, -g, 3$. Wir brauchen uns also weiter nur mit den zwei ersten Tripeln zu beschäftigen. Aus diesen Tripeln lässt sich ein System vom Range vier erzeugen. Die Frage ist nun, wie dieses System sich zu dem Tripel (23) verhält. In dieser Hinsicht finden wir, dass ein Element von (23) zu dem System gehört, indem $-1, -3\,g.h.h_1, 1$ das Produkt von $-3, h, g$ und $g, h_1, 3$ darstellt. Dagegen kommt man nicht zu den beiden übrigen Elementen von (23). Hierauf beruht der Schluss auf einen Rang $\geqq 5$.

Auf den jetzt behandelten Fall lässt sich der Fall mit $m^4+n^4<6m^2n^2$ zurückführen. Der Übergang zwischen den beiden Fällen involviert eine Vertauschung von h und h_1 in den Charakteren. Dazu kommt, dass die zu (65) und (65_1) gehörenden Tripel Platz wechseln.

19. Setzt man für die in der vorhergehenden Nummer behandelte Schar vom Range fünf $m=1$, $n=2$, so bekommt man

$$c=2.3.7.17.41. \tag{67}$$

Für dieses erste Glied der Schar ist der Rang sechs. Dass hier eine Erhöhung des Ranges eintritt, steht im Zusammenhange damit, dass man durch fünf Folgen auf die Kurve (67) geführt wird. Diese Folgen werden hier gegeben. Dabei schreiben wir neben jede Folge die drei Charaktere, welche sich unmittelbar aus ihr ableiten lassen.

(68) $\quad -27, 7, 41, 75.\ -41, -7, 3;\ 7, 41, 3;\ -1, -1, 7.41.$

(68_1) $\quad -48, -7, 34, 75.\ -3, -7, 2.17;\ -3, -2.17, 7;\ 2.7.17, 1, 1.$

(68_2) $\quad 27, 34, 41, 48.\ 3, 2.17, 41;\ 2.17, 41, 3;\ 41, 3, 2.17.$

(68_3) $\quad 4, 123, 242, 361.\ 1, 3.41, 2;\ 3.41, 2, 1;\ 2, 1, 3.41.$

(68_4) $\quad -507, -82, 343, 768.\ -3, -2.41, 7;\ -3, -7, 2.41;\ 2.7.41, 1, 1.$

Wie man sieht, haben zwei beliebige von diesen fünf Tripeln kein gemeinsames Element; durch Komposition erhält man also aus denselben ein System vom Range vier. Geht man von (68) und (68_3) aus, so kommt in den Charakteren dieses Systems die Primzahl 17 nicht vor. Das System ist also unabhängig von den Tripeln (68_1) und (68_2). Wenn man also weiter mit einem von diesen Tripeln kombiniert, so wird der Rang sechs erreicht. Dasselbe Resultat erhält man übrigens auch durch Komposition mit dem Tripel (23).

Auf der Kurve (67) gibt es mithin 64 Klassen von rationalen Punkten. Für jede von diesen Klassen wollen wir hier einen Repräsentanten angeben. Von vornherein haben wir in den drei Punkten auf der Achse und dem unendlich entfernten Punkt Repräsentanten von vier Klassen, der Einheitsklasse und den Klassen mit den Charakteren (23). Wir fangen an, indem wir für diese vier Klassen die Charaktere aufschreiben.

(Q) $\quad 1,\ 1,\ 1;\ 3.7.17.41,\ 1,\ 2;\ -1,\ -2.3.7.17.41,\ 1;\ -2,\ -1,\ 3.7.17.41.$

Die übrigen Klassen nehmen wir vier und vier zusammen, indem wir zu jeder Klasse diejenigen hinzufügen, welche durch Komposition mit dem obigen Quadrupel entstehen. Die Klassen werden also nach der Faktorgruppe in Bezug auf die Untergruppe der obigen vier Klassen geordnet. Wir indizieren die Klassenquadrupel in solcher Weise, dass man daraus versteht, wie die Elemente der oben besprochenen Faktorgruppe sich mit einander komponieren. Für jedes Quadrupel geben wir zuerst die Charaktere und dann die zugehörigen Repräsentanten. Die Darstellung ist derjenigen ganz ähnlich, die wir in »Rang von Kurven», S. 234 für $c = 2.3.5.7.11.13.17$ ausgeführt haben. Die gemeinsamen Faktoren für $x - c$, x und $x + c$ werden hier in Primfaktoren aufgelöst.

(Q_1) $\quad 7,\ 2.3,\ 41;\ 2.17,\ 41,\ 3;\ -41,\ -17,\ 7;\ -3,\ -7,\ 2.17.$
$(7,\ 24,\ 41)\ 2.3.7.41;\ (34,\ 41,\ 48)\ 2.3.17.41;\ (-41,\ -17,\ 7)\ \frac{7.17.41}{2^2};$
$(-48,\ -7,\ 34)\ 2.3.7.17.$

(Q_2) $\quad 3,\ 2.17,\ 41;\ 2.7,\ 41,\ 17;\ -41,\ -7,\ 3;\ -17,\ -3,\ 2.7.$
$(27,\ 34,\ 41)\ 2.3.17.41;\ (14,\ 41,\ 68)\ \frac{2.7.17.41}{3^2};\ (-41,\ -7,\ 27)\ 3.7.41;$
$(-68,\ -27,\ 14)\ 2.3.7.17.$

$(Q_{1,2})$ $\quad 7,\ 17,\ 3;\ 41,\ 3,\ 2.17;\ -3,\ -2.41,\ 7;\ -2.17,\ -7,\ 41.$
$(343,\ 425,\ 507)\ 3.7.17;\ (164,\ 507,\ 850)\ \frac{2.3.17.41}{7^2};$
$(-507,\ -82,\ 343)\ \frac{2.3.7.41}{5^2};\ (-850,\ -343,\ 164)\ \frac{2.7.17.41}{13^2}.$

(Q_3) $7, 41, 3;\ 17, 3, 2.41;\ -3, -2.17, 7;\ -2.41, -7, 17.$
$(7, 41, 75)\ 3.7.41;\ (68, 75, 82)\ 2.3.17.41;\ (-75, -34, 7)\ 2.3.7.17;$
$(-82, -7, 68)\ \frac{2.7.17.41}{5^2}.$

$(Q_{1,3})$ $3.41, 2, 1;\ 2.7.17, 1, 1;\ -1, -7.17, 3.41;\ -1, -3.41, 2.7.17.$
$(123, 242, 361)\ 2.3.41;\ (238, 361, 484)\ 2.7.17;$
$(-361, -119, 123)\ \frac{3.7.17.41}{11^2};\ (-484, -123, 238)\ \frac{2.3.7.17.41}{19^2}.$

$(Q_{2,3})$ $7.41, 2.3.17, 1;\ 2, 1, 3.17;\ -1, -1, 7.41;\ -3.17, -7.41, 2.$
$(287, 408, 529)\ \frac{2.3.7.17.41}{11^2};\ (242, 529, 816)\ 2.3.17;$
$(-529, -121, 287)\ \frac{7.41}{2^2};\ (-816, -287, 242)\ \frac{2.3.7.17.41}{23^2}.$

$(Q_{1,2,3})$ $1, 17.41, 1;\ 3.7, 1, 2.17.41;\ -1, -2.3.7, 1;\ -2.17.41, -1, 3.7.$
$(25, 697, 1369)\ \frac{17.41}{4^2};\ (1344, 1369, 1394)\ \frac{2.3.7.17.41}{5^2};$
$(-1369, -672, 25)\ 2.3.7;\ (-1394, -25, 1344)\ \frac{2.3.7.17.41}{37^2}.$

(Q_4) $7.17, 1, 3.41;\ 1, 3.41, 2;\ -3.41, -2, 7.17;\ -2, -7.17, 1.$
$(119, 121, 123)\ 3.7.17.41;\ (4, 123, 242)\ 2.3.41;$
$(-123, -2, 119)\ \frac{2.3.7.17.41}{11^2};\ (-242, -119, 4)\ 2.7.17.$

$(Q_{1,4})$ $3.17, 2, 1;\ 2.7.41, 1, 1;\ -1, -7.41, 3.17;\ -1, -3.17, 2.7.41.$
$(51, 338, 625)\ 2.3.17;\ (574, 625, 676)\ 2.7.41;$
$(-625, -287, 51)\ \frac{3.7.17.41}{13^2};\ (-676, -51, 574)\ \frac{2.3.7.17.41}{25^2}.$

$(Q_{2,4})$ $7, 2.3, 17;\ 2.41, 17, 3;\ -17, -41, 7;\ -3, -7, 2.41.$
$(343, 384, 425)\ 2.3.7.17;\ (82, 425, 768)\ \frac{2.3.17.41}{7^2};$
$(-425, -41, 343)\ \frac{7.17.41}{9^2};\ (-768, -343, 82)\ \frac{2.3.7.41}{5^2}.$

$(Q_{1,2,4})$ $1, 1, 17.41;\ 3.7, 17.41, 2;\ -17.41, -2.3.7, 1;\ -2, -1, 3.7.$
$(361, 529, 697)\ \frac{17.41}{2^2};\ (336, 697, 1058)\ \frac{2.3.7.17.41}{19^2};$
$(-697, -168, 361)\ \frac{2.3.7.17.41}{23^2};\ (-1058, -361, 336)\ 2.3.7.$

$(Q_{3,4})$ $17.41, 1, 1;\ 3.7, 1, 2;\ -1, -2.3.7, 17.41;\ -2, -17.41, 3.7.$
$(697, 2209, 3721)\ \frac{17.41}{6^2};\ (3024, 3721, 4418)\ 2.3.7;$
$(-3721, -1512, 697)\ \frac{2.3.7.17.41}{47^2};\ (-4418, -697, 3024)\ \frac{2.3.7.17.41}{61^2}.$

$(Q_{1,3,4})$ $7.17, 2.3.41, 1;\ 2, 1, 3.41;\ -1, -1, 7.17;\ -3.41, -7.17, 2.$
$(5831, 8856, 11881)\ \frac{2.3.7.17.41}{55^2};\ (6050, 11881, 17712)\ \frac{2.3.41}{7^2};$
$(-11881, -3025, 5831)\ \frac{7.17}{6^2};\ (-17712, -5831, 6050)\ \frac{2.3.7.17.41}{109^2}.$

$(Q_{2,3,4})$ $3,\ 2.41,\ 17;\ 2.7,\ 17{,}41;\ -17,\ -7,\ 3;\ -41,\ -3,\ 2.7.$

$(5547,\ 9922,\ 14297)\ \frac{2.3.17.41}{25^2};\ (8750,\ 14297,\ 19844)\ \frac{2.7.17.41}{43^2};$

$(-14297,\ -4375,\ 5547)\ \frac{3.7.17}{11^2};\ (-19844,\ -5547,\ 8750)\ \frac{2.3\,7.41}{29^2}.$

$(Q_{1,2,3,4})$ $7.41,\ 1,\ 3.17;\ 1,\ 3.17,\ 2;\ -3.17,\ -2,\ 7.41;\ -2,\ -7.41,\ 1.$

$(287,\ 2209,\ 4131)\ \frac{3.7.17.41}{31^2};\ (3844,\ 4131,\ 4418)\ 2.3.17;$

$(-4131,\ 1922,\ 287)\ \frac{2.3.7.17.41}{47^2};\ (-4418,\ -287,\ 3844)\ \frac{2.7.41}{9^2}.$

Wir haben hier oben eine Anordnung der Charaktere der 64 Klassen in 16 Zeilen und vier Kolonnen. Auch die vier Kolonnen sind Elemente einer Faktorgruppe. In den Charakteren der ersten und zweiten Kolonne kommt das Zeichen — nicht vor, und die Primzahl 2 tritt in der ersten und dritten Kolonne entweder nicht oder nur an der mittleren Stelle auf. Die erste Kolonne hat also die Eigenschaften einer Untergruppe, und die übrigen Kolonnen sind Elemente in der zugehörigen Faktorgruppe. Hieraus folgt, dass auch die Kolonnen sich indizieren lassen. Man gibt etwa der zweiten Kolonne den Index 5, der dritten den Index 6, und der vierten die Indizes 5, 6. Einem einzelnen Charakter gibt man jetzt die Indizes der Zeile und der Kolonne, welche sich in ihm kreuzen, und hierdurch werden die Kompositionseigenschaften der Charaktere völlig klargelegt.

Vom Range sechs ist mir keine andere Kurve (2) als (67) bekannt und vom Range fünf, ausser den bereits besprochenen Fällen, nur die einzige Kurve

(69) $$c = 2.3.11.17.41.43.$$

Zu diesem Falle führen die Folgen:

(70) $1369,\ 1394,\ 1419,\ 1444;\ 1,\ 2.17.41,\ 3.11.43;\ 2.17.41,\ 3.11.43,\ 1;$
$3.11.43,\ 1,\ 2.17.41.$

(70_1) $25,\ 722,\ 1419,\ 2116;\ 1,\ 2,\ 3.11.43;\ 2,\ 3.11.43,\ 1;\ 3.11.43,\ 1,\ 2.$

Da die zugehörigen Charakterentripel kein gemeinsames Element besitzen, so bekommt man aus (70) und (70_1) die Basispunkte für ein System rationaler Punkte vom Range vier. Da hierzu noch rationale Punkte hinzukommen, für welche das Zeichen — in den Charakteren auftritt, so muss der Rang der Kurve mindestens fünf sein.