

## ZUR APPROXIMATION ALGEBRAISCHER ZAHLEN. III.

(Über die mittlere Anzahl der Darstellungen grosser Zahlen  
durch binäre Formen.)

VON

KURT MAHLER

in KREFELD.

Im Sommer 1925 teilte mir Herr Prof. C. Siegel einen bisher unveröffentlichten Beweis des folgenden Satzes mit:

»Sei  $F(x, y)$  eine irreduzible Binärform mit ganzen rationalen Koeffizienten vom Grad  $n \geq 3$ . Dann konvergiert die Dirichletsche Reihe

$$Z(s) = \sum_{\substack{p=-\infty \\ p^2+q^2 \neq 0}}^{\infty} \sum_{q=-\infty}^{\infty} |F(p, q)|^{-s} \quad (s = \sigma_0 + ti)$$

für  $\sigma_0 > 2/n$ ; die durch sie dargestellte Funktion  $Z(s)$  lässt sich in die ganze Halbebene  $\sigma_0 > 1/n - 1$  fortsetzen und ist hier überall regulär, bis auf einen einfachen

Pol bei  $s = 2/n$  mit dem Residuum  $\frac{2}{n} \int_{-\infty}^{+\infty} |F(x, 1)|^{-2/n} dx$ .»

Der Beweis machte, abgesehen von elementaren Abschätzungen und von der Eulerschen Summenformel, in wesentlicher Weise Gebrauch vom Thueschen Satz über die Approximation algebraischer Zahlen durch rationale. Dass man vom Thueschen Satz Gebrauch machen muss, ist fast selbstverständlich; denn bereits die Tatsache, dass  $Z(s)$  überhaupt eine Konvergenzhalbebene besitzt, besagt mehr, als dass  $F(x, y)$  jede ganze Zahl nur endlich oft darstellt.

Es gelang mir später, den Siegelschen Beweis durch Hinzunahme von Kettenbruchbetrachtungen so abzuändern, dass er zu folgender schärferen Aussage führte:

»Ist  $A(k)$  die Anzahl der Paare ganzer rationaler Zahlen  $p, q$ , die der Ungleichung

$$|F(p, q)| \leq k$$

genügen, so besteht für grosses  $k > 0$  die asymptotische Formel

$$A(k) = \int_{-\infty}^{+\infty} |F(x, 1)|^{-2/n} dx \cdot k^{2/n} + O\left(k^{\frac{1}{n-1}}\right).$$

Da offenbar  $A(k)/k$  die mittlere Anzahl der Darstellungen grosser natürlicher Zahlen durch den Absolutbetrag von  $F(x, y)$  bedeutet, so ist hiernach diese mittlere Anzahl gleich

$$O\left(k^{\frac{2}{n}-1}\right) = o(1),$$

und es gibt demnach gewissermassen nur 0% aller Zahlen, die sich durch die betrachtete Binärform darstellen lassen.

Zu ganz analogen Sätzen kommt man, wenn man in der Reihe für  $Z(s)$  nur über die teilerfremden Paare  $p, q$  summiert oder die Anzahl  $A'(k)$  der Lösungspaare  $p, q$  von

$$|F(p, q)| \leq k, \quad (p, q) = 1$$

betrachtet; man muss in den letzten Aussagen dann nur

$$\int_{-\infty}^{+\infty} |F(x, 1)|^{-2/n} dx \quad \text{durch} \quad \frac{6}{\pi^2} \int_{-\infty}^{+\infty} |F(x, 1)|^{-2/n} dx$$

ersetzen.

Das Ziel der vorliegenden Arbeit ist nicht der Beweis der zitierten Sätze, sondern der Beweis eines allgemeineren Ergebnisses, das sie als blosse Spezialfälle enthält. Diese Verallgemeinerung beruht darauf, dass neben dem gewöhnlichen Absolutbetrag auch die  $p$ -adischen Bewertungen herangezogen werden, wie dies bereits in den beiden ersten Teilen der vorliegenden Abhandlung geschah. Dort wurde u. a. gezeigt<sup>1</sup>:

<sup>1</sup> Siehe meine Arbeit: »Zur Approximation algebraischer Zahlen«, Teil I in Math. Ann. 107 (1933), 691—730 und Teil II in Math. Ann. 108 (1933), 37—55, weiter zitiert als I und II. Der angegebene Satz ist eine triviale Folge aus I, Satz 2, S. 722.

»Sind  $P_1, P_2, \dots, P_t$  endlichviele verschiedene Primzahlen und ist  $Q(p, q)$  für irgend zwei ganze rationale Zahlen  $p, q$ , die nicht beide verschwinden, ihr grösstes Potenzprodukt, das in  $F(p, q)$  aufgeht, so besitzt die Ungleichung

$$\frac{|F(p, q)|}{Q(p, q)} \leq k$$

für noch so grosses  $k > 0$  nur endlichviele Lösungspaare  $p, q$  mit  $(p, q) = 1$  und also auch nur endlichviele Lösungspaare  $p, q$ , die nur der geringeren Forderung  $(p, q, P_1 P_2 \dots P_t) = 1$  genügen.»

Es hat also Sinn, nach einer asymptotischen Formel für die Anzahl  $A(k)$  der Lösungspaare  $p, q$  von

$$\frac{|F(p, q)|}{Q(p, q)} \leq k, \quad (p, q, P_1 P_2 \dots P_t) = 1$$

oder für die Anzahl  $A'(k)$  der Lösungspaare  $p, q$  von

$$\frac{|F(p, q)|}{Q(p, q)} \leq k, \quad (p, q) = 1$$

zu fragen, unter der Annahme, dass  $k > 0$  über alle Grenzen wächst. Ich zeige als Antwort auf diese Frage die beiden Beziehungen

$$A(k) = \begin{cases} \sigma \prod_{\tau=1}^t \sigma(P_\tau) \cdot k^{2/n} + O(k^{1/n}) & \text{für } t_0 = 0, \\ \sigma \prod_{\tau=1}^t \sigma(P_\tau) \cdot k^{2/n} + O(k^{\frac{1}{n-1}} (\log k)^{t_0-1}) & \text{für } t_0 \geq 1, \end{cases}$$

und

$$A'(k) = \begin{cases} \sigma' \prod_{\tau=1}^t \sigma'(P_\tau) \cdot k^{2/n} + O(k^{1/n} \log k) & \text{für } t_0 = 0, \\ \sigma' \prod_{\tau=1}^t \sigma'(P_\tau) \cdot k^{2/n} + O(k^{\frac{1}{n-1}} (\log k)^{t_0-1}) & \text{für } t_0 \geq 1. \end{cases}$$

Dabei geben die Konstanten

$$\sigma = \int_{-\infty}^{+\infty} |F(x, 1)|^{-2/n} dx, \quad \sigma' = \frac{6}{\pi^2} \int_{-\infty}^{+\infty} |F(x, 1)|^{-2/n} dx$$

gewissermassen das Verhalten der Form  $F(x, y)$  in bezug auf die Absolutbetragbewertung wieder; entsprechenderweise sind die Zahlen

$$\sigma(P_\tau) = \sum_{h=0}^{\infty} d(P_\tau^h) (P_\tau^h)^{2/n}, \quad \sigma'(P_\tau) = \frac{\sigma(P_\tau)}{1 - P_\tau^2}$$

für  $\tau = 1, 2, \dots, t$  der  $P_\tau$ -adischen Bewertung zugeordnet, und es bedeutet in ihnen  $d(P_\tau^h)$  die Dichte der Paare ganzer rationaler Zahlen  $p, q$  mit

$$(F(p, q), P_\tau^{h+1}) = P_\tau^h, \quad (p, q, P_\tau) = 1$$

im Gitter aller Paare ganzer rationaler Zahlen  $p, q$ . Ferner ist  $t_0$  die Anzahl derjenigen Körper unter den Körpern der reellen, der  $P_1$ -adischen, der  $P_2$ -adischen, ..., der  $P_t$ -adischen Zahlen, in denen die Gleichung

$$F(x, 1) = 0$$

mindestens eine Nullstelle hat.

Das Bemerkenswerte an diesen beiden Ergebnissen ist, dass sie in klarer Weise die Gleichberechtigung der verschiedenen  $P_\tau$ -adischen Bewertungen untereinander und mit der Absolutbetragbewertung zum Ausdruck bringen. Dies wird noch klarer, wenn man beachtet, dass ja

$$\left| \frac{F(p, q)}{Q(p, q)} \right| = |F(p, q)| \prod_{\tau=1}^t |F(p, q)|_{P_\tau}$$

ist. Merkwürdig ist auch das Auftreten der Anzahl  $t_0$  in den Fehlergliedern; ob diese allerdings die richtige Grössenordnung des Fehlers geben, bleibe dahingestellt. Die Entscheidung hierüber wird sich vielleicht durch eine Verschärfung des Beweises in dieser Arbeit erbringen lassen.

Aus den asymptotischen Formeln für  $A(k)$  und  $A'(k)$  lässt sich auch eine Verallgemeinerung des Siegelschen Satzes gewinnen. *Es folgt leicht aus ihnen, dass die beiden Dirichletschen Reihen*

$$Z(s) = \sum_{\substack{p=-\infty \\ (p, q, P_1 P_2 \dots P_t) = 1}}^{+\infty} \sum_{q=-\infty}^{+\infty} \left\{ \left| \frac{F(p, q)}{Q(p, q)} \right| \right\}^{-s} \quad \text{und} \quad Z'(s) = \sum_{\substack{p=-\infty \\ (p, q) = 1}}^{+\infty} \sum_{q=-\infty}^{+\infty} \left\{ \left| \frac{F(p, q)}{Q(p, q)} \right| \right\}^{-s}$$

für  $\sigma_0 > 2/n$  konvergieren und dass sich die durch sie dargestellten Funktionen in

die Halbebene  $\sigma_0 > 1/n - 1$  fortsetzen lassen und hier regulär sind bis auf einen einfachen Pol bei  $s = 2/n$  mit dem Residuum

$$\frac{2}{n} \sigma \prod_{\tau=1}^t \sigma(P_\tau) \quad \text{bzw.} \quad \frac{2}{n} \sigma' \prod_{\tau=1}^t \sigma'(P_\tau).$$

Im Spezialfall  $t_0 = 0$  kann man beide Funktionen sogar bis in die ganze Halbebene  $\sigma_0 > 1/n$  fortsetzen und die erste von ihnen existiert darüber hinaus nach einem alten Satz von Hj. Mellin in der ganzen  $s$ -Ebene als meromorphe Funktion.<sup>1</sup>

Es sei noch kurz einiges über den Beweis der Näherungsformeln für  $A(k)$  und  $A'(k)$  gesagt. Diese beiden Anzahlen sind mit einander durch die beiden Gleichungen

$$A(k) = \sum A' \left( \frac{k}{d^n} \right), \quad A'(k) = \sum \mu(d) A \left( \frac{k}{d^n} \right)$$

verbunden, wo über alle natürlichen Zahlen mit

$$(d, P_1 P_2 \dots P_t) = 1$$

summiert wird und wo  $\mu(d)$  wie üblich die Möbiussche arithmetische Funktion bedeutet. Es genügt also, eine von ihnen zu berechnen, da man dann die andere auch leicht angeben kann. Da nun  $A(k)$  ein einfacheres Verhalten zeigt, so wird in dieser Arbeit die Anzahl  $A(k)$  der Lösungspaare von

$$\left| \frac{F(p, q)}{Q(p, q)} \right| \leq k, \quad (p, q, P_1 P_2 \dots P_t) = 1$$

abgeschätzt. Es wird unterschieden, ob

$$|p, q| \geq k^{\frac{1}{n-1}} \quad \text{oder} \quad |p, q| < k^{\frac{1}{n-1}}$$

ist. Die zweite Teilanzahl wird auf elementare Weise bestimmt, indem man sie weiter unterteilt je nach dem Wert von  $Q(p, q)$  und den Kongruenzeigenschaften von  $p$  und  $q$ ; alsdann ist es nur nötig, von trivialen Gitterpunktsabschätzungen Gebrauch zu machen. Wesentlich schwieriger ist die Abschätzung der zweiten Teilanzahl. Man muss zu diesem Zweck meine Verallgemeinerung des Thue-Siegelschen Satzes heranziehen und sich einfacher Sätze über Kettenbrüche bedienen. Der Beweis enthält implizit eine Theorie der Kettenbrüche bei Berück-

<sup>1</sup> Siehe Acta Soc. Scient. Fenn. 29, (1900), Nr. 4.

sichtigung der reellen und verschiedener  $P$ -adischer Bewertungen. In einer späteren Veröffentlichung hoffe ich diese Dinge eingehender darstellen zu können.

Zum Schluss möge noch erwähnt werden, dass die Ergebnisse dieser Arbeit auch dann richtig bleiben, wenn die Binärform  $F(x, y)$  nicht mehr irreduzibel ist, sondern nur noch nichtverschwindende Diskriminante hat und im Körper der rationalen Zahlen in keine Faktoren von niederem als zweiten Grad zerfällt. Dieselbe Verallgemeinerung ist auch in den beiden ersten Teilen zulässig, wenn man sich überall statt mit dem Siegelschen mit dem Thueschen Exponenten zufrieden gibt.

Herrn Prof. C. Siegel gilt mein aufrichtiger Dank dafür, dass er mir seinerzeit seinen Satz und Beweis mitteilte.

**Tabelle der Zahlen  $\nu, \sigma, \sigma'$  für die spezielle Binärform**

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

1. Absolutbetrag-Bewertung:

$$\nu = 1, \quad \sigma = \int_{-\infty}^{+\infty} |x^3 - 2|^{-2/3} dx, \quad \sigma' = \frac{6}{\pi^2} \int_{-\infty}^{+\infty} |x^3 - 2|^{-2/3} dx.$$

2.  $P$ -adische Bewertungen:

$P = 2$	$\nu = 0$	$\sigma = \frac{2 + \sqrt[3]{4}}{4}$	$\sigma' = \frac{2 + \sqrt[3]{4}}{3} > 1$
$P = 3$	$\nu = 0$	$\sigma = \frac{6 + 2\sqrt[3]{9}}{9}$	$\sigma' = \frac{3 + \sqrt[3]{9}}{4} > 1$
$P = 5$	$\nu = 1$	$\sigma = \frac{20\sqrt[3]{5} - 4}{25(\sqrt[3]{5} - 1)}$	$\sigma' = \frac{5\sqrt[3]{5} - 1}{6(\sqrt[3]{5} - 1)} > 1$
$P = 7$	$\nu = 0$	$\sigma = \frac{48}{49}$	$\sigma' = 1$
$P = 11$	$\nu = 1$	$\sigma = \frac{110\sqrt[3]{11} - 10}{121(\sqrt[3]{11} - 1)}$	$\sigma' = \frac{11\sqrt[3]{11} - 1}{12(\sqrt[3]{11} - 1)} > 1$
$P = 13$	$\nu = 0$	$\sigma = \frac{168}{169}$	$\sigma' = 1$

$P = 17$	$\nu = 1$	$\sigma = \frac{272 \sqrt[3]{17} - 16}{289(\sqrt[3]{17} - 1)}$	$\sigma' = \frac{17 \sqrt[3]{17} - 1}{18(\sqrt[3]{17} - 1)} > 1$
$P = 19$	$\nu = 0$	$\sigma = \frac{360}{361}$	$\sigma' = 1$
$P = 23$	$\nu = 1$	$\sigma = \frac{506 \sqrt[3]{23} - 22}{529(\sqrt[3]{23} - 1)}$	$\sigma' = \frac{23 \sqrt[3]{23} - 1}{24(\sqrt[3]{23} - 1)} > 1$
$P = 29$	$\nu = 1$	$\sigma = \frac{812 \sqrt[3]{29} - 28}{841(\sqrt[3]{29} - 1)}$	$\sigma' = \frac{29 \sqrt[3]{29} - 1}{30(\sqrt[3]{29} - 1)} > 1$
$P = 31$	$\nu = 3$	$\sigma = \frac{870 \sqrt[3]{31} + 1830}{961(\sqrt[3]{31} - 1)}$	$\sigma' = \frac{29 \sqrt[3]{31} + 61}{32(\sqrt[3]{31} - 1)} > 1$

Die beiden Primzahlen  $P = 2$  und  $P = 3$  sind irregulär, alle anderen Primzahlen dagegen regulär in bezug auf die Form  $F(x, y)$ .

### Bezeichnungen:

Wie in den beiden ersten Teilen sind folgende festen Bezeichnungen gewählt worden:

$F(x, y)$  bedeutet eine feste irreduzible Binärform mit ganzen rationalen Koeffizienten vom Grad  $n \geq 3$ , und es ist  $f(x) \equiv F(x, 1)$ .

$|\alpha|$  bedeutet den gewöhnlichen Absolutbetrag einer reellen Zahl.

$|\alpha|_P$  bedeutet den  $P$ -adischen Wert einer  $P$ -adischen Zahl.

$P_1, P_2, \dots, P_t$  sind endlichviele verschiedene Primzahlen.

$p$  und  $q$  sind zwei ganze rationale Zahlen, die entweder teilerfremd oder der Bedingung  $(p, q, P_1 P_2 \dots P_t) = 1$  genügend angenommen werden; es wird  $|p, q| = \max(|p|, |q|)$  gesetzt.

$Q(p, q)$  ist das grösste Potenzprodukt der Zahlen  $P_1, P_2, \dots, P_t$ , das in  $F(p, q)$  aufgeht.

$k$  ist eine positive und über alle Grenzen wachsende Zahl.

$\zeta, \zeta', \dots, \zeta^{(\nu-1)}$  sind die sämtlichen reellen Nullstellen von  $f(x)$ .

$\zeta_\tau, \zeta'_\tau, \dots, \zeta_\tau^{(\nu_\tau-1)}$  sind für  $\tau = 1, 2, \dots, t$  die sämtlichen  $P_\tau$ -adischen Nullstellen von  $f(x)$ .

$t_0^*$  und  $t_0$  sind die beiden Anzahlen  $t_0^* = \sum_{\tau=1}^t \operatorname{sgn} v_\tau$  und  $t_0 = \operatorname{sgn} v + t_0^*$ .

$\sigma$  und  $\sigma'$  sind die beiden positiven Zahlen  $\sigma = \int_{-\infty}^{+\infty} |F(x, 1)|^{-2/n} dx$  und  $\sigma' = \frac{6\sigma}{\pi^2}$ .

$d(P^h)$  ist die Dichte der Paare ganzer rationaler Zahlen  $p, q$  mit

$$|F(p, q)|_P = P^{-h}, \quad (p, q, P) = 1$$

im Gitter aller ganzer rationaler  $p, q$ , wenn  $P$  irgend eine Primzahl bedeutet.

$\sigma(P)$  und  $\sigma'(P)$  sind die beiden Summen  $\sigma(P) = \sum_{h=0}^{\infty} d(P^h) (P^h)^{2/n}$ ,  $\sigma'(P) = \frac{\sigma(P)}{1 - P^{-2}}$ .

$A(k)$  ist die Anzahl der Lösungspaare  $p, q$  von

$$\left| \frac{F(p, q)}{Q(p, q)} \right| \leq k, \quad (p, q, P_1 P_2 \dots P_t) = 1.$$

$A'(k)$  ist die Anzahl der Lösungspaare  $p, q$  von

$$\left| \frac{F(p, q)}{Q(p, q)} \right| \leq k, \quad (p, q) = 1.$$

## I.

1. Einige Ergebnisse, die in den beiden ersten Teilen dieser Arbeit erhalten wurden und von denen weiterhin Gebrauch gemacht wird, lassen sich zu folgendem Satz zusammenfassen<sup>1</sup>:

**Satz 1:** *Bedeute*

$f(x)$  *ein irreduzibles Polynom mit ganzen rationalen Koeffizienten vom Grad*  $n \geq 3$ ,

$\zeta$  *eine reelle Nullstelle von*  $f(x)$ , *falls eine solche existiert,*

$P_1, P_2, \dots, P_t$  *endlichviele verschiedene Primzahlen,*

$\zeta_1, \zeta_2, \dots, \zeta_t$  *je eine*  $P_1$ -*adische, eine*  $P_2$ -*adische, ..., eine*  $P_t$ -*adische Nullstelle von*  $f(x)$ , *falls solche existieren,*

<sup>1</sup> Die Aussage (1) ist offenbar eine triviale Folge aus (2); letztere ist identisch mit I, Satz 1, S. 710 (Die dortige Einschränkung  $k \geq 1$  ist unwesentlich). Der Beweis von (3) ist enthalten im Beweis von II, Hilfssatz 3, S. 39–46.



$\beta$  eine Zahl im Intervall  $\min_{s=1, 2, \dots, n-1} \left( \frac{n}{s+1} + s \right) < \beta \leq n$ ,  
 $k$  eine positive Zahl,  
 $p$  und  $q$  zwei teilerfremde ganze rationale Zahlen mit  $q \neq 0$ .

Dann gelten die drei Aussagen:

(1): Es gibt drei positive Zahlen

$$c_0(\zeta, \beta), c'_0(\zeta_1, \zeta_2, \dots, \zeta_t, \beta), c''_0(\zeta, \zeta_1, \zeta_2, \dots, \zeta_t, \beta),$$

die von  $p$  und  $q$  nicht abhängen, so dass stets

$$\left| \frac{p}{q} - \zeta \right| \geq c_0 |p, q|^{-\beta},$$

$$\prod_{\tau=1}^t |p - q \zeta_\tau|_{P_\tau} \geq c'_0 |p, q|^{-\beta},$$

$$\left| \frac{p}{q} - \zeta \right| \prod_{\tau=1}^t |p - q \zeta_\tau|_{P_\tau} \geq c''_0 |p, q|^{-\beta}$$

ist.

(2): Jede der drei Ungleichungen

$$\left| \frac{p}{q} - \zeta \right| \leq k |p, q|^{-\beta},$$

$$\prod_{\tau=1}^t |p - q \zeta_\tau|_{P_\tau} \leq k |p, q|^{-\beta},$$

$$\left| \frac{p}{q} - \zeta \right| \prod_{\tau=1}^t |p - q \zeta_\tau|_{P_\tau} \leq k |p, q|^{-\beta}$$

besitzt nur endlichviele Lösungspaare  $p, q$ .

(3): Von diesen Lösungspaaren genügen für über alle Grenzen wachsendes  $k$  höchstens

$$O(\log \log k)$$

der weiteren Ungleichung

$$|p, q| \geq (4k)^{\frac{1}{\beta-2}}.$$

2. **Satz 2:** Gelten die Voraussetzungen von Satz 1, während jedoch die Zahlen  $p$  und  $q$  nicht mehr notwendigerweise teilerfremd sind, so hat jedes der drei Bedingungssysteme

$$A(I, o): \quad \left| \frac{p}{q} - \zeta \right| \leq k |p, q|^{-\beta}, \quad |p, q| \geq (4k)^{\frac{1}{\beta-2}};$$

$$A(o, t): \quad \prod_{\tau=1}^t |p - q \zeta_{\tau}|_{P_{\tau}} \leq k |p, q|^{-\beta}, \quad |p, q| \geq (4k)^{\frac{1}{\beta-2}}, \quad (p, q, P_1 P_2 \dots P_t) = 1;$$

$$A(I, t): \quad \left| \frac{p}{q} - \zeta \right| \prod_{\tau=1}^t |p - q \zeta_{\tau}|_{P_{\tau}} \leq k |p, q|^{-\beta}, \quad |p, q| \geq (4k)^{\frac{1}{\beta-2}}, \quad (p, q, P_1 P_2 \dots P_t) = 1$$

höchstens

$$O(k^{\frac{1}{\beta}} \log \log k)$$

Lösungspaare  $p, q$ .

**Beweis:** Sei  $p, q$  ein Lösungspaar eines dieser drei Systeme und etwa

$$(p, q) = d, \quad p = dp', \quad q = dq',$$

so dass in den zwei Fällen  $A(o, t)$  und  $A(I, t)$  die natürliche Zahl  $d$  zu sämtlichen Primzahlen  $P_1, P_2, \dots, P_t$  teilerfremd ist. Das teilerfremde Paar  $p', q'$  genügt somit der Reihe nach den Bedingungen

$$A'(I, o): \quad \left| \frac{p'}{q'} - \zeta \right| \leq k' |p', q'|^{-\beta}, \quad |p', q'| \geq (4k')^{\frac{1}{\beta-2}};$$

$$A'(o, t): \quad \prod_{\tau=1}^t |p' - q' \zeta_{\tau}|_{P_{\tau}} \leq k' |p', q'|^{-\beta}, \quad |p', q'| \geq (4k')^{\frac{1}{\beta-2}};$$

$$A'(I, t): \quad \left| \frac{p'}{q'} - \zeta \right| \prod_{\tau=1}^t |p' - q' \zeta_{\tau}|_{P_{\tau}} \leq k' |p', q'|^{-\beta}, \quad |p', q'| \geq (4k')^{\frac{1}{\beta-2}},$$

wo zur Abkürzung  $k' = k/d^{\beta}$  gesetzt wurde. Nach Satz 1, (3) hat demnach  $p', q'$  jedesmal nur höchstens

$$O(\log \log k)$$

Möglichkeiten. Andererseits ergibt sich aus Satz 1, (1), dass der Reihe nach in den drei Fällen (I, o), (o, t), (I, t)

$$c_0 |p', q'|^{-\beta} \leq k' |p', q'|^{-\beta}, \quad c'_0 |p', q'|^{-\beta} \leq k' |p', q'|^{-\beta}, \quad c''_0 |p', q'|^{-\beta} \leq k' |p', q'|^{-\beta},$$

also

$$d \leq \left( \frac{k}{c_0} \right)^{1/\beta}, \quad d \leq \left( \frac{k}{c'_0} \right)^{1/\beta}, \quad d \leq \left( \frac{k}{c''_0} \right)^{1/\beta}$$

ist, so dass  $d$  nur

$$O(k^{1/\beta})$$

verschiedene Werte annehmen kann. Berücksichtigt man sämtliche Möglichkeiten, die sowohl für das Paar  $p', q'$ , als auch für  $d$  bestehen, so folgt somit schliesslich, dass die Zahl der sämtlichen Paare  $p, q$  gleich

$$O(k^{1/\beta}) O(\log \log k) = O(k^{1/\beta} \log \log k)$$

ist, w. z. b. w.

3. **Satz 3:** *Gelten die Voraussetzungen von Satz 1, während jedoch die Zahlen  $p$  und  $q$  nicht mehr notwendigerweise teilerfremd sind, so hat das Bedingungssystem*

$$a(1, 0): \quad \left| \frac{p}{q} - \zeta \right| \leq k |p, q|^{-\beta}, \quad |p, q| \geq k^{\frac{1}{\beta-1}}$$

höchstens

$$O(k^{\frac{1}{\beta-1}})$$

Lösungspaare.

**Beweis:** Nach Satz 2 genügt es, die Behauptung allein für die Anzahl der Lösungspaare  $p, q$  mit

$$k^{\frac{1}{\beta-1}} \leq |p, q| < (4k)^{\frac{1}{\beta-2}}$$

zu beweisen, denn die Anzahl der restlichen Lösungspaare ist ja gleich

$$O(k^{\frac{1}{\beta}} \log \log k) \leq O(k^{\frac{1}{\beta-1}}).$$

Der Beweis beruht auf bekannten Kettenbruchsätzen.

Sei zur Abkürzung

$$a_j = 2^j k^{\frac{1}{\beta-1}} \quad \text{für} \quad 2^j k^{\frac{1}{\beta-1}} < (4k)^{\frac{1}{\beta-2}},$$

$$a_g = (4k)^{\frac{1}{\beta-2}} \quad \text{für} \quad 2^{g-1} k^{\frac{1}{\beta-1}} < (4k)^{\frac{1}{\beta-2}} \leq 2^g k^{\frac{1}{\beta-1}}$$

und bedeute  $M_j$  die Menge der Paare  $p, q$  mit

$$\left| \frac{p}{q} - \zeta \right| \leq k |p, q|^{-\beta}, \quad a_j \leq |p, q| < a_{j+1} \quad (j=0, 1, \dots, g-1),$$

$N_j$  die Anzahl ihrer Elemente.

Zu jeder der Mengen  $M_j$  gibt es drei auf einander folgende Näherungen

$$\frac{\mathfrak{P}_{f-1}}{\mathfrak{D}_{f-1}}, \frac{\mathfrak{P}_f}{\mathfrak{D}_f}, \frac{\mathfrak{P}_{f+1}}{\mathfrak{D}_{f+1}}$$

des Kettenbruches für  $\zeta$  mit

$$\mathfrak{D}_f \leq a_{j+1} < \mathfrak{D}_{f+1}.$$

Nach bekannten Sätzen sind diese Brüche gekürzt und gilt ferner

$$\begin{aligned} \mathfrak{P}_{f-1}\mathfrak{D}_f - \mathfrak{P}_f\mathfrak{D}_{f-1} &= \mp 1, \\ \left| \frac{\mathfrak{P}_f}{\mathfrak{D}_f} - \zeta \right| &\leq \frac{1}{\mathfrak{D}_f\mathfrak{D}_{f+1}}. \end{aligned}$$

Aus der letzten Ungleichung und der Identität

$$p\mathfrak{D}_f - q\mathfrak{P}_f = q\mathfrak{D}_f \left( \frac{p}{q} - \zeta \right) - q\mathfrak{D}_f \left( \frac{\mathfrak{P}_f}{\mathfrak{D}_f} - \zeta \right)$$

folgt für alle Paare  $p, q$  aus  $M_j$  die Ungleichung

$$|p\mathfrak{D}_f - q\mathfrak{P}_f| \leq |p, q| \mathfrak{D}_f \frac{k}{|p, q|^3} + |p, q| \mathfrak{D}_f \frac{1}{\mathfrak{D}_f\mathfrak{D}_{f+1}} \leq \frac{k\mathfrak{D}_f}{|p, q|^{3-1}} + 1$$

und da nach Definition in dieser Menge

$$|p, q| \geq a_j$$

ist, so ergibt sich

$$|p\mathfrak{D}_f - q\mathfrak{P}_f| \leq \frac{k\mathfrak{D}_f}{a_j^{3-1}} + 1.$$

Jedem Lösungspaar  $p, q$  aus  $M_j$  werde jetzt durch

$$\begin{aligned} p &= \mathfrak{P}_{f-1}\mathfrak{p} + \mathfrak{P}_f\mathfrak{q}, \\ q &= \mathfrak{D}_{f-1}\mathfrak{p} + \mathfrak{D}_f\mathfrak{q} \end{aligned}$$

ein Zahlpaar  $\mathfrak{p}, \mathfrak{q}$  zugeordnet; da diese linearen Gleichungen die Determinante  $\mp 1$  haben, so sind  $\mathfrak{p}$  und  $\mathfrak{q}$  eindeutig bestimmt und wieder ganz rational. Wegen

$$p\mathfrak{D}_f - q\mathfrak{P}_f = \mathfrak{p}(\mathfrak{P}_{f-1}\mathfrak{D}_f - \mathfrak{P}_f\mathfrak{D}_{f-1}) = \mp \mathfrak{p}$$

muss sein:

$$|p| \leq \frac{k \mathfrak{D}_f}{a_j^{\beta-1}} + 1,$$

so dass für  $p$  höchstens

$$\frac{2k \mathfrak{D}_f}{a_j^{\beta-1}} + 3$$

verschiedene Werte möglich sind. Ferner genügt  $q$  der Ungleichung

$$|q| = |\mathfrak{D}_{f-1} p + \mathfrak{D}_f q| \leq |p, q| \leq a_{j+1} \leq 2a_j,$$

ist also für jeden Wert von  $p$  höchstens

$$\frac{4a_j}{\mathfrak{D}_f} + 1$$

oder wegen

$$\mathfrak{D}_f \leq a_{j+1} \leq 2a_j, \quad \frac{2a_j}{\mathfrak{D}_f} \geq 1$$

höchstens

$$\frac{6a_j}{\mathfrak{D}_f}$$

verschiedener Werte fähig.

Die Anzahl  $N_j$  genügt demnach der Ungleichung

$$N_j \leq \left( \frac{2k \mathfrak{D}_f}{a_j^{\beta-1}} + 3 \right) \frac{6a_j}{\mathfrak{D}_f} = \frac{12k}{a_j^{\beta-2}} + \frac{18a_j}{\mathfrak{D}_f} \quad (j=0, 1, \dots, g-1).$$

Wegen

$$a_j = 2^j k^{\frac{1}{\beta-1}} \quad (j=0, 1, \dots, g-1)$$

ist hier

$$\frac{12k}{a_j^{\beta-2}} = \frac{12k^{\frac{1}{\beta-1}}}{2^{(\beta-2)j}}.$$

Nach Satz 1, (I) gibt es ferner eine positive Zahl  $c_0$ , so dass für jedes Paar teilerfremder ganzer rationaler Zahlen  $\mathfrak{P}, \mathfrak{Q}$

$$\left| \frac{\mathfrak{P}}{\mathfrak{Q}} - \zeta \right| \geq c_0 |\mathfrak{P}, \mathfrak{Q}|^{-\beta}$$

ist; es gibt somit eine zweite positive Konstante  $c_0^*$ , so dass sogar

$$\left| \frac{\mathfrak{B}}{\mathfrak{D}} - \zeta \right| \geq c_0^* |\mathfrak{D}|^{-\beta}$$

gilt. Wegen der Teilerfremdheit von  $\mathfrak{B}_f$  und  $\mathfrak{D}_f$  ist hiernach insbesondere

$$\left| \frac{\mathfrak{B}_f}{\mathfrak{D}_f} - \zeta \right| \geq c_0^* \mathfrak{D}_f^{-\beta},$$

wegen

$$\left| \frac{\mathfrak{B}_f}{\mathfrak{D}_f} - \zeta \right| \leq \frac{1}{\mathfrak{D}_f \mathfrak{D}_{f+1}}$$

also

$$c_0^* \mathfrak{D}_f^{-\beta} \leq \frac{1}{\mathfrak{D}_f \mathfrak{D}_{f+1}}, \quad \mathfrak{D}_f \geq c_0^{*\frac{1}{\beta-1}} \mathfrak{D}_{f+1}^{\frac{1}{\beta-1}}.$$

Nach Annahme hat man aber

$$\mathfrak{D}_{f+1} \geq a_{j+1} \geq a_j;$$

also wird

$$\mathfrak{D}_f \geq c_0^{*\frac{1}{\beta-1}} a_j^{\frac{1}{\beta-1}}$$

und

$$\frac{18a_j}{\mathfrak{D}_f} \leq 18c_0^{*\frac{1}{\beta-1}} a_j^{\frac{\beta-2}{\beta-1}}$$

und da nach Definition von  $a_j$

$$a_j = 2^{j-g+1} a_{g-1} \leq 2^{j-g+1} (4k)^{\frac{1}{\beta-2}} \quad (j=0, 1, \dots, g-1)$$

ist, so kommt man zu

$$\frac{18a_j}{\mathfrak{D}_f} \leq 18c_0^{*\frac{1}{\beta-1}} 2^{-\frac{\beta-2}{\beta-1}(g-j-1)} (4k)^{\frac{1}{\beta-1}}$$

und damit schliesslich zu der Ungleichung

$$N_j \leq 12 \cdot 2^{-(\beta-2)j} k^{\frac{1}{\beta-1}} + 18c_0^{*\frac{1}{\beta-1}} 2^{-\frac{\beta-2}{\beta-1}(g-j-1)} (4k)^{\frac{1}{\beta-1}} \quad (j=0, 1, \dots, g-1).$$

Wie aber zu Beginn des Beweises gezeigt wurde, gibt es gerade

$$\sum_{j=0}^{g-1} N_j + O(k^{\frac{1}{\beta-1}})$$

Lösungspaare, die den Ungleichungen

$$\left| \frac{p}{q} - \zeta \right| \leq k |p, q|^{-\beta}, \quad |p, q| \geq k^{\frac{1}{\beta-1}}$$

genügen. Wird hier die vorige obere Schranke für  $N_j$  eingesetzt und beachtet, dass die beiden geometrischen Reihen

$$\sum_{j=0}^{g-1} 12 \cdot 2^{-(\beta-2)j} \quad \text{und} \quad \sum_{j=0}^{g-1} 18 c_0^* \cdot \frac{1}{\beta-1} 2^{-\frac{\beta-2}{\beta-1}(g-j-1)}$$

wegen  $\beta > 2$  unterhalb einer von  $k$  unabhängigen Schranke bleiben, so erhält man also für die Lösungsanzahl die obere Schranke

$$k^{\frac{1}{\beta-1}} O(1) + O(k^{\frac{1}{\beta-1}}) = O(k^{\frac{1}{\beta-1}}),$$

und diese sollte gerade erhalten werden.

4. **Satz 4:** *Gelten die Voraussetzungen von Satz 1, während jedoch die Zahlen  $p$  und  $q$  nicht mehr notwendigerweise teilerfremd sind, so hat das Bedingungssystem*

$$a(o, t): \prod_{\tau=1}^t |p - q \zeta_\tau|_{P_\tau} \leq k |p, q|^{-\beta}, \quad |p, q| \geq k^{\frac{1}{\beta-1}}, \quad (p, q, P_1 P_2 \dots P_t) = 1,$$

$$|p - q \zeta_\tau|_{P_\tau} < 1 \quad (\tau = 1, 2, \dots, t)$$

höchstens

$$O(k^{\frac{1}{\beta-1}} (\log k)^{t-1})$$

Lösungspaare.

**Beweis:** Nach Satz 2 genügt es, die behauptete Schranke allein für diejenigen Lösungen nachzuweisen, die der Ungleichung

$$k^{\frac{1}{\beta-1}} \leq |p, q| < (4k)^{\frac{1}{\beta-2}}$$

genügen, denn die Anzahl der übrigen ist ja höchstens gleich

$$O(k^{\frac{1}{\beta}} \log \log k) \leq O(k^{\frac{1}{\beta-1}} (\log k)^{t-1}).$$

Das Intervall

$$k^{\frac{1}{\beta-1}} \leq |p, q| < (4k)^{\frac{1}{\beta-2}}$$

werde wie in 3. in die endlichvielen Teilintervalle

$$a_j \leq |p, q| < a_{j+1}$$

zerlegt und unter  $M_j$  wieder die Menge, unter  $N_j$  wieder die Anzahl der Lösungspaare in diesem Intervall verstanden.

Durch

$$z = \prod_{\tau=1}^t \max(1, |\zeta_\tau|_{P_\tau})$$

wird eine solche natürliche Zahl definiert, so dass alle Zahlen

$$\zeta_\tau^* = z \zeta_\tau \quad (\tau = 1, 2, \dots, t)$$

ganz in ihrem jeweiligen Körper werden. Offenbar können wegen der Ganzheit von  $p$  und  $q$  die Voraussetzungen

$$|p - q \zeta_\tau|_{P_\tau} < 1 \quad (\tau = 1, 2, \dots, t)$$

nur dann erfüllt sein, wenn  $q$  ein ganzes rationales Vielfaches

$$q = z q^*$$

von  $z$  ist. Die Menge  $M_j$  ist somit eindeutig bezogen auf die Menge der Paare ganzer rationaler Zahlen  $p, q^*$  mit

$$\prod_{\tau=1}^t |p - q^* \zeta_\tau^*|_{P_\tau} \leq k |p, z q^*|^{-\beta}, \quad a_j \leq |p, z q^*| < a_{j+1},$$

$$|p - q^* \zeta_\tau^*|_{P_\tau} < 1 \quad (\tau = 1, 2, \dots, t), \quad (p, z q^*, P_1 P_2 \dots P_t) = 1$$

und hat die gleiche Elementenanzahl. Folglich ist erst recht  $N_j$  höchstens gleich der Anzahl der Paare ganzer rationaler Zahlen  $p, q$  mit

$$(I): \quad \prod_{\tau=1}^t |p - q \zeta_\tau^*|_{P_\tau} \leq \frac{k}{a_j^\beta}, \quad |p - q \zeta_\tau^*|_{P_\tau} < 1 \quad (\tau = 1, 2, \dots, t),$$

$$|p| < a_{j+1}, \quad |q| < a_{j+1}.$$

Bedeute  $P_\sigma$  die grösste der Primzahlen  $P_1, P_2, \dots, P_t$  und

$$\mathbf{Q} = \{Q_1, Q_2, \dots, Q_t\}$$



die Menge der Potenzprodukte

$$Q = P_1^{h_1} P_2^{h_2} \dots P_t^{h_t},$$

deren Exponenten natürliche Zahlen sind und die der Ungleichung

$$(II): \quad \frac{a_j^\beta}{k} \leq Q < \frac{a_j^\beta}{k} P_\sigma$$

genügen. Wegen

$$P_1 \geq 2, P_2 \geq 2, \dots, P_t \geq 2, \quad a_j \leq a_g = (4k)^{\frac{1}{\beta-2}}, \quad \frac{a_j^\beta}{k} \leq 4^{\frac{\beta}{\beta-2}} k^{\frac{2}{\beta-2}}$$

ist für die Elemente von  $\mathbf{Q}$

$$h_\tau \leq \frac{\log \left( \frac{a_j^\beta}{k} P_\sigma \right)}{\log 2} \leq \frac{\log (4^{\frac{\beta}{\beta-2}} k^{\frac{2}{\beta-2}} P_\sigma)}{\log 2} \quad (\tau = 1, 2, \dots, t).$$

Sind ferner  $h_1, h_2, \dots, h_{t-1}$  gegeben, so hat  $h_t$  nur höchstens

$$\frac{\log P_\sigma}{\log 2}$$

Möglichkeiten;  $\mathbf{Q}$  enthält somit nicht mehr als

$$\frac{\log P_\sigma \{ \log (4^{\frac{\beta}{\beta-2}} k^{\frac{2}{\beta-2}} P_\sigma) \}^{t-1}}{(\log 2)^t}$$

Potenzprodukte.

Es ist klar, dass jedes beliebige Potenzprodukt

$$P_1^{h_1} P_2^{h_2} \dots P_t^{h_t} \geq \frac{a_j^\beta}{k}$$

mit natürlichen Zahlen als Exponenten ein ganzzahliges Vielfaches eines der Elemente aus  $\mathbf{Q}$  sein muss. Folglich lässt sich jeder Lösung  $p, q$  von (I) auf mindestens eine Art ein Potenzprodukt  $Q$  aus  $\mathbf{Q}$  zuordnen, so dass

$$|p - q \zeta_\tau^*|_{P_\tau} \leq |Q|_{P_\tau}, \quad \text{d. h. } p \equiv q \zeta_\tau^* \pmod{|Q|_{P_\tau}^{-1}} \quad (\tau = 1, 2, \dots, t)$$

ist. Versteht man unter  $Z$  diejenige ganze rationale Zahl mit

$$0 \leq Z \leq Q - 1, \quad Z \equiv \zeta_\tau^* \pmod{|Q|_{P_\tau}^{-1}} \quad (\tau = 1, 2, \dots, t),$$

so befriedigen  $p, q$  daher die Kongruenz

$$p \equiv qZ \pmod{Q}$$

und es gibt eine ganze rationale Zahl  $r$  mit

$$p = qZ - rQ.$$

Wegen (I), (II) und

$$a_{j+1} \leq 2a_j$$

wird folglich

$$\left| q \frac{Z}{Q} - r \right| = \left| \frac{p}{Q} \right| \leq a_{j+1} \frac{k}{a_j^3} \leq \frac{2k}{a_j^{\beta-1}}.$$

Bedeutet  $N_j(Q)$  die Anzahl der Paare ganzer rationaler Zahlen  $q$  und  $r$ , die den Bedingungen

$$(III): \quad \left| q \frac{Z}{Q} - r \right| \leq \frac{2k}{a_j^{\beta-1}}, \quad |q| \leq 2a_j$$

Genüge leisten, so ergibt sich also

$$N_j \leq \sum_{\mathfrak{Q}} N_j(Q) \leq \frac{\log P_\sigma \{ \log (4^{\frac{3}{\beta-2}} k^{\frac{2}{\beta-2}} P_\sigma) \}^{t-1}}{(\log 2)^t} \max_{\mathfrak{Q}} N_j(Q),$$

wobei sich die Zeichen  $\Sigma$  und  $max$  auf die Gesamtheit der Elemente  $Q$  aus  $\mathfrak{Q}$  beziehen. Es bleibt noch übrig, die Anzahl der Lösungspaare von (III) nach oben abzuschätzen.

5. Diese Abschätzung wird durch dasselbe Verfahren wie in 3. gewonnen. Sei zur Abkürzung

$$z^* = \prod_{\tau=1}^t \min(1, |\zeta_\tau|_{p_\tau}^{-1}).$$

Wegen

$$Z \equiv \zeta_\tau^* \pmod{|Q|_{p_\tau}^{-1}} \quad (\tau = 1, 2, \dots, t)$$

geht der grösste gemeinschaftliche Teiler

$$\delta = (Q, Z)$$

von  $Q$  und  $Z$  in  $z^*$  auf, ist also gleichmässig in  $k$  und  $j$  beschränkt. Sei

$$Q^* = \frac{Q}{\delta}, \quad Z^* = \frac{Z}{\delta}, \quad \zeta^* = \frac{Z}{Q} = \frac{Z^*}{Q^*},$$

demnach

$$Q^* \geq \frac{a_j^\beta}{kz^*}.$$

Wegen

$$a_j = 2^j k^{\frac{1}{\beta-1}}$$

gilt folglich

$$Q^* \geq \frac{a_j}{z^*} 2^{(\beta-1)j} \geq \frac{a_j}{z^*}.$$

Also existieren drei auf einander folgende Naherungsbruche

$$\frac{\mathfrak{N}_{f-1}}{\mathfrak{D}_{f-1}}, \quad \frac{\mathfrak{N}_f}{\mathfrak{D}_f}, \quad \frac{\mathfrak{N}_{f+1}}{\mathfrak{D}_{f+1}}$$

des Kettenbruches fur  $\zeta^*$ , deren Nenner der Bedingung

$$\mathfrak{D}_f \leq \frac{a_j}{2z^*} 2^{(\beta-2-\varepsilon)j} < \mathfrak{D}_{f+1}$$

genugen;  $\varepsilon < \beta - 2$  bedeutet dabei eine positive Konstante, uber die nachher ver-  
fugt wird. Diese Naherungsbruche haben die Eigenschaften

$$\mathfrak{N}_{f-1}\mathfrak{D}_f - \mathfrak{N}_f\mathfrak{D}_{f-1} = \pm 1,$$

$$|\mathfrak{D}_f\zeta^* - \mathfrak{N}_f| \leq \frac{1}{\mathfrak{D}_{f+1}}.$$

Auf Grund der Identitat

$$r\mathfrak{D}_f - q\mathfrak{N}_f = -\mathfrak{D}_f(q\zeta^* - r) + q(\mathfrak{D}_f\zeta^* - \mathfrak{N}_f)$$

und nach (III) ist somit

$$|r\mathfrak{D}_f - q\mathfrak{N}_f| \leq \frac{2k\mathfrak{D}_f}{a_j^{\beta-1}} + \frac{|q|}{\mathfrak{D}_{f+1}} \leq \frac{2k\mathfrak{D}_f}{a_j^{\beta-1}} + 4z^*.$$

Jedem Losungspaar  $q, r$  von (III) werde durch

$$q = \mathfrak{D}_{f-1}p + \mathfrak{D}_f q,$$

$$r = \mathfrak{N}_{f-1}p + \mathfrak{N}_f q$$

ein Zahlpaar  $p, q$  zugeordnet; da die Determinante dieser linearen Gleichungen gleich  $\bar{\tau} + 1$  ist, so sind  $p$  und  $q$  eindeutig bestimmt und wieder ganz rational. Wegen

$$r\bar{\Sigma}_f - q\bar{\mathfrak{H}}_f = p(\mathfrak{H}_{f-1}\bar{\Sigma}_f - \mathfrak{H}_f\bar{\Sigma}_{f-1}) = \bar{\tau} + p$$

muss sein:

$$|p| \leq \frac{2k\bar{\Sigma}_f}{a_j^{\beta-1}} + 4z^*,$$

so dass für  $p$  höchstens

$$\frac{4k\bar{\Sigma}_f}{a_j^{\beta-1}} + 9z^*$$

verschiedene Werte möglich sind. Ferner genügt  $q$  der Ungleichung

$$|q| = |\bar{\Sigma}_{f-1}p + \bar{\Sigma}_f q| \leq 2a_j,$$

ist also für jeden Wert von  $p$  höchstens

$$\frac{4a_j}{\bar{\Sigma}_f} + 1$$

verschiedener Werte fähig. Für die Anzahl  $N_j(Q)$  ergibt sich daher

$$N_j(Q) \leq \left( \frac{4k\bar{\Sigma}_f}{a_j^{\beta-1}} + 9z^* \right) \left( \frac{4a_j}{\bar{\Sigma}_f} + 1 \right) = \frac{16k}{a_j^{\beta-2}} + \frac{4k\bar{\Sigma}_f}{a_j^{\beta-1}} + \frac{36z^*a_j}{\bar{\Sigma}_f} + 9z^*.$$

Wegen

$$a_j = 2^j k^{\frac{1}{\beta-1}}, \quad \bar{\Sigma}_f \leq \frac{a_j}{2z^*} 2^{(\beta-2-\epsilon)j} = \frac{2^{(\beta-1-\epsilon)j} k^{\frac{1}{\beta-1}}}{2z^*}$$

gilt für die beiden ersten Summanden auf der rechten Seite

$$\frac{16k}{a_j^{\beta-2}} = \frac{16k^{\frac{1}{\beta-1}}}{2^{(\beta-2)j}}, \quad \frac{4k\bar{\Sigma}_f}{a_j^{\beta-1}} \leq \frac{2k^{\frac{1}{\beta-1}}}{z^* 2^{\epsilon j}}.$$

Um auch den dritten Summanden nach oben abzuschätzen, muss Gebrauch gemacht werden vom verallgemeinerten Thue-Siegelschen Satz. Nach Satz 1, (1) gibt es eine positive Konstante

$$c'_0 = c'_0(\zeta_1^*, \zeta_2^*, \dots, \zeta_t^*),$$

so dass für alle Paare teilerfremder ganzer rationaler Zahlen  $\mathfrak{B}, \mathfrak{D}$

$$\prod_{\tau=1}^t |\mathfrak{B} - \mathfrak{D} \zeta_{\tau}^*|_{P_{\tau}} \geq c'_0 |\mathfrak{B}, \mathfrak{D}|^{-\beta}$$

ist. Sei nun zur Abkürzung

$$\mathfrak{B}_f = \mathfrak{D}_f Z - \mathfrak{R}_f Q,$$

ferner der grösste gemeinschaftliche Teiler von  $\mathfrak{B}_f$  und  $\mathfrak{D}_f$  gleich

$$(\mathfrak{B}_f, \mathfrak{D}_f) = d;$$

dieser muss wegen der Teilerfremdheit von  $\mathfrak{D}_f$  und  $\mathfrak{R}_f$  ein Potenzprodukt allein der Zahlen  $P_1, P_2, \dots, P_t$  sein. Nach Konstruktion von  $Z$  ist

$$\mathfrak{B}_f - \mathfrak{D}_f \zeta_{\tau}^* \equiv \mathfrak{B}_f - \mathfrak{D}_f Z \equiv 0 \pmod{|Q|_{P_{\tau}}^{-1}} \quad (\tau = 1, 2, \dots, t)$$

und somit

$$\prod_{\tau=1}^t |\mathfrak{B}_f - \mathfrak{D}_f \zeta_{\tau}^*|_{P_{\tau}} \leq \frac{1}{Q}, \quad \prod_{\tau=1}^t \left| \frac{\mathfrak{B}_f}{d} - \frac{\mathfrak{D}_f}{d} \zeta_{\tau}^* \right|_{P_{\tau}} \leq \frac{d}{Q},$$

also nach der erwähnten Verallgemeinerung des Thue-Siegelschen Satzes

$$\frac{d}{Q} \geq c'_0 \left| \frac{\mathfrak{B}_f}{d}, \frac{\mathfrak{D}_f}{d} \right|^{-\beta}.$$

Somit gilt entweder die Ungleichung

$$(a): \quad |\mathfrak{B}_f| \geq d^{\frac{\beta-1}{\beta}} (c'_0 Q)^{\frac{1}{\beta}}$$

oder die Ungleichung

$$(b): \quad |\mathfrak{D}_f| \geq d^{\frac{\beta-1}{\beta}} (c'_0 Q)^{\frac{1}{\beta}}.$$

Um hiervon die Ungleichung (a) für geeignete  $\varepsilon$  und grosse  $k$  als unmöglich nachzuweisen, muss zurückgegangen werden auf die Formel

$$|\mathfrak{D}_f \zeta^* - \mathfrak{R}_f| \leq \frac{1}{\mathfrak{D}_{f+1}}.$$

Da  $\zeta^* = \frac{Z}{Q}$  ist, so folgt aus derselben

$$|\mathfrak{B}_f| \leq \frac{Q}{\mathfrak{D}_{f+1}}$$

und wegen

$$Q < \frac{a_j^\beta P_\sigma}{k}, \quad |\mathfrak{Q}_{f+1}| > \frac{a_j 2^{(\beta-2-\epsilon)j}}{2z^*}, \quad a_j = 2^j k^{\frac{1}{\beta-1}}$$

ergibt sich

$$|\mathfrak{R}_f| < \frac{a_j^\beta P_\sigma}{k} \frac{2z^*}{a_j 2^{(\beta-2-\epsilon)j}} = \frac{2z^* P_\sigma a_j^{\beta-1}}{k 2^{(\beta-2-\epsilon)j}} = 2z^* P_\sigma 2^{(1+\epsilon)j};$$

andererseits gilt

$$Q \geq \frac{a_j^\beta}{k} = 2^{j\beta} k^{\frac{1}{\beta-1}}$$

und folglich

$$d^{\frac{\beta-1}{\beta}} (c'_0 Q)^{\frac{1}{\beta}} \geq (c'_0 Q)^{\frac{1}{\beta}} \geq c'_0{}^{\frac{1}{\beta}} 2^j k^{\frac{1}{\beta(\beta-1)}}.$$

Die Ungleichung (a) kann also nicht bestehen, wenn für jeden Index  $j \leq g-1$

$$2z^* P_\sigma 2^{(1+\epsilon)j} \leq c'_0{}^{\frac{1}{\beta}} 2^j k^{\frac{1}{\beta(\beta-1)}}$$

oder

$$2^{\epsilon j} \leq \frac{c'_0{}^{\frac{1}{\beta}}}{2z^* P_\sigma} k^{\frac{1}{\beta(\beta-1)}}$$

ist. Nach Definition von  $j$  und  $g$  ist aber immer

$$2^j k^{\frac{1}{\beta-1}} \leq (4k)^{\frac{1}{\beta-2}},$$

also

$$2^j \leq 4^{\frac{1}{\beta-2}} k^{\frac{1}{(\beta-1)(\beta-2)}}$$

und daher

$$2^{\epsilon j} \leq 4^{\frac{\epsilon}{\beta-2}} k^{\frac{\epsilon}{(\beta-1)(\beta-2)}}.$$

Wird die wegen  $\beta > 2$  erlaubte Annahme

$$\epsilon = \frac{\beta-2}{2\beta} = \frac{(\beta-1)(\beta-2)}{2\beta(\beta-1)} < \beta-2$$

gemacht, so ist somit für hinreichend grosses  $k$  die Bedingung (a) niemals erfüllt.

Somit muss (b) zutreffen und

$$|\mathfrak{Q}_f| \geq d^{\frac{\beta-1}{\beta}} (c'_0 Q)^{\frac{1}{\beta}} \geq (c'_0 Q)^{\frac{1}{\beta}} \geq \frac{c'_0{}^{1/\beta} a_j}{k^{1/\beta}}$$

sein. Demnach hat man für den dritten Summanden

$$\frac{36 z^* a_j}{\mathfrak{D}_j} \leq \frac{36 z^* a_j}{c_0^{1/\beta} Q^{1/\beta}} \leq \frac{36 z^*}{c_0^{1/\beta}} k^{\frac{1}{\beta}},$$

und es ist bewiesen, dass die Ungleichung

$$N_j(Q) \leq \frac{16 k^{\frac{1}{\beta-1}}}{2^{(\beta-2)j}} + \frac{2 k^{\frac{1}{\beta-1}}}{z^* 2^{\varepsilon j}} + \frac{36 z^* k^{\frac{1}{\beta}}}{c_0^{1/\beta}} + 9 z^*$$

besteht. Weil hier rechts  $Q$  nicht mehr vorkommt, so folgt weiter

$$N_j \leq \frac{\log P_\sigma \{ \log (4^{\frac{\beta}{\beta-2}} k^{\frac{2}{\beta-2}} P_\sigma) \}^{t-1}}{(\log 2)^t} \left( \frac{16 k^{\frac{1}{\beta-1}}}{2^{(\beta-2)j}} + \frac{2 k^{\frac{1}{\beta-1}}}{z^* 2^{\varepsilon j}} + \frac{36 z^* k^{\frac{1}{\beta}}}{c_0^{1/\beta}} + 9 z^* \right).$$

Wie aber zu Anfang des Beweises festgestellt wurde, hat das Bedingungssystem  $a(o, t)$  gerade

$$N = \sum_{j=0}^{g-1} N_j + O(k^{\frac{1}{\beta-1}} (\log k)^{t-1})$$

Lösungspaare. Da nun die beiden geometrischen Reihen

$$\sum_{j=0}^{g-1} \frac{16}{2^{(\beta-2)j}}, \quad \sum_{j=0}^{g-1} \frac{2}{z^* 2^{\varepsilon j}}$$

unterhalb einer von  $k$  unabhängigen Schranke bleiben und da

$$g = O(\log k)$$

ist, so ergibt sich schliesslich

$$N = O((\log k)^{t-1}) \{ O(k^{\frac{1}{\beta-1}}) + O(k^{\frac{1}{\beta-1}}) + O(k^{\frac{1}{\beta}} \log k) + O(\log k) \} + O(k^{\frac{1}{\beta-1}} (\log k)^{t-1})$$

oder

$$N = O(k^{\frac{1}{\beta-1}} (\log k)^{t-1}),$$

und das sollte gerade gezeigt werden.

6. **Satz 5:** *Gelten die Voraussetzungen von Satz 1, während jedoch die Zahlen  $p$  und  $q$  nicht mehr notwendigerweise teilerfremd sind, so hat das Bedingungssystem*

$$a(1, t): \left| \frac{p}{q} - \zeta \right| \prod_{\tau=1}^t |p - q \zeta_{\tau}|_{P_{\tau}} \leq k |p, q|^{-\beta}, \quad |p, q| \geq k^{\frac{1}{\beta-1}}, \quad (p, q, P_1 P_2 \dots P_t) = 1,$$

$$\left| \frac{p}{q} - \zeta \right| < 1, \quad |p - q \zeta_{\tau}|_{P_{\tau}} < 1 \quad (\tau = 1, 2, \dots, t)$$

höchstens

$$O(k^{\frac{1}{\beta-1}} (\log k)^t)$$

Lösungspaare.

**Beweis:** Es ist hinreichend, die behauptete Schranke allein für die Anzahl derjenigen Lösungen von  $a(1, t)$  nachzuweisen, die der Zusatzbedingung

$$a'(1, t): \prod_{\tau=1}^t |p - q \zeta_{\tau}|_{P_{\tau}} > k |p, q|^{-\beta}$$

genügen; denn die Anzahl der Lösungspaare, die diese Ungleichung nicht befriedigen, ist nach Satz 4 höchstens gleich

$$O(k^{\frac{1}{\beta-1}} (\log k)^{t-1}) \leq O(k^{\frac{1}{\beta-1}} (\log k)^t).$$

Weiter genügt es nach Satz 2, allein diejenigen Lösungen zu betrachten, für die

$$k^{\frac{1}{\beta-1}} \leq |p, q| < (4k)^{\frac{1}{\beta-2}}$$

ist, denn die Anzahl der übrigen ist höchstens gleich

$$O(k^{\frac{1}{\beta}} \log \log k) \leq O(k^{\frac{1}{\beta-1}} (\log k)^t).$$

Das Intervall

$$k^{\frac{1}{\beta-1}} \leq |p, q| < (4k)^{\frac{1}{\beta-2}}$$

werde wie in 3. und 4. in die endlichvielen Teilintervalle

$$a_j \leq |p, q| < a_{j+1}$$

zerlegt und unter  $M_j$  wieder die Menge, unter  $N_j$  die Anzahl der Lösungen in diesem Intervall verstanden.

Sei

$$z = \prod_{\tau=1}^t \max(1, |\zeta_{\tau}|_{P_{\tau}})$$



und alsdann

$$\zeta^* = z\zeta, \quad \zeta_\tau^* = z\zeta_\tau \quad (\tau = 1, 2, \dots, t).$$

Wie in 4. zeigt man, dass  $q$  ein ganzes Vielfaches

$$q = zq^*$$

von  $z$  sein muss. Die Menge  $M_j$  ist daher eindeutig bezogen auf die Menge der Paare ganzer rationaler Zahlen  $p, q^*$  mit

$$\left| \frac{p}{q^*} - \zeta^* \right| \prod_{\tau=1}^t |p - q^* \zeta_\tau^*|_{P_\tau} \leq kz |p, zq^*|^{-\beta}, \quad a_j \leq |p, zq^*| < a_{j+1},$$

$$\left| \frac{p}{q^*} - \zeta^* \right| < z, \quad |p - q^* \zeta_\tau^*|_{P_\tau} < 1 \quad (\tau = 1, 2, \dots, t),$$

$$\prod_{\tau=1}^t |p - q^* \zeta_\tau^*|_{P_\tau} > k |p, zq^*|^{-\beta},$$

und hat gleiche Elementenzahl. Folglich ist erst recht  $N_j$  höchstens gleich der Anzahl der Paare ganzer rationaler Zahlen  $p, q$  mit

$$(I): \quad \left| \frac{p}{q} - \zeta^* \right| \prod_{\tau=1}^t |p - q \zeta_\tau^*|_{P_\tau} \leq \frac{kz}{a_j^\beta}, \quad |p| < a_{j+1}, \quad |q| < a_{j+1},$$

$$\left| \frac{p}{q} - \zeta^* \right| < z, \quad |p - q \zeta_\tau^*|_{P_\tau} < 1 \quad (\tau = 1, 2, \dots, t),$$

$$\prod_{\tau=1}^t |p - q \zeta_\tau^*|_{P_\tau} > \frac{k}{a_{j+1}^\beta}.$$

Bedeute  $P_\sigma$  die grösste der Primzahlen  $P_1, P_2, \dots, P_t$  und

$$\mathbf{Q} = \{Q_1, Q_2, \dots, Q_r\}$$

die Menge der Potenzprodukte

$$Q = P_1^{h_1} P_2^{h_2} \dots P_t^{h_t},$$

deren Exponenten natürliche Zahlen sind und die der Ungleichung

$$Q < \frac{a_{j+1}^\beta}{kz}$$

genügen; wie in 4. zeigt man, dass  $\mathbf{Q}$  nicht mehr als

$$\left( \frac{\log (4^{\frac{\beta}{2}-2} k^{\frac{2}{\beta-2}} / z)}{\log 2} \right)^t$$

Elemente enthält.

Aus den letzten Ungleichungen des Bedingungssystem (I) folgt, dass zu jedem Lösungspaar  $p, q$  ein Potenzprodukt  $Q$  aus  $\mathbf{Q}$  gehört, so dass

$$|p - q\zeta_\tau^*|_{P_\tau} = |Q|_{P_\tau}, \quad p \equiv q\zeta_\tau^* \pmod{|Q|_{P_\tau}^{-1}} \quad (\tau = 1, 2, \dots, t),$$

ist. Versteht man unter  $Z$  diejenige ganze rationale Zahl mit

$$0 \leq Z \leq Q - 1, \quad Z \equiv \zeta_\tau^* \pmod{|Q|_{P_\tau}^{-1}} \quad (\tau = 1, 2, \dots, t),$$

so befriedigen  $p, q$  daher die Kongruenz

$$p \equiv qZ \pmod{Q}$$

und es gibt eine ganze rationale Zahl  $r$  mit

$$p = Zq - Qr.$$

Aus (I) und

$$\prod_{\tau=1}^t |p - q\zeta_\tau^*|_{P_\tau} = \prod_{\tau=1}^t |Q|_{P_\tau} = \frac{1}{Q}$$

ergibt sich aber

$$\left| \frac{p}{q} - \zeta^* \right| \leq \frac{kQz}{a_j^\beta},$$

und wenn  $p$  eliminiert wird:

$$\frac{1}{Q} \left| \frac{Zq - Qr}{q} - \zeta^* \right| = \left| \frac{r}{q} - \frac{Z - \zeta^*}{Q} \right| \leq \frac{kz}{a_j^\beta}.$$

Bezeichnet jetzt  $N_j(Q)$  die Anzahl der Lösungspaare  $q, r$  von

$$(II): \quad \left| \frac{r}{q} - \frac{Z - \zeta^*}{Q} \right| \leq \frac{kz}{a_j^\beta}, \quad |q| < a_{j+1},$$

so ist also

$$N_j \leq \sum_{\mathbf{Q}} N_j(Q) \leq \left( \frac{\log (4^{\frac{\beta}{2}-2} k^{\frac{2}{\beta-2}} / z)}{\log 2} \right)^t \max_{\mathbf{Q}} N_j(Q),$$

wobei sich die beiden Zeichen  $\sum_Q$  und  $\max_Q$  auf die Gesamtheit der Elemente  $Q$  aus  $\mathfrak{Q}$  beziehen.

7. Die Anzahl  $N_j(Q)$  der Lösungen von (II) wird durch ein ähnliches Verfahren abgeschätzt, wie in den bisherigen Paragraphen.

Sei zur Abkürzung

$$\zeta^{**} = \frac{Z - \zeta^*}{Q}$$

und  $\alpha \geq 1$  eine positive Zahl, über die nachher verfügt wird. Dann seien

$$\frac{\mathfrak{R}_{f-1}}{\mathfrak{D}_{f-1}}, \frac{\mathfrak{R}_f}{\mathfrak{D}_f}, \frac{\mathfrak{R}_{f+1}}{\mathfrak{D}_{f+1}}$$

drei auf einander folgende Kettenbruch-Näherungsbrüche für  $\zeta^{**}$ , die der Bedingung

$$\mathfrak{D}_f \leq 2^{\alpha j} k^{\beta-1} < \mathfrak{D}_{f+1}$$

genügen. Es gilt also

$$\mathfrak{R}_{f-1}\mathfrak{D}_f - \mathfrak{R}_f\mathfrak{D}_{f-1} = \mp 1,$$

$$\left| \frac{\mathfrak{R}_f}{\mathfrak{D}_f} - \zeta^{**} \right| \leq \frac{1}{\mathfrak{D}_f\mathfrak{D}_{f+1}}.$$

Nach (II) und auf Grund der Identität

$$r\mathfrak{D}_f - q\mathfrak{R}_f = q\mathfrak{D}_f \left( \frac{r}{q} - \zeta^{**} \right) - q\mathfrak{D}_f \left( \frac{\mathfrak{R}_f}{\mathfrak{D}_f} - \zeta^{**} \right)$$

ist demnach

$$|r\mathfrak{D}_f - q\mathfrak{R}_f| \leq \frac{2\mathfrak{D}_f k z}{a_j^{\beta-1}} + \frac{2a_j}{\mathfrak{D}_{f+1}} \leq \frac{2\mathfrak{D}_f k z}{a_j^{\beta-1}} + 2.$$

Jedem Lösungspaar  $q, r$  von (II) werde jetzt durch

$$r = \mathfrak{R}_{f-1}p + \mathfrak{R}_f q$$

$$q = \mathfrak{D}_{f-1}p + \mathfrak{D}_f q$$

ein Zahlpaar  $p, q$  zugeordnet; da diese linearen Gleichungen die Determinante  $\mp 1$  haben, so sind  $p, q$  eindeutig bestimmt und wieder ganz rational. Wegen

$$r\mathfrak{D}_f - q\mathfrak{R}_f = p(\mathfrak{R}_{f-1}\mathfrak{D}_f - \mathfrak{R}_f\mathfrak{D}_{f-1}) = \mp p$$

muss sein:

$$|p| \leq \frac{2\mathfrak{D}_f kz}{a_j^{\beta-1}} + 2,$$

so dass  $p$  höchstens

$$\frac{4\mathfrak{D}_f kz}{a_j^{\beta-1}} + 5$$

Möglichkeiten hat. Weiter gilt

$$|q| = |\mathfrak{D}_{f-1} p + \mathfrak{D}_f q| < a_{j+1} \leq 2a_j;$$

zu jedem Wert von  $p$  lassen sich also höchstens

$$\frac{4a_j}{\mathfrak{D}_f} + 1$$

verschiedene Werte von  $q$  angeben. Somit folgt:

$$N_j(Q) \leq \left( \frac{4\mathfrak{D}_f kz}{a_j^{\beta-1}} + 5 \right) \left( \frac{4a_j}{\mathfrak{D}_f} + 1 \right) = \frac{16kz}{a_j^{\beta-2}} + \frac{4\mathfrak{D}_f kz}{a_j^{\beta-1}} + \frac{20a_j}{\mathfrak{D}_f} + 5.$$

Hier ist für die zwei ersten Summanden

$$\frac{16kz}{a_j^{\beta-2}} = \frac{16zk^{\frac{1}{\beta-1}}}{2^{(\beta-2)j}}, \quad \frac{4\mathfrak{D}_f kz}{a_j^{\beta-1}} \leq \frac{4zk^{\frac{1}{\beta-1}}}{2^{(\beta-1-a)j}},$$

damit der zweite hiervon für wachsendes  $j$  wie das Glied einer geometrischen Reihe gegen Null strebt, möge weiterhin

$$\alpha < \beta - 1$$

angenommen werden.

Es bleibt noch übrig, den Summanden

$$\frac{20a_j}{\mathfrak{D}_f}$$

nach oben abzuschätzen, indem man eine untere Schranke für  $\mathfrak{D}_f$  herleitet. Sei zur Abkürzung

$$\mathfrak{P}_f = Z\mathfrak{D}_f - Q\mathfrak{R}_f.$$

Der grösste gemeinschaftliche Teiler

$$d = (\mathfrak{P}_f, \mathfrak{D}_f)$$

von  $\mathfrak{R}_f$  und  $\mathfrak{D}_f$  ist wegen der Teilerfremdheit von  $\mathfrak{D}_f$  und  $\mathfrak{R}_f$  ein Potenzprodukt allein der Primzahlen  $P_1, P_2, \dots, P_t$ .

Man hat

$$\mathfrak{R}_f - \mathfrak{D}_f \zeta^{**} = \mathfrak{R}_f - \mathfrak{D}_f \frac{Z - \zeta^*}{Q} = \frac{\mathfrak{R}_f Q - \mathfrak{D}_f Z + \mathfrak{D}_f \zeta^*}{Q} = \frac{\mathfrak{D}_f \zeta^* - \mathfrak{R}_f}{Q},$$

wegen

$$|\mathfrak{R}_f - \mathfrak{D}_f \zeta^{**}| \leq \frac{1}{\mathfrak{D}_{f+1}}$$

also

$$|\mathfrak{D}_f \zeta^* - \mathfrak{R}_f| \leq \frac{Q}{\mathfrak{D}_{f+1}}$$

Andrerseits ist nach Definition von  $\mathfrak{R}_f$

$$\prod_{\tau=1}^t |\mathfrak{R}_f - \mathfrak{D}_f \zeta_\tau^*|_{P_\tau} \leq \prod_{\tau=1}^t |Q|_{P_\tau} = \frac{1}{Q}.$$

Somit muss

$$\left| \frac{\mathfrak{R}_f}{\mathfrak{D}_f} - \zeta^* \right| \prod_{\tau=1}^t |\mathfrak{R}_f - \mathfrak{D}_f \zeta_\tau^*|_{P_\tau} \leq \frac{1}{\mathfrak{D}_f \mathfrak{D}_{f+1}},$$

und wenn

$$\mathfrak{R}_f = d\mathfrak{R}, \quad \mathfrak{D}_f = d\mathfrak{D}$$

gesetzt wird, auch

$$\left| \frac{\mathfrak{R}}{\mathfrak{D}} - \zeta^* \right| \prod_{\tau=1}^t |\mathfrak{R} - \mathfrak{D} \zeta_\tau^*|_{P_\tau} \leq \frac{d}{\mathfrak{D}_f \mathfrak{D}_{f+1}}$$

sein. Die Verallgemeinerung des Thue-Siegelschen Satzes erlaubt, für die linke Seite dieser Ungleichung auch eine untere Schranke herzuleiten. Um zu einem möglichst guten Ergebnis zu kommen, muss man dabei aber zwei Fälle unterscheiden.

Es möge erstens gelten:

$$|\mathfrak{R}_f| \geq \max(1, 2|\zeta^*|) \mathfrak{D}_f,$$

also

$$\left| \frac{\mathfrak{R}}{\mathfrak{D}} - \zeta^* \right| = \left| \frac{\mathfrak{R}_f}{\mathfrak{D}_f} - \zeta^* \right| \geq \frac{1}{2} \frac{|\mathfrak{R}_f|}{\mathfrak{D}_f}, \quad |\mathfrak{R}, \mathfrak{D}| \leq |\mathfrak{R}| = \frac{1}{d} |\mathfrak{R}_f|.$$

Nach Satz 1, (1) gibt es eine positive Konstante

$$c'_0 = c'_0(\zeta_1^*, \zeta_2^*, \dots, \zeta_t^*),$$

so dass wegen der Teilerfremdheit von  $\mathfrak{P}$  und  $\mathfrak{Q}$

$$\prod_{\tau=1}^t |\mathfrak{P} - \mathfrak{Q} \zeta_{\tau}^*|_{P_{\tau}} \geq c'_0 |\mathfrak{P}, \mathfrak{Q}|^{-\beta} \geq c'_0 d^{\beta} |\mathfrak{P}_f|^{-\beta}$$

und also

$$\left| \frac{\mathfrak{P}}{\mathfrak{Q}} - \zeta^* \right| \prod_{\tau=1}^t |\mathfrak{P} - \mathfrak{Q} \zeta_{\tau}^*|_{P_{\tau}} \geq \frac{c'_0 d^{\beta} |\mathfrak{P}_f|^{1-\beta}}{2 \mathfrak{Q}_f}$$

ist. Es muss demnach in diesem Fall

$$\frac{d}{\mathfrak{Q}_f \mathfrak{Q}_{f+1}} \geq \frac{c'_0 d^{\beta} |\mathfrak{P}_f|^{1-\beta}}{2 \mathfrak{Q}_f}$$

oder

$$|\mathfrak{P}_f|^{\beta-1} \geq \frac{c'_0 d^{\beta-1}}{2} \mathfrak{Q}_{f+1} \geq \frac{c'_0}{2} \mathfrak{Q}_{f+1}$$

sein, wegen

$$\mathfrak{Q}_{f+1} \geq 2^{\alpha j} k^{\frac{1}{\beta-1}}$$

somit

$$|\mathfrak{P}_f| \geq \left( \frac{c'_0}{2} \right)^{\frac{1}{\beta-1}} 2^{\frac{\alpha}{\beta-1} j} k^{\frac{1}{(\beta-1)^2}}.$$

Andrerseits ist

$$|\mathfrak{P}_f - \mathfrak{Q}_f \zeta^*| \leq \frac{Q}{\mathfrak{Q}_{f+1}}$$

und

$$Q \leq \frac{a_{j+1}^{\beta}}{kz} \leq \frac{2^{\beta}}{z} 2^{\beta j} k^{\frac{1}{\beta-1}},$$

so dass

$$|\mathfrak{P}_f| \leq |\zeta^*| \mathfrak{Q}_f + \frac{2^{\beta}}{z} 2^{(\beta-\alpha)j}$$

folgt. Wir werden jetzt zeigen, dass sich die Zahl  $\alpha$  in erlaubter Weise derart in der Form

$$\alpha = \beta - 1 - \varepsilon, \quad 0 < \varepsilon \leq \beta - 2,$$

wählen lässt, so dass für alle Werte  $j \leq g - 1$  und für alle genügend grossen positiven Zahlen  $k$

$$\frac{2^\beta}{\varepsilon} 2^{(\beta-\alpha)j} < \frac{1}{2} \left(\frac{c'_0}{2}\right)^{\frac{1}{\beta-1}} 2^{\frac{\alpha}{\beta-1}j} \frac{1}{k^{(\beta-1)^2}}$$

ist; dann muss also

$$|\mathfrak{R}_f| < 2 |\zeta^*| \mathfrak{Q}_f \leq \max(1, 2 |\zeta^*|) \mathfrak{Q}_f$$

sein, gegen unsere Annahme

$$|\mathfrak{R}_f| \geq \max(1, 2 |\zeta^*|) \mathfrak{Q}_f$$

die also alsdann nie erfüllt sein kann. Zum Beweis genügt es zu zeigen, dass sich immer

$$2^{(\beta-\alpha-\frac{\alpha}{\beta-1})j} < \frac{\varepsilon}{2^{\beta+1}} \left(\frac{c'_0}{2}\right)^{\frac{1}{\beta-1}} \frac{1}{k^{(\beta-1)^2}}$$

machen lässt. Wegen  $\alpha = \beta - 1 - \varepsilon$  ist hier

$$\beta - \alpha - \frac{\alpha}{\beta-1} = \frac{\beta}{\beta-1} \varepsilon,$$

wegen

$$2^j k^{\frac{1}{\beta-1}} \leq (4k)^{\frac{1}{\beta-2}}$$

ferner

$$2^j \leq 4^{\frac{1}{\beta-2}} k^{\frac{1}{(\beta-1)(\beta-2)}}.$$

Es genügt also,  $\varepsilon$  so klein zu wählen, dass für alle grossen  $k$

$$\left(\frac{1}{4^{\beta-2}} k^{\frac{1}{(\beta-1)(\beta-2)}}\right)^{\beta} \beta^{-1} \varepsilon < \frac{\varepsilon}{2^{\beta+1}} \left(\frac{c'_0}{2}\right)^{\frac{1}{\beta-1}} \frac{1}{k^{(\beta-1)^2}}$$

ist, und dazu ist offenbar hinreichend, die wegen  $\beta > 2$  erlaubte Wahl

$$\varepsilon \leq \frac{1}{2} \frac{\beta-2}{\beta(\beta-1)^2} \leq \beta-2$$

zu treffen.

Es gelte zweitens

$$|\mathfrak{R}_f| \leq \max(1, 2 |\zeta^*|) \mathfrak{Q}_f;$$

wie gerade gezeigt wurde, liegt in dieser Annahme in Wirklichkeit keine Einschränkung. Es ist somit

$$|\mathfrak{R}, \mathfrak{Q}| = \frac{1}{d} |\mathfrak{R}_f, \mathfrak{Q}_f| \leq \frac{1}{d} \max(1, 2 |\zeta^*|) \mathfrak{Q}_f.$$

Nach Satz 1, (1) gibt es eine positive Konstante

$$c'' = c''(\zeta^*, \zeta_1^*, \zeta_2^*, \dots, \zeta_t^*),$$

so dass wegen der Teilerfremdheit von  $\mathfrak{P}$  und  $\mathfrak{Q}$

$$\left| \frac{\mathfrak{P}}{\mathfrak{Q}} - \zeta^* \prod_{\tau=1}^t |\mathfrak{P} - \mathfrak{Q} \zeta_\tau^*|_{p_\tau} \right| \geq c'' |\mathfrak{P}, \mathfrak{Q}|^{-\beta} \geq \frac{c'' d^\beta}{c^\beta} \mathfrak{Q}_f^{-\beta},$$

$$c = \max(1, 2 |\zeta^*|),$$

ist. Diesmal folgt also

$$\frac{d}{\mathfrak{Q}_f \mathfrak{Q}_{f+1}} \geq \frac{c'' d^\beta}{c^\beta} \mathfrak{Q}_f^{-\beta},$$

oder

$$\mathfrak{Q}_f^{\beta-1} \geq \frac{c'' d^{\beta-1}}{c^\beta} \mathfrak{Q}_{f+1} \geq \frac{c''}{c^\beta} \mathfrak{Q}_{f+1}.$$

Wegen

$$\mathfrak{Q}_{f+1} > 2^{\alpha j} k^{\frac{1}{\beta-1}}$$

kommt man also zu

$$\mathfrak{Q}_f \geq \left( \frac{c''}{c^\beta} \right)^{\frac{1}{\beta-1}} 2^{\frac{\alpha}{\beta-1} j} k^{\frac{1}{(\beta-1)^2}}, \quad \alpha = \beta - 1 - \varepsilon$$

und von hier aus zu

$$\frac{20 a_j}{\mathfrak{Q}_f} \leq 20 \left( \frac{c''}{c^\beta} \right)^{\frac{1}{\beta-1}} 2^{\frac{\varepsilon}{\beta-1} j} k^{\frac{1}{\beta-1} - \frac{1}{(\beta-1)^2}}.$$

Wegen

$$2^j \leq 4^{\frac{1}{\beta-2}} k^{\frac{1}{(\beta-1)(\beta-2)}}$$

lässt sich hier ohne Widerspruch zu der früheren Ungleichung

$$\varepsilon \leq \frac{\beta - 2}{2\beta(\beta - 1)^2}$$

die Zahl  $\varepsilon$  so klein annehmen, dass für alle hinreichend grossen  $k$

$$\frac{20 a_j}{\mathfrak{Q}_f} \leq k^{\frac{1}{\beta-1} - \vartheta}$$

ist; dabei bedeutet  $\vartheta$  eine sehr kleine positive Zahl, die von  $\varepsilon$  abhängt und auf deren genauen Wert es offenbar nicht ankommt.



Damit ist schliesslich die Ungleichung

$$N_j(Q) \leq \frac{16z k^{\frac{1}{\beta-1}}}{2^{(\beta-2)j}} + \frac{4z k^{\frac{1}{\beta-1}}}{2^{\varepsilon j}} + k^{\frac{1}{\beta-1}-g} + 5$$

bewiesen; weil auf ihrer rechten Seite  $Q$  nicht auftritt, folgt weiter

$$N_j \leq \left( \frac{\log(4^{\frac{\beta}{\beta-2}} k^{\frac{2}{\beta-2}}/z)}{\log 2} \right)^t \left( \frac{16z k^{\frac{1}{\beta-1}}}{2^{(\beta-2)j}} + \frac{4z k^{\frac{1}{\beta-1}}}{2^{\varepsilon j}} + k^{\frac{1}{\beta-1}-g} + 5 \right).$$

Wie aber zu Anfang des Beweises festgestellt wurde, hat das Bedingungs-  
system  $a(1, t)$  gerade

$$N = \sum_{j=0}^{g-1} N_j + O(k^{\frac{1}{\beta-1}} (\log k)^t)$$

Lösungspaare. Da nun die beiden geometrischen Reihen

$$\sum_{j=0}^{g-1} \frac{16z}{2^{(\beta-2)j}}, \quad \sum_{j=0}^{g-1} \frac{4z}{2^{\varepsilon j}}$$

unterhalb einer von  $k$  unabhängigen Schranke bleiben und da

$$g = O(\log k)$$

ist, so ergibt sich schliesslich

$$N = O((\log k)^t) \{ O(k^{\frac{1}{\beta-1}}) + O(k^{\frac{1}{\beta-1}}) + O(k^{\frac{1}{\beta-1}-g} \log k) + O(\log k) \} + \\ + O(k^{\frac{1}{\beta-1}} (\log k)^t) = O(k^{\frac{1}{\beta-1}} (\log k)^t),$$

und das sollte gerade bewiesen werden.

8. Die Sätze 3—5, die in den letzten Paragraphen abgeleitet wurden, lassen sich zusammenfassen zu folgender Aussage:

**1. Hauptsatz:** *Bedeute*

$f(x)$  ein irreduzibles Polynom mit ganzen rationalen Koeffizienten vom Grad  $n \geq 3$ ,

$\zeta, \zeta', \dots, \zeta^{(v-1)}$  die sämtlichen reellen Nullstellen von  $f(x)$ , falls solche existieren, und  $v$  ihre Anzahl,

$P_1, P_2, \dots, P_t$  endlichviele verschiedene Primzahlen,

$\zeta_\tau, \zeta'_\tau, \dots, \zeta_\tau^{(v_\tau-1)}$  für  $\tau = 1, 2, \dots, t$  die sämtlichen  $P_\tau$ -adischen Nullstellen von  $f(x)$ , falls solche existieren, und  $v_\tau$  ihre Anzahl,

$t_0$  die Anzahl der Zahlen  $v, v_1, \dots, v_t$ , die nicht den Wert Null haben,

$\beta$  eine Zahl im Intervall  $\min_{s=1, 2, \dots, t-1} \left( \frac{n}{s+1} + s \right) < \beta \leq n$ ,

$k$  eine über alle Grenzen wachsende positive Zahl,

$p$  und  $q$  zwei ganze rationale Zahlen mit  $q \neq 0$ .

Wird dann unter dem Ausdruck

$$\min \left( 1, \left| \frac{p}{q} - \zeta \right|, \left| \frac{p}{q} - \zeta' \right|, \dots, \left| \frac{p}{q} - \zeta^{(v-1)} \right| \right),$$

bzw. unter den Ausdrücken

$$\min (1, |p - q\zeta_\tau|_{P_\tau}, |p - q\zeta'_\tau|_{P_\tau}, \dots, |p - q\zeta_\tau^{(v_\tau-1)}|_{P_\tau}) \quad (\tau = 1, 2, \dots, t)$$

die Eins verstanden, falls die zugehörige Anzahl  $v$ , bzw.  $v_\tau$ , verschwinden sollte, so besitzt das Bedingungssystem

$$(f): \quad \min \left( 1, \left| \frac{p}{q} - \zeta \right|, \left| \frac{p}{q} - \zeta' \right|, \dots, \left| \frac{p}{q} - \zeta^{(v-1)} \right| \right) \times \\ \times \prod_{\tau=1}^t \min (1, |p - q\zeta_\tau|_{P_\tau}, |p - q\zeta'_\tau|_{P_\tau}, \dots, |p - q\zeta_\tau^{(v_\tau-1)}|_{P_\tau}) \leq k |p, q|^{-\beta},$$

$$|p, q| \geq k^{\frac{1}{\beta-1}}, \quad (p, q, P_1 P_2 \dots P_t) = 1$$

im Fall  $t_0 = 0$  keine, im Fall  $t_0 \geq 1$  höchstens

$$O(k^{\frac{1}{\beta-1}} (\log k)^{t_0-1})$$

Lösungspaare  $p, q$ , falls  $k$  hinreichend gross ist.

**Beweis:** Für  $t_0 = 0$  ist die Behauptung trivial. Ist dagegen  $t_0 \geq 1$ , so genügt jede Lösung von (f) einer Ungleichung von einem der Typen

$$\left| \frac{p}{q} - \zeta^{(u)} \right| \leq k |p, q|^{-\beta}$$

oder

$$\prod_{\sigma=1}^{t'} |p - q\zeta_{\tau_\sigma}^{(\mu_{\tau_\sigma})}|_{P_{\tau_\sigma}} \leq k |p, q|^{-\beta}, \\ |p - q\zeta_{\tau_\sigma}^{(\mu_{\tau_\sigma})}|_{P_{\tau_\sigma}} < 1 \quad (\sigma = 1, 2, \dots, t')$$

oder

$$\left| \frac{p}{q} - \zeta^{(\mu)} \right| \prod_{\sigma=1}^{t'} |p - q \zeta_{\sigma}^{(\mu_{\sigma})}|_{P_{\sigma}} \leq k |p, q|^{-\beta},$$

$$\left| \frac{p}{q} - \zeta^{(\mu)} \right| < 1, \quad |p - q \zeta_{\sigma}^{(\mu_{\sigma})}|_{P_{\sigma}} < 1 \quad (\sigma = 1, 2, \dots, t'),$$

wie sie in den Sätzen 3—5 auftraten. Ferner ist die Bedingung

$$(p, q, P_1 P_2 \dots P_t) = 1$$

um so enger, je mehr Primzahlen in ihr vorkommen. Folglich ist jede Lösung von (f) Lösung eines Bedingungssystems  $(1, 0)$  oder  $(0, t')$  oder  $(1, t')$ , wobei  $t'$  höchstens gleich der Anzahl der Nichtverschwindenden unter den Zahlen  $\nu_1, \nu_2, \dots, \nu_t$  ist und für  $\nu = 0$  kein Bedingungssystem der Form  $(1, 0)$  oder  $(1, t')$  auftreten kann. Daraus folgt nach früher die Behauptung.

**Zusatz:** Auch das allgemeinere Bedingungssystem

$$(f'): \min \left( 1, \left| \frac{p}{q} - \zeta \right|, \left| \frac{p}{q} - \zeta' \right|, \dots, \left| \frac{p}{q} - \zeta^{(v-1)} \right| \right) \times$$

$$\times \prod_{\tau=1}^t \min (1, |p - q \zeta_{\tau}|_{P_{\tau}}, |p - q \zeta'_{\tau}|_{P_{\tau}}, \dots, |p - q \zeta_{\tau}^{(v_{\tau}-1)}|_{P_{\tau}}) \leq \frac{Ck}{|p, q|^{\beta}},$$

$$|p, q| \geq k^{\frac{1}{\beta-1}}, \quad (p, q, P_1 P_2 \dots P_t) = 1,$$

wo  $C$  irgend eine positive Konstante bedeutet, die von  $k$  nicht abhängt, hat für  $t_0 = 0$  keine und für  $t_0 \geq 1$  höchstens

$$O(k^{\frac{1}{\beta-1}} (\log k)^{t_0-1})$$

Lösungspaare  $p, q$ , falls  $k$  hinreichend gross ist.

In der Tat zeigt eine einfache Durchsicht der Beweise der Sätze 3—5, dass diese Sätze unverändert richtig bleiben, wenn in ihnen die Forderungen

$$\left| \frac{p}{q} - \zeta \right| \leq k |p, q|^{-\beta},$$

bzw. . . 
$$\prod_{\tau=1}^t |p - q \zeta_{\tau}|_{P_{\tau}} \leq k |p, q|^{-\beta},$$

bzw. 
$$\left| \frac{p}{q} - \zeta \right| \prod_{\tau=1}^t |p - q \zeta_{\tau}|_{P_{\tau}} \leq k |p, q|^{-\beta}$$

der Reihe nach ersetzt werden durch

$$\left| \frac{p}{q} - \zeta \right| \leq Ck |p, q|^{-\beta},$$

bzw. 
$$\prod_{\tau=1}^t |p - q\zeta_{\tau}|_{P_{\tau}} \leq Ck |p, q|^{-\beta},$$

bzw. 
$$\left| \frac{p}{q} - \zeta \right| \prod_{\tau=1}^t |p - q\zeta_{\tau}|_{P_{\tau}} \leq Ck |p, q|^{-\beta}.$$

Auch der Hauptsatz muss also diese Verallgemeinerung zulassen.

Zum Schluss dieses Kapitels sei noch erwähnt, dass man für die Anzahl der Lösungspaare  $p, q$  des Bedingungssystems

$$\begin{aligned} \min \left( 1, \left| \frac{p}{q} - \zeta \right|, \left| \frac{p}{q} - \zeta' \right|, \dots, \left| \frac{p}{q} - \zeta^{(r-1)} \right| \right) \times \\ \times \prod_{\tau=1}^t \min (1, |p - q\zeta_{\tau}|_{P_{\tau}}, |p - q\zeta'_{\tau}|_{P_{\tau}}, \dots, |p - q\zeta_{\tau}^{(r-1)}|_{P_{\tau}}) \leq k |p, q|^{-\beta}, \\ (p, q, P_1 P_2 \dots P_t) = 1 \end{aligned}$$

oder auch des Bedingungssystems

$$\begin{aligned} \min \left( 1, \left| \frac{p}{q} - \zeta \right|, \left| \frac{p}{q} - \zeta' \right|, \dots, \left| \frac{p}{q} - \zeta^{(r-1)} \right| \right) \times \\ \times \prod_{\tau=1}^t \min (1, |p - q\zeta_{\tau}|_{P_{\tau}}, |p - q\zeta'_{\tau}|_{P_{\tau}}, \dots, |p - q\zeta_{\tau}^{(r-1)}|_{P_{\tau}}) \leq k |p, q|^{-\beta}, \\ (p, q) = 1 \end{aligned}$$

eine asymptotische Formel aufstellen kann, falls  $k > 0$  über alle Grenzen zunimmt. Man muss zu diesem Zweck ein ähnliches Verfahren wie in den folgenden Kapiteln anwenden und sich elementarer Gitterpunktsüberlegungen bedienen. Die Durchführung dieser Untersuchung bleibe dem Leser überlassen.

## II.

9. Die Ergebnisse des ersten Kapitels wurden hergeleitet, um sie auf die *Theorie der Binärformen* anzuwenden; alsdann wird immer  $\beta$  den Wert  $n$  haben. Bevor jedoch zu diesen Anwendungen übergegangen werden kann, müssen einige einfachen Kongruenzeigenschaften dieser Formen besprochen werden.

Sei  $F(x, y)$  eine irreduzible Binärform mit ganzen rationalen Koeffizienten vom Grad  $n \geq 3$ ; ferner bedeute wieder  $P_1, P_2, \dots, P_t$  endlichviele verschiedene Primzahlen. Unter  $p, q$  seien ganze rationale Zahlen mit

$$(p, q, P_1 P_2 \dots P_t) = 1$$

verstanden; für solche Zahlpaare werde

$$Q(p, q) = \left( \prod_{\tau=1}^t |F(p, q)|_{P_\tau} \right)^{-1}$$

gesetzt, so dass also  $Q(p, q)$  das grösste Potenzprodukt der Primzahlen  $P_1, P_2, \dots, P_t$  ist, das in  $F(p, q)$  aufgeht. Es bezeichne  $m(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})$  die Menge aller Paare  $p, q$  mit

$$\begin{aligned} 0 \leq p \leq P_1^{h_1+1} P_2^{h_2+1} \dots P_t^{h_t+1} - 1, \quad 0 \leq q \leq P_1^{h_1+1} P_2^{h_2+1} \dots P_t^{h_t+1} - 1, \\ Q(p, q) = P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}, \quad (p, q, P_1 P_2 \dots P_t) = 1 \end{aligned}$$

und  $m^*(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})$  die Menge dieser Paare mit

$$\begin{aligned} 0 \leq p \leq P_1^{h_1+1} P_2^{h_2+1} \dots P_t^{h_t+1} - 1, \quad 0 \leq q \leq P_1^{h_1+1} P_2^{h_2+1} \dots P_t^{h_t+1} - 1, \\ Q(p, q) \equiv 0 \pmod{P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}}, \quad (p, q, P_1 P_2 \dots P_t) = 1, \end{aligned}$$

ferner  $n(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})$  und  $n^*(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})$  die Anzahl der Elemente dieser beiden Mengen.

10. Sind  $p, q$  zwei ganze rationale Zahlen mit

$$0 \leq p \leq P_1^{h_1+1} P_2^{h_2+1} \dots P_t^{h_t+1} - 1, \quad 0 \leq q \leq P_1^{h_1+1} P_2^{h_2+1} \dots P_t^{h_t+1} - 1,$$

so lassen sich hierzu immer  $t$  Paare ganzer rationaler Zahlen

$$p_1, q_1; p_2, q_2; \dots; p_t, q_t$$

in eindeutiger Weise bestimmen, so dass

$$0 \leq p_\tau \leq P_\tau^{h_\tau+1} - 1, \quad 0 \leq q_\tau \leq P_\tau^{h_\tau+1} - 1 \quad (\tau = 1, 2, \dots, t)$$

ist und die Kongruenzen

$$p \equiv p_\tau \pmod{P_\tau^{h_\tau+1}}, \quad q \equiv q_\tau \pmod{P_\tau^{h_\tau+1}} \quad (\tau = 1, 2, \dots, t)$$

bestehen. Somit ist auch

$$(p, q, P_1 P_2 \dots P_t) = \prod_{\tau=1}^t (p, q, P_\tau) = \prod_{\tau=1}^t (p_\tau, q_\tau, P_\tau),$$

und die Gleichung

$$(p, q, P_1 P_2 \dots P_t) = 1$$

zieht die  $t$  Gleichungen

$$(p_\tau, q_\tau, P_\tau) = 1$$

nach sich und ist umgekehrt eine Folge aus diesen. Auf Grund der Taylorschen Reihenentwicklung bestehen ferner die Kongruenzen

$$F(p, q) \equiv F(p_\tau, q_\tau) \pmod{P_\tau^{h_\tau+1}} \quad (\tau = 1, 2, \dots, t);$$

aus der Gleichung

$$Q(p, q) = P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}$$

folgen demnach die  $t$  Gleichungen

$$|F(p_\tau, q_\tau)|_{P_\tau} = P_\tau^{-h_\tau} \quad (\tau = 1, 2, \dots, t),$$

die umgekehrt zu ihr zurückführen. Ebenso folgen aus der Beziehung

$$Q(p, q) \equiv 0 \pmod{P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}}$$

die  $t$  Beziehungen

$$|F(p_\tau, q_\tau)|_{P_\tau} \leq P_\tau^{-h_\tau} \quad (\tau = 1, 2, \dots, t),$$

und sie sind ihrerseits wieder eine Folge aus den letzteren.

Damit ist der Beweis erbracht, dass sich die Menge

$$m(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}),$$

bzw. die Menge

$$m^*(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})$$

umkehrbar eindeutig abbilden lässt auf das Produkt der  $t$  Mengen

$$m(P_1^{h_1}), m(P_2^{h_2}), \dots, m(P_t^{h_t}),$$

bzw. auf das Produkt der  $t$  Mengen

$$m^*(P_1^{h_1}), m^*(P_2^{h_2}), \dots, m^*(P_t^{h_t}).$$

Durch Übergang zu den Elementen-Anzahlen ergibt sich demnach

$$n(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}) = \prod_{\tau=1}^t n(P_\tau^{h_\tau}),$$

$$n^*(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}) = \prod_{\tau=1}^t n^*(P_\tau^{h_\tau}).$$

Es genügt also, allein die Mengen

$$m(P^h) \text{ und } m^*(P^h)$$

und die Anzahlen

$$n(P^h) \text{ und } n^*(P^h),$$

die sich auf eine einzige Primzahl  $P$  beziehen, zu untersuchen.

II. Unter den Paaren ganzer rationaler Zahlen  $p, q$  mit

$$0 \leq p \leq P^{h+1} - 1, \quad 0 \leq q \leq P^{h+1} - 1$$

genügen offenbar genau

$$(P^2 - 1) P^{2h}$$

der Bedingung

$$(p, q, P) = 1.$$

Die Menge der so bestimmten Paare werde in  $h + 1$  Teilmengen

$$m_\varrho \quad (\varrho = 0, 1, \dots, h-1) \text{ und } m_h^*$$

zerlegt, jenachdem

$$|F(p, q)|_P = P^{-\varrho} \quad (\varrho = 0, 1, \dots, h-1) .$$

oder

$$|F(p, q)|_P \leq P^{-h}$$

ist. Die Menge  $m_h^*$  ist offenbar mit  $m^*(P^h)$  identisch, die Anzahl ihrer Elemente demnach gleich

$$n^*(P^h).$$

Sei dagegen  $\varrho$  einer der Indizes  $0, 1, \dots, h-1$ . Jedem Element von  $m_\varrho$  lässt sich dann offenbar durch die Bedingungen

$$\bar{p} \equiv p \pmod{P^{\varrho+1}}, \quad \bar{q} \equiv q \pmod{P^{\varrho+1}}, \quad 0 \leq \bar{p} \leq P^{\varrho+1} - 1, \quad 0 \leq \bar{q} \leq P^{\varrho+1} - 1$$

eindeutig ein Zahlpaar  $\bar{p}, \bar{q}$  aus  $m(P^e)$  zuordnen; umgekehrt entsprechen jedem Element der Menge  $m(P^e)$  durch diese Zuordnung genau  $P^{2(h-e)}$  Elemente aus  $m_0$ . Folglich besitzt  $m_0$  genau

$$n(P^e) P^{2(h-e)}$$

Elemente.

Zählt man die Elementen-Anzahlen der Mengen

$$m_0, m_1, \dots, m_{h-1}, m_h^*$$

zusammen, so erhält man daher die Gleichung

$$\sum_{e=0}^{h-1} n(P^e) P^{2(h-e)} + n^*(P^h) = (P^2 - 1) P^{2h}$$

oder durch Division mit  $P^{2h+2}$ :

$$\sum_{e=0}^{h-1} \frac{n(P^e)}{P^{2e+2}} + \frac{n^*(P^h)}{P^{2h+2}} = 1 - \frac{1}{P^2}.$$

Diese Formel hat eine sehr anschauliche Bedeutung. Es ist

$$d(P^e) = \frac{n(P^e)}{P^{2e+2}}, \quad \text{bzw.} \quad d^*(P^e) = \frac{n^*(P^e)}{P^{2e+2}}$$

offenbar gerade gleich der Dichte der Paare ganzer rationaler Zahlen  $p, q$ , die den beiden Bedingungen

$$|F(p, q)|_P = P^{-e}, \quad (p, q, P) = 1,$$

bzw. den beiden Bedingungen

$$|F(p, q)|_P \leq P^{-h}, \quad (p, q, P) = 1$$

genügen, im Gitter aller Paare ganzer rationaler Zahlen  $p, q$ . Es ist ferner

$$1 - \frac{1}{P^2} = d_0(P)$$

gerade gleich der Dichte der Paare  $p, q$  in diesem Gitter, für die

$$(p, q, P) = 1.$$



Die Formel

$$\sum_{\rho=0}^{h-1} d(P^\rho) + d^*(P^h) = d_0(P)$$

ist also fast trivial; sie besagt eben nur, dass für jedes Zahlpaar  $p, q$  die Funktion  $F(p, q)$  dieses Paares durch eine der Potenzen

$$1, P, P^2, \dots, P^{h-1}$$

oder durch eine noch höhere Potenz genau teilbar ist.

12. Die Anzahl  $n^*(P^h)$  lässt sich für genügend grosses  $h$  explizit angeben. Zu diesem Zweck möge jedem Element  $p, q$  dieser Menge eine nichtnegative ganze rationale Zahl  $f$  durch die Gleichung

$$|q|_P = P^{-f}$$

zugeordnet werden; in

$$q = P^f q_0$$

ist dann also  $q_0$  zu  $P$  teilerfremd und wegen der Voraussetzung

$$0 \leq q \leq P^{h+1} - 1$$

offenbar nur genau

$$(P-1)P^{h-f}$$

verschiedener Werte fähig. Es ist leicht einzusehen, dass  $f$  nach oben beschränkt ist; ist nämlich  $a_0$  der Koeffizient von  $x^n$  der Form  $F(x, y)$ , der wegen der Irreduzibilität dieser Form gewiss nicht verschwindet, und wird

$$|q|_P = P^{-f} < |a_0|_P \leq 1,$$

wegen  $(p, q, P) = 1$  also gleichzeitig

$$p \not\equiv 0 \pmod{P}$$

vorausgesetzt, so gilt offenbar

$$|F(p, q)|_P = |a_0|_P,$$

und das steht für hinreichend grosses  $h$  im Widerspruch zu der Forderung

$$|F(p, q)|_P \leq P^{-h}.$$

Wegen der Homogenität von  $F(x, y)$  gilt für alle Paare  $p, q$  aus  $m^*(P^h)$

$$\left| F\left(\frac{p}{q}, 1\right) \right|_P \leq P^{-h+nf}.$$

Für hinreichend grosses  $h$  ist also nach der eben bewiesenen Beschränktheit von  $f$  die linke Seite beliebig klein. Das ist nach einem grundlegenden Satz aus der Theorie der  $P$ -adischen Zahlen nur dann möglich, wenn  $p/q$  beliebig nahe bei einer  $P$ -adischen Nullstelle von  $F(x, 1)$  liegt, etwa in der Nähe von  $Z$ , und zwar muss von einem  $h$  ab

$$\left| \frac{p}{q} - Z \right|_P < |Z|_P,$$

also

$$\left| \frac{p}{q} \right|_P = |Z|_P \text{ oder } \max(1, |Z|_P) = P^f = \frac{1}{|q|_P}$$

sein. Auf Grund der Taylorschen Reihenentwicklung ist nun

$$F\left(\frac{p}{q}, 1\right) - \left(\frac{p}{q} - Z\right) F'(Z, 1) = \sum_{g=2}^n \frac{1}{g!} \left(\frac{p}{q} - Z\right)^g F^{(g)}(Z, 1),$$

wobei die Akzente die Ableitungen von  $F(x, 1)$  nach  $x$  bedeuten und insbesondere wegen der Irreduzibilität von  $F(x, 1)$

$$F'(Z, 1) \neq 0$$

ist. Setzt man  $h$  hinreichend gross, also

$$\left| F\left(\frac{p}{q}, 1\right) \right|_P \text{ und damit } \left| \frac{p}{q} - Z \right|_P$$

hinreichend klein voraus, so gilt folglich

$$\left| F\left(\frac{p}{q}, 1\right) - \left(\frac{p}{q} - Z\right) F'(Z, 1) \right|_P < \left| \left(\frac{p}{q} - Z\right) F'(Z, 1) \right|_P,$$

und man hat

$$\left| \frac{p}{q} - Z \right|_P = \frac{\left| F\left(\frac{p}{q}, 1\right) \right|_P}{|F'(Z, 1)|_P},$$

wegen

$$\left| F\left(\frac{p}{q}, 1\right) \right|_P \leq P^{-h+nf} = P^{-h} \max(1, |Z|_P)^n$$

also

$$|p - qZ|_P = \frac{\left| F\left(\frac{p}{q}, 1\right) \right|_P}{|F'(Z, 1)|_P} \max(1, |Z|_P)^{-1} \leq P^{-h} \frac{\max(1, |Z|_P)^{n-1}}{|F'(Z, 1)|_P}.$$

Umgekehrt genügt für hinreichend grosses  $h$  jedes Lösungspaar dieser Ungleichung wieder der vorigen Ungleichung. Auf der rechten Seite dieser Ungleichung ist der Faktor

$$\frac{\max(1, |Z|_P)^{n-1}}{|F'(Z, 1)|_P}$$

aber offenbar eine Potenz von  $P$  mit nichtnegativem ganzen rationalen Exponenten, denn man hat

$$\frac{\max(1, |Z|_P)^{n-1}}{|F'(Z, 1)|_P} \geq 1.$$

Zu jedem zulässigen Wert von  $q$  gibt es also genau

$$\frac{\max(1, |Z|_P)^{n-1}}{|F'(Z, 1)|_P} P$$

Zahlen  $p$ , die der Ungleichung

$$|p - qZ|_P \leq P^{-h} \frac{\max(1, |Z|_P)^{n-1}}{|F'(Z, 1)|_P}$$

genügen und die im Intervall

$$0 \leq p \leq P^{h+1} - 1$$

liegen. Das zu der Nullstelle  $Z$  gehörige Bedingungssystem

$$|p - qZ|_P \leq P^{-h} \frac{\max(1, |Z|_P)^{n-1}}{|F'(Z, 1)|_P}, \quad (p, q, P) = 1,$$

$$0 \leq p \leq P^{h+1} - 1, \quad 0 \leq q \leq P^{h+1} - 1$$

hat somit genau

$$\frac{\max(1, |Z|_P)^{n-2}}{|F'(Z, 1)|_P} (P-1) P^{h+1}$$

Lösungspaare  $p, q$ , und jedes dieser Lösungspaare gehört zu  $m^*(P^h)$ , während

umgekehrt jedes Paar aus  $m^*(P^h)$  für hinreichend grosses  $h$  einem solchen Bedingungssystem genügen muss. Andererseits hat  $F(x, 1)$  lauter verschiedene Nullstellen; die zu zwei solchen verschiedenen Nullstellen  $Z$  und  $Z'$  gehörigen vorigen Bedingungssysteme können also für hinreichend grosses  $h$  kein Lösungspaar  $p, q$  gemein haben, da die Differenz  $Z - Z'$  positiven  $P$ -adischen Betrag hat. Man erhält also die Menge aller Lösungspaare von  $m^*(P^h)$ , wenn man die Vereinigungsmenge aller Paare  $p, q$  bildet, die für irgend eine  $P$ -adische Nullstelle von  $F(x, 1)$  dem zugehörigen Bedingungssystem genügen, und zwar tritt dabei jedes solche Paar  $p, q$  einmal und nur einmal auf.

Geht man zu den Anzahlen über, so folgt damit

$$n^*(P^h) = (P-1) P^{h+1} \sum_Z \frac{\max(1, |Z|_P)^{h-2}}{|F'(Z, 1)|_P}$$

und zwar ist hier die Summe über die sämtlichen  $P$ -adischen Nullstellen von  $F(x, 1)$  zu erstrecken. Hieraus folgt weiter für grosses  $h$  die analoge Gleichung

$$n(P^h) = (P-1)^2 P^h \sum_Z \frac{\max(1, |Z|_P)^{h-2}}{|F'(Z, 1)|_P},$$

denn es ist nach 11.

$$\sum_{\rho=0}^{h-1} \frac{n(P^\rho)}{P^{2\rho+2}} + \frac{n^*(P^h)}{P^{2h+2}} = 1 - \frac{1}{P^2}$$

und demnach

$$n(P^h) = n^*(P^h) - \frac{1}{P^2} n^*(P^{h+1}).$$

Man entnimmt den so gewonnenen Formeln, die den Wert von  $n(P^h)$  und  $n^*(P^h)$  geben, falls  $h$  eine gewisse Grenze überschreitet, die folgenden zwei Aussagen:

- (1): *Hat das Polynom  $F(x, 1)$  keine  $P$ -adischen Nullstellen, so ist von einem Wert von  $h$  ab  $n(P^h) = 0$  und  $n^*(P^h) = 0$ .*  
 (2): *Die beiden Anzahlen  $n(P^h)$  und  $n^*(P^h)$  genügen für grosses  $h$  den zwei Ungleichungen*

$$n(P^h) = O(P^h), \quad n^*(P^h) = O(P^h).$$

Diese zwei Aussagen werden weiterhin angewandt.

13. Die Formeln des vorigen Paragraphen setzen voraus, dass der Wert von  $h$  genügend gross ist, geben also noch nicht den Wert der Anzahlen  $n(P^h)$

und  $n^*(P^h)$  für jedes  $h$ . Es scheint nicht ganz einfach, diesen Zahlwert auch für kleine  $h$  explizit anzugeben. Lässt man jedoch endlichviele Primzahlen  $P$  ausseracht, so gelingt es in der Tat, beide Anzahlen ausnahmslos zu bestimmen.

Zu diesem Zweck setzen wir voraus: »Die Primzahl geht weder in der Diskriminante  $d$ , noch in dem ersten Koeffizienten  $a_0$  der Binärform  $F(x, y)$  auf«. Eine Primzahl, die diese beiden Bedingungen befriedigt, heisse zur Abkürzung *regulär*; da  $d$  und  $a_0$  wegen der Irreduzibilität von  $F(x, y)$  nicht verschwinden, so können natürlich nur endlichviele Primzahlen nichtregulär sein.

Liegt eine solche reguläre Primzahl vor, so ist erstens

$$n^*(P^0) = P^2 - 1;$$

diese Formel bleibt sogar für nichtreguläre Primzahlen bestehen. Sei dagegen zweitens  $h \geq 1$ . Alsdann werde Gebrauch gemacht von der Relation

$$|F(p, q)|_P = \min(1, |p - qZ|_P, |p - qZ'|_P, \dots, |p - qZ^{(N-1)}|_P),$$

die nach dem ersten Teil dieser Arbeit für alle regulären Primzahlen und zwar unter der Voraussetzung  $(p, q, P) = 1$  gilt.<sup>1</sup> Dabei bedeuten

$$Z, Z', \dots, Z^{(N-1)}$$

die sämtlichen  $P$ -adischen Nullstellen von  $F(x, 1)$  und  $N$  ihre Anzahl.

Gibt es keine solche Nullstellen, so ist in der vorigen Ungleichung die rechte Seite gleich Eins; somit muss alsdann  $m^*(P^h)$  leer und

$$n^*(P^h) = 0 \text{ für } h \geq 1$$

sein.

Sei dagegen  $N \geq 1$ . Dann liegen wegen der Regularität von  $P$  alle Nullstellen von  $F(x, 1)$  in verschiedenen Restklassen mod  $P$ . Somit folgt, dass jedes Paar  $p, q$  von  $m^*(P^h)$  genau einem der  $N$  Bedingungssysteme

$$|p - qZ^{(M)}|_P \leq P^{-h}, \quad 0 \leq p \leq P^{h+1}, \quad 0 \leq q \leq P^{h+1}, \quad (p, q, P) = 1$$

genügen muss, wo  $Z^{(M)}$  der Reihe nach durch alle Nullstellen läuft. Aus der ersten und letzten dieser Forderungen folgt nun, dass  $q$  zu  $P$  teilerfremd sein muss; es gibt demnach genau

$$(P - 1)P^h$$

Möglichkeiten für  $q$ . Für jede der so gewählten Zahlen  $q$  gibt es weiter

<sup>1</sup> Siehe I, S. 719—722.

$$P$$

Lösungszahlen  $\nu$ . Also hat jedes dieser Bedingungssysteme

$$(P - 1) P^{h+1}$$

Lösungspaare und es folgt demnach die Gleichung

$$n^*(P^h) = N(P - 1) P^{h+1} \quad \text{für } h \geq 1.$$

Nachdem auf diese Weise  $n^*(P^h)$  bestimmt ist, folgt wie in 12. weiter

$$n(P^h) = \begin{cases} (P - 1)(P - N + 1) & \text{für } h = 0, \\ N(P - 1)^2 P^h & \text{für } h \geq 1. \end{cases}$$

Ohne Schwierigkeit erkennt man, dass diese Ausdrücke für  $n^*(P^h)$  und  $n(P^h)$  für  $h \geq 1$  zusammenfallen mit den Formeln, die in 12. für diese Anzahlen unter der Voraussetzung, dass die Zahl  $h$  hinreichend gross ist, und ohne die Einschränkung, dass  $P$  regulär sei, hergeleitet wurden.

14. Durch die bisherigen Entwicklungen wurden auch die beiden Anzahlen  $n(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})$  und  $n^*(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})$  ausgewertet, wenigstens wenn alle Exponenten  $h_1, h_2, \dots, h_t$  hinreichend gross sind oder es sich um reguläre Primzahlen  $P_1, P_2, \dots, P_t$  handelt; denn nach 10. gilt

$$n(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}) = \prod_{\tau=1}^t n(P_\tau^{h_\tau}),$$

$$n^*(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}) = \prod_{\tau=1}^t n^*(P_\tau^{h_\tau}).$$

Man hat auf Grund von 12. hiernach die beiden Aussagen:

(1): *Hat das Polynom  $F(x, 1)$  keine  $P_\tau$ -adische Nullstelle, wo  $P_\tau$  eine der Primzahlen  $P_1, P_2, \dots, P_t$  bedeutet, so ist*

$$n(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}) = 0, \quad n^*(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}) = 0,$$

*sobald der Exponent  $h_\tau$  hinreichend gross ist und wenn die anderen Exponenten irgend welche Werte haben.*

(2): *Es gibt eine positive Zahl  $c$ , die von  $h_1, h_2, \dots, h_t$  nicht abhängt, so dass immer*

$$n(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}) \leq c P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}, \quad n^*(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}) \leq c P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}$$

ist.

Zur Abkürzung möge die Funktion

$$d(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}) = \frac{n(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})}{P_1^{2h_1+2} P_2^{2h_2+2} \dots P_t^{2h_t+2}}$$

eingeführt werden; sie ist gleich der Dichte der Paare ganzer rationaler Zahlen  $p, q$  mit

$$Q(p, q) = P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}, \quad (p, q, P_1 P_2 \dots P_t) = 1$$

im Gitter aller Paare ganzer rationaler Zahlen. Aus (2) ergibt sich die Abschätzung

$$0 \leq d(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}) \leq C(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})^{-1}$$

wo auch  $C$  eine positive Zahl bedeutet, die von  $h_1, h_2, \dots, h_t$  nicht abhängt.

Aus dieser Abschätzung folgt insbesondere die Konvergenz der Reihe

$$\sigma(P_1 P_2 \dots P_t) = \sum_{h_1=0}^{\infty} \sum_{h_2=0}^{\infty} \dots \sum_{h_t=0}^{\infty} d(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}) (P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})^{2/n},$$

die im Folgenden auftritt. Man kann diese Reihe in Faktoren zerlegen, die sich nur noch auf einzelne Primzahlen beziehen; es ist nämlich

$$\sigma(P_1 P_2 \dots P_t) = \prod_{\tau=1}^t \sigma(P_\tau),$$

wobei

$$\sigma(P) = \sum_{h=0}^{\infty} d(P^h) (P^h)^{2/n}$$

gesetzt wurde.

Für reguläre Primzahlen  $P$  ergibt das vorige Kapitel durch Summation einer geometrischen Reihe den Zahlwert

$$\sigma(P) = \frac{(P-1)(P-N+1)}{P^2} + \frac{N(P-1)^2}{P^2(P^{1-2/n}-1)}$$

Die Reihe  $\sigma(P)$  stellt also eine Zahl des durch  $P^{2/n}$  erzeugten algebraischen Zahlkörpers dar. Aus den Ergebnissen in 12. folgt, dass diese Aussage auch dann noch bestehen bleibt, wenn die Primzahl  $P$  nicht mehr regulär ist.

15. Bei den folgenden Abschätzungen wird nicht die Reihe

$$\sigma(P_1 P_2 \cdots P_t) = \sum_{h_1=0}^{\infty} \sum_{h_2=0}^{\infty} \cdots \sum_{h_t=0}^{\infty} d(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}) (P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})^{2/n}$$

selbst auftreten, sondern nur der endliche Abschnitt

$$\sigma_x(P_1 P_2 \cdots P_t) = \sum_{h_1=0}^{\infty} \sum_{h_2=0}^{\infty} \cdots \sum_{h_t=0}^{\infty} d(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}) (P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})^{2/n},$$

$$P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t} \leq x$$

wo  $x$  eine sehr grosse positive Zahl bedeutet. Man kann eine sehr einfache asymptotische Formel für diesen Abschnitt herleiten, wenn man von den Aussagen (1) und (2) in 14. Gebrauch macht.

Zu diesem Zweck werde ohne Einschränkung der Allgemeinheit angenommen, dass die Gleichung  $F(x, 1) = 0$  Wurzeln im Körper der  $P$ -adischen Zahlen hat für die Indizes

$$\tau = 1, 2, \dots, t_0^*,$$

nicht aber für die Indizes

$$\tau = t_0^* + 1, t_0^* + 2, \dots, t;$$

dabei kann  $t_0^*$  irgend einen der Werte  $0, 1, 2, \dots, t$  haben. Ist  $t_0^* = 0$ , ist also die Gleichung in keinem der  $t$  Körper lösbar, so besitzt die Reihe für  $\sigma(P_1 P_2 \cdots P_t)$  nur endlichviele Summanden; in diesem Fall ist also von einem hinreichend grossen  $x$  ab

$$\sigma_x(P_1 P_2 \cdots P_t) = \sigma(P_1 P_2 \cdots P_t).$$

Sei dagegen  $t_0^* \geq 1$ . Alsdann treten in der Reihe für  $\sigma(P_1 P_2 \cdots P_t)$  nur solche nichtverschwindenden Summanden

$$d(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}) (P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})^{2/n},$$

für die die Exponenten

$$h_{t_0^*+1}, h_{t_0^*+2}, \dots, h_t$$



unterhalb einer nicht von  $x$  abhängigen Schranke liegen, auf. Diese nichtverschwindenden Summanden genügen ferner der Ungleichung

$$d(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}) (P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})^{2/n} \leq C (P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})^{2/n-1}.$$

Sei  $N(u)$  die Anzahl dieser nichtverschwindenden Summanden, für die

$$u \leq P_1^{h_1} P_2^{h_2} \dots P_t^{h_t} < 2u$$

ist. Wegen

$$P_1 \geq 2, P_2 \geq 2, \dots, P_t \geq 2$$

kann also keiner der Exponenten  $h_0, h_1, \dots, h_{t_0^*-1}$  grösser als

$$\frac{\log(2u)}{\log 2}$$

sein; jeder derselben hat somit höchstens

$$\frac{\log(4u)}{\log 2}$$

Möglichkeiten. Sind  $h_1, h_2, \dots, h_{t_0^*-1}$  gegeben, so können die übrigen Exponenten  $h_{t_0^*}, h_{t_0^*+1}, \dots, h_t$  nur noch eine beschränkte Anzahl von Wertsystemen annehmen, etwa höchstens  $\gamma$ . Es ist demnach für  $t_0^* \neq 0$

$$N(u) \leq \gamma \left( \frac{\log(4u)}{\log 2} \right)^{t_0^*-1}.$$

Da wegen

$$u \leq P_1^{h_1} P_2^{h_2} \dots P_t^{h_t} < 2u$$

ferner

$$d(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}) (P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})^{2/n} \leq C (P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})^{2/n-1} \leq \frac{C}{u^{1-2/n}}$$

ist, so ist die Summe der Glieder mit dieser Eigenschaft höchstens gleich

$$\frac{C\gamma}{u^{1-2/n}} \left( \frac{\log(4u)}{\log 2} \right)^{t_0^*-1}$$

Aus der Definition folgt nun die Reihenentwicklung

$$\sigma_x(P_1 P_2 \cdots P_t) = \sigma(P_1 P_2 \cdots P_t) - \sum_{h_1=0}^{\infty} \sum_{h_2=0}^{\infty} \cdots \sum_{h_t=0}^{\infty} d(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}) (P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})^{2/n} \\ P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t} > x.$$

Indem man die Summe rechts in die unendlichvielen Teilsummen

$$2^j x \leq P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t} < 2^{j+1} x \quad (j = 0, 1, 2, \dots)$$

zerlegt, kommt man zu der Abschätzung

$$|\sigma_x(P_1 P_2 \cdots P_t) - \sigma(P_1 P_2 \cdots P_t)| \leq \sum_{j=0}^{\infty} \frac{C_7}{(2^j x)^{1-2/n}} \left( \frac{\log(2^{j+2} x)}{\log 2} \right)^{t_0^* - 1}$$

Setzt man jetzt  $x$  hinreichend gross, nämlich  $x \geq 2$  voraus, so ist

$$\frac{\log(2^{j+2} x)}{\log 2} \leq (j+3) \frac{\log x}{\log 2}$$

und demnach

$$|\sigma_x(P_1 P_2 \cdots P_t) - \sigma(P_1 P_2 \cdots P_t)| \leq \frac{C_7}{(\log 2)^{t_0^* - 1}} \frac{(\log x)^{t_0^* - 1}}{x^{1-2/n}} \sum_{j=0}^{\infty} \frac{(j+3)^{t_0^* - 1}}{2^{(1-2/n)j}}$$

Da die Reihe

$$\sum_{j=0}^{\infty} \frac{(j+3)^{t_0^* - 1}}{2^{(1-2/n)j}}$$

gegen einen von  $x$  unabhängigen Grenzwert konvergiert, so folgt also endlich die Abschätzung

$$\sigma_x(P_1 P_2 \cdots P_t) = \sigma(P_1 P_2 \cdots P_t) + O\left(\frac{(\log x)^{t_0^* - 1}}{x^{1-2/n}}\right)$$

für grosses  $x$ . Damit sind wir zu folgendem Satz gelangt:

## 2. Hauptsatz: Bedeute

$F(x, y)$  eine irreduzible Binärform mit ganzen rationalen Koeffizienten vom Grad  $n \geq 3$ ,

$P_1, P_2, \dots, P_t$  endlichviele verschiedene Primzahlen,

$t_0^*$  die Anzahl derjenigen unter diesen Primzahlen  $P_\tau$ , für die die Gleichung  $F(x, 1) = 0$  Wurzeln im Körper der  $P_\tau$ -adischen Zahlen hat,

$p$  und  $q$  zwei ganze rationale Zahlen mit  $(p, q, P_1 P_2 \cdots P_t) = 1$ ,  
 $Q(p, q)$  das grösste Potenzprodukt der Primzahlen  $P_1, P_2, \dots, P_t$ , das in  $F(p, q)$  aufgeht,

$n(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})$  die Anzahl der Paare ganzer rationaler Zahlen  $p, q$  mit

$$Q(p, q) = P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}, \quad (p, q, P_1 P_2 \cdots P_t) = 1,$$

$$0 \leq p \leq P_1^{h_1+1} P_2^{h_2+1} \cdots P_t^{h_t+1} - 1, \quad 0 \leq q \leq P_1^{h_1+1} P_2^{h_2+1} \cdots P_t^{h_t+1} - 1,$$

$d(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})$  die Dichte der Paare ganzer rationaler Zahlen  $p, q$  mit

$$Q(p, q) = P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}, \quad (p, q, P_1 P_2 \cdots P_t) = 1$$

im Gitter aller Paare ganzer rationaler Zahlen  $p, q$ ,

$\sigma(P_1 P_2 \cdots P_t)$  die unendliche Reihe

$$\sigma(P_1 P_2 \cdots P_t) = \sum_{h_1=0}^{\infty} \sum_{h_2=0}^{\infty} \cdots \sum_{h_t=0}^{\infty} d(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}) (P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})^{2/n},$$

$\sigma_x(P_1 P_2 \cdots P_t)$  für eine beliebige positive Zahl  $x$  ihren Abschnitt mit

$$\sigma_x(P_1 P_2 \cdots P_t) = \sum_{h_1=0}^{\infty} \sum_{h_2=0}^{\infty} \cdots \sum_{h_t=0}^{\infty} d(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}) (P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})^{2/n},$$

$$P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t} \leq x$$

$\sigma(P_\tau)$  die Summe  $\sigma(P_1 P_2 \cdots P_t)$  im Fall einer einzigen Primzahl.

Dann besteht die Beziehung

$$d(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}) = \frac{n(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})}{P_1^{2h_1+2} P_2^{2h_2+2} \cdots P_t^{2h_t+2}},$$

und es ist für über alle Grenzen wachsendes positives  $x$

$$\sigma_x(P_1 P_2 \cdots P_t) = \sigma(P_1 P_2 \cdots P_t) + \begin{cases} 0 & \text{für } t_0^* = 0, \\ O\left(\frac{(\log x)^{t_0^*-1}}{x^{1-2/n}}\right) & \text{für } t_0^* \geq 1. \end{cases}$$

Auf der rechten Seite dieser Beziehung lässt sich das Hauptglied auf folgende Weise in Faktoren, die sich nur noch auf einzelne Primzahlen beziehen, zerlegen:

$$\sigma(P_1 P_2 \cdots P_t) = \prod_{\tau=1}^t \sigma(P_\tau).$$

Der einzelne Faktor  $\sigma(P_\tau)$  ist eine Zahl des durch  $P_\tau^{2/n}$  erzeugten algebraischen Zahl-

körpers. Wenn insbesondere  $P_\tau$  weder in der Diskriminante von  $F(x, y)$ , noch in dem Koeffizienten von  $x^n$  dieser Form aufgeht, so ist

$$\sigma(P_\tau) = \frac{(P_\tau - 1)(P_\tau - \nu_\tau + 1)}{P_\tau^2} + \frac{\nu_\tau(P_\tau - 1)^2}{P_\tau^2(P_\tau^{1-2/n} - 1)},$$

wobei  $\nu_\tau$  die Anzahl der  $P_\tau$ -adischen Nullstellen von  $F(x, 1)$ , eventuell die Null, bedeutet.

### III.

16. Sei  $G$  eine Punktmenge im Innern der  $(p, q)$ -Ebene,  $P_1, P_2, \dots, P_t$  wieder eine endliche Anzahl verschiedener Primzahlen. Die Menge aller Gitterpunkte  $(p, q)$  in  $G$  mit

$$(p, q, P_1 P_2 \cdots P_t) = 1$$

heisse  $M_G$ , die Anzahl ihrer Elemente  $N_G$ . Für die weiteren Entwicklungen ist es nötig,  $M_G$  und  $N_G$  in einfachere Bestandteile zu zerlegen.

Da  $M_G$  gewiss den Punkt  $(0, 0)$  nicht enthält, so entspricht jedem Punkt dieser Menge eine nichtverschwindende ganze rationale Zahl  $F(p, q)$  und also auch als grösstes Potenzprodukt der Primzahlen  $P_1, P_2, \dots, P_t$ , das in  $F(p, q)$  aufgeht, eine wohlbestimmte Zahl  $Q(p, q)$ . Gemäss dem Wert dieser Zahl  $Q(p, q)$  lässt sich die Menge  $M_G$  offenbar in Teilmengen  $M_G(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})$  zerlegen:

$$M_G = \sum_{h_1=0}^{\infty} \sum_{h_2=0}^{\infty} \cdots \sum_{h_t=0}^{\infty} M_G(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}),$$

so dass für alle diejenigen Paare  $p, q$  aus  $M_G$ , die in  $M_G(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})$  liegen und nur für diese gerade

$$Q(p, q) = P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}$$

ist. Wird die Elementen-Anzahl von  $M_G(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})$  mit  $N_G(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})$  bezeichnet, so gilt entsprechenderweise die Zerlegung

$$N_G = \sum_{h_1=0}^{\infty} \sum_{h_2=0}^{\infty} \cdots \sum_{h_t=0}^{\infty} N_G(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}).$$

Die Menge  $M_G(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})$  lässt weiter eine Unterteilung zu, gemäss den

Restklassen modulo  $P_1^{h_1+1} P_2^{h_2+1} \dots P_t^{h_t+1}$ , in denen die Koordinaten des Punktes  $p, q$  liegen. Sei  $p, q$  irgend ein Punkt dieser Menge, also

$$(p, q, P_1 P_2 \dots P_t) = 1, \quad Q(p, q) = P_1^{h_1} P_2^{h_2} \dots P_t^{h_t},$$

und  $p', q'$  ein Paar ganzer rationaler Zahlen, das mit  $p, q$  durch die Kongruenzen

$$p' \equiv p \pmod{P_1^{h_1+1} P_2^{h_2+1} \dots P_t^{h_t+1}}, \quad q' \equiv q \pmod{P_1^{h_1+1} P_2^{h_2+1} \dots P_t^{h_t+1}}$$

verknüpft ist. Dann ist offenbar

$$(p', q', P_1 P_2 \dots P_t) = 1,$$

ferner nach der Taylorschen Reihenentwicklung

$$F(p, q) \equiv F(p', q') \pmod{P_1^{h_1+1} P_2^{h_2+1} \dots P_t^{h_t+1}},$$

also

$$Q(p', q') = Q(p, q) = P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}.$$

Das Paar  $p', q'$  hat also wieder dieselben arithmetischen Eigenschaften wie das Paar  $p, q$ , bestimmt aber natürlich im allgemeinen keinen in  $M_G$  liegenden Punkt. Man kann seine Eigenschaften zu folgender Zerlegung der Menge  $M_G(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})$  benutzen:

Die Paare  $p, q$  aus  $M_G(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})$  müssen sich auf gewisse Restklassen modulo  $P_1^{h_1+1} P_2^{h_2+1} \dots P_t^{h_t+1}$  verteilen. Aus jeder solchen Restklasse lässt sich ein Repräsentant  $p', q'$  mit

$$\begin{aligned} p' &\equiv p \pmod{P_1^{h_1+1} P_2^{h_2+1} \dots P_t^{h_t+1}}, & q' &\equiv q \pmod{P_1^{h_1+1} P_2^{h_2+1} \dots P_t^{h_t+1}}, \\ (p', q', P_1 P_2 \dots P_t) &= 1, & Q(p', q') &= P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}, \\ 0 \leq p' &\leq P_1^{h_1+1} P_2^{h_2+1} \dots P_t^{h_t+1} - 1, & 0 \leq q' &\leq P_1^{h_1+1} P_2^{h_2+1} \dots P_t^{h_t+1} - 1, \end{aligned}$$

d. h. ein Element aus  $m(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})$  wählen. Alle Elemente aus  $M_G(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})$ , die den Kongruenzen

$$p \equiv p' \pmod{P_1^{h_1+1} P_2^{h_2+1} \dots P_t^{h_t+1}}, \quad q \equiv q' \pmod{P_1^{h_1+1} P_2^{h_2+1} \dots P_t^{h_t+1}}$$

genügen, mögen zu der Menge  $M_G(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}; p', q')$  zusammengefasst werden. Alsdann ist gerade

$$M_G(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}) = \sum_{p', q' \text{ in } m(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})} M_G(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}; p', q'),$$

und wenn mit  $N_G(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}; p', q')$  die Anzahl der Elemente der neuen Menge verstanden wird, so besteht entsprechenderweise die Relation

$$N_G(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}) = \sum_{p', q' \text{ in } m(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})} N_G(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}; p', q').$$

17. Die vorigen Zerlegungen sollen angewandt werden unter der Voraussetzung, dass  $G$  die Menge der Gitterpunkte in der  $(p, q)$ -Ebene bezeichnet, für die

$$\left| \frac{F(p, q)}{Q(p, q)} \right| \leq k, \quad |p, q| \leq k^{\frac{1}{n-1}}$$

ist, wobei  $k$  eine positive, über alle Grenzen wachsende Zahl bedeutet. Dann ist also speziell  $M_G$  die Menge aller Paare ganzer rationaler Zahlen  $p, q$  mit

$$\left| \frac{F(p, q)}{Q(p, q)} \right| \leq k, \quad (p, q, P_1 P_2 \cdots P_t) = 1, \quad |p, q| \leq k^{\frac{1}{n-1}}$$

und enthält natürlich nur endlichviele Elemente; die Anzahl  $N_G$  und erst recht die Teilanzahlen  $N_G(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})$  und  $N_G(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}; p', q')$  werden demnach von selbst endlich, so dass die Zerlegungen des vorigen Paragraphen Sinn haben. Es handelt sich darum, für diese Anzahlen asymptotische Formeln zu gewinnen. Dies wird gelingen durch einige elementaren Gitterpunktsbetrachtungen.

18. Die Gleichung  $F(x, 1) = 0$  hat im Körper der reellen Zahlen etwa die sämtlichen Wurzeln

$$\zeta, \zeta', \dots, \zeta^{(r-1)};$$

ihre Anzahl  $\nu$  ist höchstens gleich  $n$  und kann auch unter Umständen verschwinden. Wie im ersten Teil dieser Arbeit gezeigt wurde, gibt es eine positive Konstante  $C_0$ , die allein von der Binärform  $F(x, y)$  abhängt, so dass für alle reellen Zahlen  $x, y$ , die nicht beide verschwinden, die Ungleichung

$$|F(x, y)| \geq C_0 \max(|x|, |y|)^n \min \left( \left| \frac{x}{y} - \zeta \right|, \left| \frac{x}{y} - \zeta' \right|, \dots, \left| \frac{x}{y} - \zeta^{(r-1)} \right|, 1 \right)$$

besteht; dabei muss für  $\nu = 0$  auf der rechten Seite der Ausdruck

$$\min \left( \left| \frac{x}{y} - \zeta \right|, \left| \frac{x}{y} - \zeta' \right|, \dots, \left| \frac{x}{y} - \zeta^{(v-1)} \right|, 1 \right)$$

durch Eins ersetzt werden.<sup>1</sup>

Sei  $Q$  zunächst eine beliebige natürliche Zahl, die der Ungleichung

$$Q \leq \frac{C_0}{2} k^{\frac{1}{n-1}}$$

genügt. Für alle Punkte der durch

$$|F(x, y)| \leq kQ, \quad \max(|x|, |y|) \geq k^{\frac{1}{n-1}}$$

definierten Punktmenge  $H$  muss die Ungleichung

$$\min \left( \left| \frac{x}{y} - \zeta \right|, \left| \frac{x}{y} - \zeta' \right|, \dots, \left| \frac{x}{y} - \zeta^{(v-1)} \right|, 1 \right) \leq \frac{kQ}{C_0 \max(|x|, |y|)^n}$$

bestehen. Wegen

$$\frac{kQ}{C_0 \max(|x|, |y|)^n} \leq \frac{k \frac{C_0}{2} k^{\frac{1}{n-1}}}{C_0 (k^{\frac{1}{n-1}})^n} = \frac{1}{2}$$

ist hier aber die rechte Seite kleiner als Eins; auf der linken Seite muss also für jeden Punkt von  $H$  mindestens einer der Ausdrücke

$$\left| \frac{x}{y} - \zeta^{(\mu)} \right| \quad (\mu = 0, 1, \dots, v-1)$$

kleiner als Eins sein, wenn nicht  $v=0$  und alsdann  $H$  eine leere Menge ist.

Wird von diesem Fall  $v=0$  abgesehen, so lässt sich der Inhalt von  $H$  leicht nach oben abschätzen. Da nach vorhin für jeden Punkt von  $H$  eine der Ungleichungen

$$\left| \frac{x}{y} - \zeta^{(\mu)} \right| \leq \frac{kQ}{C_0 \max(|x|, |y|)^n} \leq \frac{1}{2} \quad (\mu = 0, 1, \dots, v-1)$$

erfüllt ist, so gilt insbesondere

$$\left| \frac{x}{y} - \zeta^{(\mu)} \right| \leq \frac{1}{2}, \quad |x - \zeta^{(\mu)} y| \leq \frac{1}{2} |y|, \quad |x| \leq \left( \frac{1}{2} + |\zeta^{(\mu)}| \right) |y|$$

<sup>1</sup> Siehe I, S. 714—716.

und wenn zur Abkürzung

$$1 + \max(|\zeta|, |\zeta'|, \dots, |\zeta^{(v-1)}|) = C_1$$

gesetzt wird, so folgt also, dass für jeden Punkt von  $H$

$$\max(|x|, |y|) \leq C_1 |y|,$$

wegen

$$\max(|x|, |y|) \geq k^{\frac{1}{n-1}}$$

demnach

$$|y| \geq \frac{1}{C_1} k^{\frac{1}{n-1}}$$

sein muss. Ein jeder Punkt dieser Menge liegt somit in einem der  $\nu$  Bereiche

$$\left| \frac{x}{y} - \zeta^{(u)} \right| \leq \frac{kQ}{C_0 |y|^n}, \quad |y| \geq \frac{1}{C_1} k^{\frac{1}{n-1}} \quad (u = 0, 1, \dots, \nu - 1).$$

Der Inhalt jedes dieser Bereiche ist aber gleich

$$4 \int_{\frac{1}{C_1} k^{\frac{1}{n-1}}}^{\infty} \frac{kQ}{C_0 y^{n-1}} dy$$

und folglich gleich

$$\frac{4 C_1^{n-2}}{(n-2) C_0} Q k^{\frac{1}{n-1}},$$

wie sich durch Ausrechnung des Integrales ergibt. Damit folgt für den Inhalt von  $H$  die obere Schranke

$$\frac{4\nu C_1^{n-2}}{(n-2) C_0} Q k^{\frac{1}{n-1}},$$

und diese bleibt trivialerweise auch für  $\nu = 0$  richtig.

19. Aus der letzten Abschätzung ergibt sich insbesondere, dass das Integral

$$\int \int_{|F(x,y)| \leq Qk} dx dy$$



existiert; es hat wegen der Homogenität von  $F(x, y)$  offenbar den Wert

$$\sigma(Qk)^{2/n},$$

wobei unter  $\sigma$  die Konstante

$$\sigma = \int \int_{|F(x, y)| \leq 1} dx dy = \int_{-\infty}^{+\infty} |F(x, 1)|^{-2/n} dx$$

verstanden wird. Da der Inhalt  $J$  des Bereiches  $\Gamma$ :

$$|F(x, y)| \leq Qk, \quad \max(|x|, |y|) \leq k^{\frac{1}{n-1}}$$

gleich

$$J = \int \int_{|F(x, y)| \leq Qk} dx dy - \int \int_H dx dy,$$

so ergibt sich nach den letzten Abschätzungen für diesen Inhalt die Ungleichung

$$|J - \sigma(Qk)^{2/n}| \leq \frac{4^\nu C_1^{n-1}}{(n-2) C_0} Qk^{\frac{1}{n-1}}.$$

Auch der Umfang  $L$  von  $\Gamma$  lässt sich leicht abschätzen; dabei wird zweckmässigerweise unterschieden, ob  $\nu = 0$  oder  $\nu \geq 1$  ist. Im ersteren Fall bekommt man wegen der Homogenität von  $F(x, y)$  für grosses  $k$

$$L = C_2(Qk)^{1/n},$$

wo  $C_2$  die Bogenlänge der geschlossenen endlichen Kurve

$$|F(x, y)| = 1$$

bedeutet. Dies folgt daraus, dass die Kurve

$$|F(x, y)| = Qk$$

mit dem Quadratrand

$$\max(|x|, |y|) = k^{\frac{1}{n-1}}$$

keinen Punkt gemein hat, da wegen  $\nu = 0$  die Menge  $H$  leer ist.

Sei dagegen  $\nu \geq 1$ . Die Berandung von  $\Gamma$  setzt sich alsdann zusammen aus reellen Bogenstücken der beiden algebraischen Kurven

$$F(x, y) = \overline{+} Qk$$

und aus Stücken der vier Geraden

$$x = \overline{+} k^{\frac{1}{n-1}}, \quad y = \overline{+} k^{\frac{1}{n-1}}.$$

Es gibt also jeweils höchstens

$$2n + 2$$

Punkte auf dem Rand von  $\Gamma$  mit gegebener Abszisse oder Ordinate. Es ist nun

$$L = \int (dx^2 + dy^2)^{1/2},$$

wobei über die ganze Berandung von  $\Gamma$  integriert wird, also erst recht

$$L \leq \int (|dx| + |dy|),$$

d. h.  $L$  ist höchstens gleich der Summe der Projektionen des Randes von  $\Gamma$  auf die beiden Achsen. Die Länge dieser Projektion übersteigt nicht den Wert

$$2 \cdot (2n + 2) \cdot 2k^{\frac{1}{n-1}}$$

und also ist für  $v \geq 1$

$$L \leq (8n + 8)k^{\frac{1}{n-1}}.$$

20. Der Bereich  $\Gamma$  werde jetzt mit einem Quadratnetz der Seitenlänge

$$P_1 P_2 \cdots P_t Q$$

überdeckt; dabei seien die Quadratecken durch die Kongruenzen

$$p \equiv p' \pmod{P_1 P_2 \cdots P_t Q}, \quad q \equiv q' \pmod{P_1 P_2 \cdots P_t Q}$$

mit festen ganzen rationalen Zahlen  $p', q'$  definiert. Alsdann fallen in  $\Gamma$  eine gewisse Anzahl  $N$  dieser Quadratecken. Diese Anzahl ist offenbar der Anzahl der gewöhnlichen Gitterpunkte gleich, die in einem Bereich  $\Gamma'$  liegen, der aus  $\Gamma$  durch die Ähnlichkeitstransformation

$$\begin{aligned} x &= P_1 P_2 \cdots P_t Q x' + p' \\ y &= P_1 P_2 \cdots P_t Q y' + q' \end{aligned}$$

hervorgeht. Diese Transformation verkleinert alle Inhalte im Verhältnis

$$(P_1 P_2 \cdots P_t Q)^2 : 1$$

und alle Umfänge im Verhältnis

$$(P_1 P_2 \cdots P_t Q) : 1.$$

Der Inhalt  $J'$  von  $\Gamma'$  genügt also der Ungleichung

$$\left| J' - \frac{\sigma(Qk)^{2/n}}{(P_1 P_2 \cdots P_t Q)^2} \right| \leq \frac{4^\nu C_1^{n-1} Q k^{\frac{1}{n-1}}}{(n-2) C_0 (P_1 P_2 \cdots P_t Q)^2}$$

und der Umfang  $L'$  von  $\Gamma'$  der Ungleichung

$$|L'| \leq \begin{cases} \frac{C_2 (Qk)^{1/n}}{P_1 P_2 \cdots P_t Q} & \text{für } \nu = 0, \\ \frac{(8n+8) k^{\frac{1}{n-1}}}{P_1 P_2 \cdots P_t Q} & \text{für } \nu \geq 1. \end{cases}$$

Andrerseits liegen nach einem bekannten elementaren Satz in einem einfach-zusammenhängenden Bereich mit dem Inhalt  $J'$  und dem Umfang  $L'$  höchstens

$$J' + 4(L' + 1)$$

und wenigstens

$$J' - 4(L' + 1)$$

Gitterpunkte. Die Anzahl  $N$  muss also der Ungleichung<sup>1</sup>

$$|N - J'| \leq 4(L' + 1)$$

genügen. Es gilt also erstens für  $\nu = 0$

$$\left| N - \frac{\sigma(Qk)^{2/n}}{(P_1 P_2 \cdots P_t Q)^2} \right| \leq \frac{4 C_2 (Qk)^{1/n}}{P_1 P_2 \cdots P_t Q} + 4.$$

Auf Grund der Voraussetzung

$$Q \leq \frac{C_0}{2} k^{\frac{1}{n-1}}$$

<sup>1</sup> Wie ich der Dissertation von L. W. Nieland (Groningen 1933) entnehme, stammt dieser bekannte Satz von C. F. Gauss, Werke II, S. 269 f.

ist jedoch

$$\frac{4 C_2 (Qk)^{1/n}}{P_1 P_2 \cdots P_t Q} \geq \frac{4 C_2}{P_1 P_2 \cdots P_t} \left( \frac{2}{C_0} \right)^{\frac{n-1}{n}}$$

so dass sich der Summand 4 in den anderen aufnehmen lässt und für  $\nu = 0$

$$\left| N - \frac{\sigma(Qk)^{2/n}}{(P_1 P_2 \cdots P_t Q)^2} \right| \leq \frac{C_3 k^{1/n}}{Q^{1-1/n}}$$

wird, mit einer positiven Zahl  $C_3$ , die von  $k$  und  $Q$  nicht abhängt.

Sei zweitens  $\nu \geq 1$ . Dann ist

$$\left| N - \frac{\sigma(Qk)^{2/n}}{(P_1 P_2 \cdots P_t Q)^2} \right| \leq \left( \frac{4\nu C_1^{n-1}}{(n-2) C_0 P_1^2 P_2^2 \cdots P_t^2} + \frac{4 \cdot (8n+8)}{P_1 P_2 \cdots P_t} \right) \frac{k^{\frac{1}{n-1}}}{Q} + 4.$$

Auf Grund der Voraussetzung

$$Q \leq \frac{C_0}{2} k^{\frac{1}{n-1}}$$

ist jedoch diesmal

$$\frac{k^{\frac{1}{n-1}}}{Q} \geq \frac{2}{C_0},$$

so dass sich der Summand 4 auch jetzt wieder in den anderen aufnehmen lässt und also für  $\nu \geq 1$

$$\left| N - \frac{\sigma(Qk)^{2/n}}{(P_1 P_2 \cdots P_t Q)^2} \right| \leq C_4 \frac{k^{\frac{1}{n-1}}}{Q}$$

wird, mit einer positiven Zahl  $C_4$ , die von  $k$  und  $Q$  nicht abhängt.

Die so gefundenen Ergebnisse führen sofort zu einer Abschätzung für die Anzahl  $N_G(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}; p', q')$ . Diese ist nach Definition gleich der Anzahl der Paare ganzer rationaler Zahlen  $p, q$ , die den Bedingungen

$$\begin{aligned} |F(p, q)| &\leq P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t} k, & |p, q| &\leq k^{\frac{1}{n-1}}, \\ p &\equiv p' \pmod{P_1^{h_1+1} P_2^{h_2+1} \cdots P_t^{h_t+1}}, & q &\equiv q' \pmod{P_1^{h_1+1} P_2^{h_2+1} \cdots P_t^{h_t+1}} \end{aligned}$$

genügen; sie ist also gerade gleich einer Anzahl  $N$ , wenn die Zahl  $Q$  mit

$$Q = P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}$$

zusammenfällt. Somit wird

$$\left| N_G(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}; p', q') - \frac{\sigma k^{2/n}}{P_1^2 P_2^2 \dots P_t^2 (P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})^{2-2/n}} \right| \leq \begin{cases} \frac{C_3 k^{1/n}}{(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})^{1-1/n}} & \text{für } \nu = 0, \\ \frac{1}{P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}} & \text{für } \nu \geq 1. \end{cases}$$

Lässt man hier das Paar  $p', q'$  die sämtlichen  $n(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})$  Elemente der Menge  $m(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})$  durchlaufen und beachtet man die Gleichung

$$d(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}) = \frac{n(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})}{P_1^{2h_1+2} P_2^{2h_2+2} \dots P_t^{2h_t+2}},$$

so ergibt sich also durch Summation aller so entstehenden Ungleichungen die Abschätzung

$$\left| N_G(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}) - \sigma k^{2/n} d(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}) (P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})^{2/n} \right| \leq \begin{cases} \frac{C_3 k^{1/n} n(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})}{(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})^{1-1/n}} & \text{für } \nu = 0, \\ \frac{1}{P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}} & \text{für } \nu \geq 1. \end{cases}$$

Es sei aber noch einmal darauf aufmerksam gemacht, dass bei dieser Herleitung ausdrücklich vorausgesetzt wurde, dass

$$Q = P_1^{h_1} P_2^{h_2} \dots P_t^{h_t} \leq \frac{C_0}{2} k^{\frac{1}{n-1}}$$

ist.

21. Die Abschätzungen in 20. machen es möglich, die Anzahl  $N_G$  aller Paare ganzer rationaler Zahlen  $p, q$  mit

$$\left| \frac{F(p, q)}{Q(p, q)} \right| \leq k, \quad (p, q, P_1 P_2 \dots P_t) = 1, \quad |p, q| \leq k^{\frac{1}{n-1}}$$

angenähert zu bestimmen. Nach 16. besteht für diese Anzahl die Reihenentwicklung

$$N_G = \sum_{h_1=0}^{\infty} \sum_{h_2=0}^{\infty} \cdots \sum_{h_t=0}^{\infty} N_G(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}).$$

Um die bisherigen Ergebnisse anwenden zu können, werde die Summe auf der rechten Seite in die endliche Teilsumme

$$N'_G = \sum_{h_1=0}^{\infty} \sum_{h_2=0}^{\infty} \cdots \sum_{h_t=0}^{\infty} N_G(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}) \\ P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t} \leq \frac{C_0}{2} k^{\frac{1}{n-1}}$$

und den unendlichen Rest

$$N''_G = \sum_{h_1=0}^{\infty} \sum_{h_2=0}^{\infty} \cdots \sum_{h_t=0}^{\infty} N_G(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}) \\ P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t} > \frac{C_0}{2} k^{\frac{1}{n-1}}$$

zerlegt, so dass

$$N_G = N'_G + N''_G$$

ist.

Die Glieder von  $N'_G$  ersetzen wir durch die Ausdrücke, die am Ende von 20. hergeleitet wurden. Mit der früheren Abkürzung

$$\sigma_x(P_1 P_2 \cdots P_t) = \sum_{h_1=0}^{\infty} \sum_{h_2=0}^{\infty} \cdots \sum_{h_t=0}^{\infty} d(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}) (P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})^{2/n} \\ P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t} \leq x$$

wird dann gerade

$$|N'_G - \sigma \cdot \sigma_{\frac{C_0}{2} k^{\frac{1}{n-1}}}(P_1 P_2 \cdots P_t) k^{2/n}| \leq \begin{cases} C_3 k^{\frac{1}{n}} S' & \text{für } \nu = 0, \\ C_4 k^{\frac{1}{n-1}} S'' & \text{für } \nu \geq 1, \end{cases}$$

wobei

$$S' = \sum_{h_1=0}^{\infty} \sum_{h_2=0}^{\infty} \cdots \sum_{h_t=0}^{\infty} n(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}) (P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})^{-\left(1-\frac{1}{n}\right)} \\ P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t} \leq \frac{C_0}{2} k^{\frac{1}{n-1}}$$

und

$$S'' = \sum_{h_1=0}^{\infty} \sum_{h_2=0}^{\infty} \cdots \sum_{h_t=0}^{\infty} n(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}) (P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})^{-1} \\ P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t} \leq \frac{C_0}{2} k^{\frac{1}{n-1}}$$

ist. Bedeute nun wieder wie beim ersten und zweiten Hauptsatz die Zahl  $t_0^*$  die Anzahl der Primzahlen  $P_1, P_2, \dots, P_t$ , für die die Gleichung  $F(x, 1) = 0$  im Körper der  $P_t$ -adischen Zahlen lösbar ist, und  $t_0$  die Zahl  $t_0^* + \text{sgn } \nu$ . Nach dem zweiten Hauptsatz besteht für hinreichend grosses  $x > 0$  die Formel

$$\sigma_x(P_1 P_2 \cdots P_t) = \sigma(P_1 P_2 \cdots P_t) + \begin{cases} 0 & \text{für } t_0^* = 0, \\ O\left(\frac{(\log x)^{t_0^*-1}}{x^{1-2/n}}\right) & \text{für } t_0^* \geq 1, \end{cases}$$

so dass also auch

$$\sigma_{\frac{C_0}{2} k^{\frac{1}{n-1}}}(P_1 P_2 \cdots P_t) k^{2/n} = \sigma(P_1 P_2 \cdots P_t) k^{2/n} + \begin{cases} 0 & \text{für } t_0^* = 0, \\ O\left(\frac{1}{k^{n-1}} (\log k)^{t_0^*-1}\right) & \text{für } t_0^* \geq 1 \end{cases}$$

sein muss. Wenn ferner  $t_0^* = 0$  ist, so verschwindet die Anzahl  $n(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})$ , sobald einer der Exponenten  $h_1, h_2, \dots, h_t$  eine gewisse endliche Grenze überschreitet; gilt dagegen  $t_0^* \geq 1$ , so besteht die Ungleichung

$$n(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}) \leq c P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t},$$

wo  $c$  eine positive Zahl bezeichnet, die von den Exponenten  $h_1, h_2, \dots, h_t$  nicht abhängt.

Um diese Aussagen anzuwenden, macht man jetzt zweckmässigerweise folgende Fallunterscheidung:

1. Fall:  $\nu = 0, t_0^* = 0$ .

Die Summe  $S'$  besteht aus einer beschränkten Anzahl von Summanden, bleibt also unterhalb einer von  $k$  unabhängigen Grenze. Demnach ist

$$N'_G = \sigma \sigma(P_1 P_2 \cdots P_t) k^{2/n} + O(k^{1/n}).$$

2. Fall:  $\nu \geq 1, t_0^* = 0$ .

Die Summe  $S''$  besteht aus einer beschränkten Anzahl von Summanden, bleibt also unterhalb einer von  $k$  unabhängigen Grenze. Demnach ist

$$N'_G = \sigma \sigma(P_1 P_2 \cdots P_t) k^{2/n} + O(k^{\frac{1}{n-1}}).$$

3. Fall:  $\nu = 0$ ,  $t_0^* \geq 1$ .

Ohne Einschränkung werde angenommen, dass die Gleichung  $F(x, 1) = 0$  im  $P_\tau$ -adischen Körper allein für die Indizes

$$\tau = 1, 2, \dots, t_0^*,$$

nicht aber für die übrigen lösbar ist. Alsdann verschwindet  $n(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})$ , falls einer der Exponenten  $h_{t_0^*+1}, h_{t_0^*+2}, \dots, h_t$  eine gewisse Grenze übersteigt, und es gilt im übrigen die Ungleichung

$$n(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}) \leq c P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}.$$

Sei wieder  $N(u)$  die Anzahl der Summanden von  $S'$ , für die

$$u \leq P_1^{h_1} P_2^{h_2} \dots P_t^{h_t} < 2u;$$

wie in 15. zeigt man, dass

$$N(u) \leq \gamma \left( \frac{\log(4u)}{\log 2} \right)^{t_0^*-1}$$

ist mit einer gewissen konstanten natürlichen Zahl  $\gamma$ . Die Summe der Summanden von  $S'$  mit

$$u \leq P_1^{h_1} P_2^{h_2} \dots P_t^{h_t} < 2u$$

hat demnach höchstens den Wert

$$\gamma c \left( \frac{\log(4u)}{\log 2} \right)^{t_0^*-1} (2u)^{\frac{1}{n}},$$

denn es gilt für diese Summanden

$$n(P_1^{h_1} P_2^{h_2} \dots P_t^{h_t}) (P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})^{-(1-\frac{1}{n})} \leq c (P_1^{h_1} P_2^{h_2} \dots P_t^{h_t})^{\frac{1}{n}} \leq c (2u)^{\frac{1}{n}}.$$

Die Summe  $S'$  werde jetzt in die Teilsummen mit

$$u \leq P_1^{h_1} P_2^{h_2} \dots P_t^{h_t} < 2u$$

für  $u = 1, 2, 4, 8, \dots$  zerlegt; natürlicherweise beschränkt man sich dabei auf diejenigen Werte von  $u$ , für die

$$u \leq \frac{C_0}{2} k^{n-1}$$



ist. Da infolgedessen gleichmässig in  $u$

$$\gamma c \left( \frac{\log(4u)}{\log 2} \right)^{t_0^* - 1} (2u)^{\frac{1}{n}} \leq O((\log k)^{t_0^* - 1}) (2u)^{\frac{1}{n}}$$

gilt, so wird also

$$S' = O((\log k)^{t_0^* - 1}) \sum_{j=0}^{\infty} (2^{j+1})^{\frac{1}{n}}$$

$$2^j \leq \frac{C_0}{2} k^{\frac{1}{n-1}}$$

und nach Summation dieser geometrischen Reihe

$$S' = O(k^{\frac{1}{n(n-1)}} (\log k)^{t_0^* - 1}),$$

und es ergibt sich

$$N'_G = \sigma \sigma(P_1 P_2 \cdots P_t) k^{\frac{2}{n}} + O(k^{\frac{1}{n-1}} (\log k)^{t_0^* - 1}).$$

4. Fall:  $\nu \geq 1, t_0^* \geq 1$ .

Wieder werde wie beim dritten Fall vorausgesetzt, dass die Gleichung  $F(x, 1) = 0$  allein für die Indizes

$$\tau = 1, 2, \dots, t_0^*$$

im Körper der  $P_\tau$ -adischen Zahlen Wurzeln hat. Alsdann verschwindet die Anzahl  $n(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})$ , falls einer der Exponenten  $h_{t_0^*+1}, h_{t_0^*+2}, \dots, h_t$  eine gewisse Grenze überschreitet und es ist im übrigen

$$n(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}) \leq c P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}.$$

Die Summe  $S''$  ist demnach nicht grösser als die  $c$ -fache Anzahl der Potenzprodukte  $P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}$ , die der Ungleichung

$$P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t} \leq \frac{C_0}{2} k^{\frac{1}{n-1}}$$

genügen und für die die letzten  $t - t_0^*$  Exponenten unter einer von  $k$  unabhängigen Schranke bleiben. Daraus folgt leicht die Abschätzung

$$S'' = O((\log k)^{t_0^*}),$$

und es ergibt sich

$$N'_G = \sigma \sigma(P_1 P_2 \cdots P_t) k^{\frac{2}{n}} + O(k^{\frac{1}{n-1}} (\log k)^{t_0^*}).$$

Nachdem so in allen vier Fällen die Anzahl  $N'_G$  abgeschätzt worden ist, zeigt ein Blick, dass die letzten drei Fälle sich zu einem zusammenfassen lassen, und zwar ergibt sich so schliesslich:

$$N'_G = \sigma\sigma(P_1 P_2 \cdots P_t) k^{2/n} + \begin{cases} O(k^{\frac{1}{n}}) & \text{für } t_0 = 0, \\ O(k^{\frac{1}{n-1}} (\log k)^{t_0-1}) & \text{für } t_0 \geq 1. \end{cases}$$

22. Um auch die zweite Teilsumme  $N''_G$  nach oben abzuschätzen, muss auf ihre Bedeutung zurückgegangen werden; offenbar stellt sie gerade die Anzahl der Paare ganzer rationaler Zahlen  $p, q$  dar, die den folgenden Bedingungen genügen:

$$|F(p, q)| \leq k Q(p, q), \quad Q(p, q) > \frac{C_0}{2} k^{\frac{1}{n-1}}, \quad |p, q| \leq k^{\frac{1}{n-1}}, \quad (p, q, P_1 P_2 \cdots P_t) = 1.$$

Diese Anzahl ist nach den früheren Ergebnissen für grosses  $k$  sicher gleich Null, wenn  $t_0^* = 0$  ist.

Sei dagegen  $t_0^* > 0$ . Die Gleichung  $F(x, 1) = 0$  möge wieder allein für  $\tau = 1, 2, \dots, t_0^*$  im Körper der  $P_\tau$ -adischen Zahlen lösbar sein. Unter  $P_\pi$  werde die grösste der Primzahlen  $P_1, P_2, \dots, P_t$  verstanden; alsdann bedeute

$$\mathbf{Q} = \{Q_1, Q_2, \dots, Q_r\}$$

die Menge aller Potenzprodukte

$$Q = P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t},$$

mit ganzen rationalen Exponenten, die der Ungleichung

$$\frac{C_0}{2} k^{\frac{1}{n-1}} < Q \leq \frac{C_0}{2} P_\pi k^{\frac{1}{n-1}}$$

genügen und für die die Kongruenz

$$F(p, q) \equiv 0 \pmod{Q}$$

sich in ganzen rationalen Zahlen  $p, q$  mit  $(p, q, P_1 P_2 \cdots P_t) = 1$  lösen lässt. Dazu ist offenbar notwendig, dass die Exponenten  $h_{t_0^*+1}, h_{t_0^*+2}, \dots, h_t$  unterhalb einer von  $k$  unabhängigen Grenze bleiben. Dasselbe Verfahren, das schon mehrfach angewandt wurde, zeigt, dass  $\mathbf{Q}$  nur höchstens

$$O((\log k)^{t_0^*-1})$$

Elemente enthält.

Es werde jetzt für jedes Element  $Q$  aus  $\mathbf{Q}$  unter  $N''(Q)$  die Anzahl der Paare ganzer rationaler Zahlen  $p, q$  mit

$$F(p, q) \equiv 0 \pmod{Q}, \quad |p, q| \leq k^{\frac{1}{n-1}}, \quad (p, q, P_1 P_2 \cdots P_t) = 1$$

verstanden. Da jeder Wert der Funktion  $Q(p, q)$ , der grösser als

$$\frac{C_0}{2} k^{\frac{1}{n-1}}$$

ist, offenbar durch mindestens ein Element  $Q$  aus  $\mathbf{Q}$  teilbar sein muss, so besteht gewiss die Ungleichung

$$N_G'' \leq \sum_{\mathbf{Q}} N''(Q),$$

wobei die Summe über alle Elemente  $Q$  der Menge  $\mathbf{Q}$  zu erstrecken ist.

Damit aber

$$F(p, q) \equiv 0 \pmod{Q}$$

gilt, wo

$$Q = P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}$$

ein Element von  $\mathbf{Q}$  bedeutet, ist notwendigerweise

$$p \equiv p' \pmod{P_1^{h_1+1} P_2^{h_2+1} \cdots P_t^{h_t+1}}, \quad q \equiv q' \pmod{P_1^{h_1+1} P_2^{h_2+1} \cdots P_t^{h_t+1}},$$

und zwar durchlaufen hier  $p', q'$  die sämtlichen  $n^*$  ( $P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}$ ) Elemente der Menge  $m^*(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})$ . Jedes derartige Kongruenzenpaar hat aber an Lösungen, die den Nebenbedingungen

$$|p, q| \leq k^{\frac{1}{n-1}}$$

genügen, wegen

$$Q = P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t} > \frac{C_0}{2} k^{\frac{1}{n-1}}$$

höchstens eine Anzahl, die unterhalb einer von  $k$  unabhängigen Schranke bleibt. Weiter gilt nach 14. die Ungleichung

$$n^*(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}) \leq c P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t} \leq c \frac{C_0}{2} P_n k^{\frac{1}{n-1}}.$$

Also muss gleichmässig in allen Elementen  $Q$  aus  $\mathbf{Q}$

$$N''(Q) = O(k^{\frac{1}{\sigma-1}})$$

sein und demnach

$$N_G'' = O(k^{\frac{1}{\sigma-1}} (\log k)^{\sigma-1}),$$

womit diese Zahl auch im Fall  $t_0^* \geq 1$  nach oben abgeschätzt ist.

23. Nachdem so die beiden Teilanzahlen  $N_G'$  und  $N_G''$  einzeln angenähert berechnet worden sind, ist wegen

$$N_G = N_G' + N_G''$$

der Wert von  $N_G$  auch bekannt, und zwar ergibt sich die Abschätzung

$$N_G = \sigma \sigma(P_1 P_2 \cdots P_t) k^{2/n} + \begin{cases} O(k^{\frac{1}{\sigma}}) & \text{für } t_0 = 0, \\ O(k^{\frac{1}{\sigma-1}} (\log k)^{\sigma-1}) & \text{für } t_0 \geq 1. \end{cases}$$

Damit ist das folgende Ergebnis bewiesen:

### 3. Hauptsatz: Bedeute

$F(x, y)$  eine irreduzible Binärform mit ganzen rationalen Koeffizienten vom Grad  $n \geq 3$ ,

$P_1, P_2, \dots, P_t$  endlichviele verschiedene Primzahlen,

$t_0$  die Anzahl derjenigen Körper unter den Körpern der reellen, der  $P_1$ -adischen, der  $P_2$ -adischen, ..., der  $P_t$ -adischen Zahlen, in denen die Gleichung  $F(x, 1) = 0$  mindestens eine Wurzel hat,

$p$  und  $q$  zwei ganze rationale Zahlen,

$Q(p, q)$  das grösste Potenzprodukt der Primzahlen  $P_1, P_2, \dots, P_t$ , das in  $F(p, q)$  aufgeht,

$\sigma$  das konvergente Integral  $\sigma = \int_{-\infty}^{+\infty} |F(x, 1)|^{-2/n} dx$ ,

$\sigma(P_1 P_2 \cdots P_t)$  die im 2. Hauptsatz definierte Reihe

$$\sigma(P_1 P_2 \cdots P_t) = \sum_{h_1=0}^{\infty} \sum_{h_2=0}^{\infty} \cdots \sum_{h_t=0}^{\infty} d(P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t}) (P_1^{h_1} P_2^{h_2} \cdots P_t^{h_t})^{2/n},$$

$k$  eine über alle Grenzen wachsende positive Zahl,  
 $N_G$  die Anzahl der Paare ganzer rationaler Zahlen  $p, q$ , die dem Bedingungssystem

$$\frac{|F(p, q)|}{Q(p, q)} \leq k, \quad |p, q| \leq k^{\frac{1}{n-1}}, \quad (p, q, P_1 P_2 \cdots P_t) = 1$$

genügen.

Dann besteht die asymptotische Gleichung

$$N_G = \sigma \sigma(P_1 P_2 \cdots P_t) k^{2/n} + \begin{cases} O(k^{\frac{1}{n}}) & \text{für } t_0 = 0, \\ O(k^{\frac{1}{n-1}} (\log k)^{t_0-1}) & \text{für } t_0 \geq 1. \end{cases}$$

(Obwohl der Beweis dieses Satzes ziemlich mühselig war, benutzte er doch nur elementare Kongruenz- und Gitterpunktsbetrachtungen, im Gegensatz zum 1. Hauptsatz, der in ganz entscheidender Weise mehrfach vom Thue-Siegelschen Satz und seiner  $P$ -adischen Verallgemeinerung Gebrauch machte.)

Die Resultate der drei Hauptsätze erlauben ohne Mühe, das gesteckte Ziel zu erreichen und eine asymptotische Formel für die Anzahl der Lösungspaare der beiden Bedingungen

$$\frac{|F(p, q)|}{Q(p, q)} \leq k, \quad (p, q, P_1 P_2 \cdots P_t) = 1,$$

oder der beiden Bedingungen

$$\frac{|F(p, q)|}{Q(p, q)} \leq k, \quad (p, q) = 1$$

anzugeben. Dies werde im letzten Kapitel jetzt dargestellt.

#### IV.

24. Zur Abkürzung werde die Anzahl der Paare ganzer rationaler Zahlen  $p, q$ , die den beiden Bedingungen

$$\frac{|F(p, q)|}{Q(p, q)} \leq k, \quad (p, q, P_1 P_2 \cdots P_t) = 1$$

genügen, mit  $A(k)$ , die Anzahl derjenigen Paare, die den beiden Bedingungen

$$\left| \frac{F(p, q)}{Q(p, q)} \right| \leq k, \quad (p, q) = 1$$

genügen, mit  $A'(k)$  bezeichnet. Diese beiden Anzahlen sind nicht unabhängig von einander, sondern lassen sich auf einander zurückführen.

Ist nämlich  $p, q$  ein Lösungspaar der Bedingungen

$$\left| \frac{F(p, q)}{Q(p, q)} \right| \leq k, \quad (p, q, P_1 P_2 \cdots P_t) = 1,$$

so muss der grösste gemeinsame Teiler von  $p$  und  $q$

$$d = (p, q)$$

teilerfremd zu den sämtlichen Primzahlen  $P_1, P_2, \dots, P_t$  sein, und es gilt also für das Zahlpaar

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

die Ungleichung

$$\left| \frac{F(p', q')}{Q(p', q')} \right| \leq \frac{k}{d^n},$$

da offenbar

$$Q(p', q') = Q(p, q)$$

ist. Somit muss die Gleichung

$$A(k) = \sum A' \left( \frac{k}{d^n} \right)$$

bestehen, wo  $d$  über alle natürlichen Zahlen läuft, in denen keine der Primzahlen  $P_1, P_2, \dots, P_t$  aufgeht. Die hier auftretende Summe ist nur scheinbar unendlich, denn trivialerweise ist

$$A'(k) = 0 \quad \text{für } k < 1.$$

In entsprechender Weise lässt sich  $A'(k)$  durch  $A(k)$  ausdrücken. Zu diesem Zweck werde wie üblich die Möbiussche arithmetische Funktion  $\mu(d)$  eingeführt als Entwicklungskoeffizient der Dirichletschen Reihe

$$\zeta(s)^{-1} = \sum_{d=1}^{\infty} \mu(d) d^{-s}$$

für die Reziproke der Riemannschen Zetafunktion. Es ist bekanntlich

$$\sum_{d'|d} \mu(d') = \begin{cases} 1 & \text{für } d = 1, \\ 0 & \text{für } d > 1, \end{cases}$$

wenn die Summe über alle Teiler  $d'$  von  $d$  erstreckt wird. Auf Grund dieser Beziehung zeigt man leicht die Gleichung

$$A'(k) = \sum \mu(d) A\left(\frac{k}{d^n}\right),$$

wo die Summation wieder über alle natürlichen Zahlen  $d$  läuft, die zu den Primzahlen  $P_1, P_2, \dots, P_t$  teilerfremd sind. Auch die hier auftretende Summe ist nur scheinbar unendlich, denn trivialerweise ist

$$A(k) = 0 \text{ für } k < 1.$$

Da sich auf solche Weise die beiden Anzahlen  $A(k)$  und  $A'(k)$  auf einander zurückführen lassen, so genügt es, eine von beiden zu bestimmen. Die Ergebnisse der drei Hauptsätze liefern am einfachsten eine Formel für die Anzahl  $A(k)$ .

25. Zu diesem Zweck möge die Menge der Lösungspaare von

$$\left| \frac{F(p, q)}{Q(p, q)} \right| \leq k, \quad (p, q, P_1 P_2 \dots P_t) = 1$$

in die Teilmenge mit

$$|p, q| \leq k^{\frac{1}{n-1}}$$

und in die Teilmenge mit

$$|p, q| > k^{\frac{1}{n-1}}$$

zerlegt werden. Was die erste dieser beiden Teilmengen anbelangt, so ist die Anzahl ihrer Elemente nach dem 3. Hauptsatz gleich

$$\sigma\sigma(P_1 P_2 \dots P_t) k^{2/n} + \begin{cases} O(k^{\frac{1}{n}}) & \text{für } t_0 = 0, \\ O(k^{\frac{1}{n-1}} (\log k)^{t_0-1}) & \text{für } t_0 \geq 1. \end{cases}$$

Um auch für die Elementenanzahl der ersten Menge eine Abschätzung zu gewinnen, muss man folgenden Hilfssatz aus dem ersten Teil dieser Arbeit zu Hilfe nehmen<sup>1</sup>:

**Satz 6:** *Werden dieselben Bezeichnungen wie beim 3. Hauptsatz angewandt und sind*

$$\zeta, \zeta', \dots, \zeta^{(v-1)}$$

*die sämtlichen reellen Nullstellen,*

$$\zeta_\tau, \zeta'_\tau, \dots, \zeta_\tau^{(v_\tau-1)}$$

*für  $\tau = 1, 2, \dots, t$  die sämtlichen  $P_\tau$ -adischen Nullstellen des Polynoms*

$$f(x) = F(x, 1),$$

*soweit solche existieren, so besteht für alle Paare ganzer rationaler Zahlen  $p, q$  mit  $q \neq 0$  und  $(p, q, P_1 P_2 \dots P_t) = 1$  die Ungleichung*

$$\frac{|F(p, q)|}{Q(p, q)} \geq \frac{|p, q|^n}{C_5} \min \left( 1, \left| \frac{p}{q} - \zeta \right|, \left| \frac{p}{q} - \zeta' \right|, \dots, \left| \frac{p}{q} - \zeta^{(v-1)} \right| \right) \times \\ \times \prod_{\tau=1}^t \min (1, |p - q \zeta_\tau|_{P_\tau}, |p - q \zeta'_\tau|_{P_\tau}, \dots, |p - q \zeta_\tau^{(v_\tau-1)}|_{P_\tau}).$$

*Dabei bedeutet  $C_5$  eine positive Konstante, die von  $p$  und  $q$  nicht abhängt; ferner ist auf der rechten Seite dieser Ungleichung der Faktor*

$$\min \left( 1, \left| \frac{p}{q} - \zeta \right|, \left| \frac{p}{q} - \zeta' \right|, \dots, \left| \frac{p}{q} - \zeta^{(v-1)} \right| \right)$$

*und jeder der Faktoren*

$$\min (1, |p - q \zeta_\tau|_{P_\tau}, |p - q \zeta'_\tau|_{P_\tau}, \dots, |p - q \zeta_\tau^{(v_\tau-1)}|_{P_\tau}) \quad (\tau = 1, 2, \dots, t)$$

*durch Eins zu ersetzen, falls die zugehörige Anzahl  $v$  bzw.  $v_\tau$  verschwindet.*

Um diesen Hilfssatz auf die Berechnung der Anzahl der Lösungspaare der Bedingungen

$$\frac{|F(p, q)|}{Q(p, q)} \leq k, \quad |p, q| > k^{\frac{1}{n-1}}, \quad (p, q, P_1 P_2 \dots P_t) = 1$$

<sup>1</sup> Siehe I, Hilfssatz 5, S. 722.



anzuwenden, bemerken wir zunächst, dass für hinreichend grosses  $k$  dieses Bedingungssystem keine Lösungspaare  $p, q$  mit  $q = 0$  haben kann; dies ist fast trivial. Somit ist die Anzahl der Lösungspaare höchstens gleich der Anzahl der Paare ganzer rationaler Zahlen  $p, q$ , die den Bedingungen

$$\min \left( 1, \left| \frac{p}{q} - \zeta \right|, \left| \frac{p}{q} - \zeta' \right|, \dots, \left| \frac{p}{q} - \zeta^{(v-1)} \right| \right) \times \\ \times \prod_{\tau=1}^t \min(1, |p - q\zeta_\tau|_{P_\tau}, |p - q\zeta'_\tau|_{P_\tau}, \dots, |p - q\zeta_\tau^{(v_\tau-1)}|_{P_\tau}) \leq C_5 k |p, q|^{-n}, \\ q \neq 0, |p, q| > k^{\frac{1}{n-1}}, (p, q, P_1 P_2 \dots P_t) = 1$$

genügen. Aus dem ersten Hauptsatz und dem Zusatz hierzu geht aber sofort hervor, dass dieses Bedingungssystem

für $t_0 = 0$	keine,
für $t_0 \geq 1$	$O(k^{\frac{1}{n-1}} (\log k)^{t_0-1})$

Lösungspaare  $p, q$  hat, sobald  $k$  hinreichend gross ist.

Damit sind die nötigen Abschätzungen zusammengestellt; aus ihnen ergibt sich der Satz:

**1. Ergebnis:** Die Anzahl  $A(k)$  der Lösungspaare  $p, q$  der beiden Bedingungen

$$\left| \frac{F(p, q)}{Q(p, q)} \right| \leq k, (p, q, P_1 P_2 \dots P_t) = 1$$

ist für grosses  $k$  gleich

$$A(k) = \sigma \prod_{\tau=1}^t \sigma(P_\tau) \cdot k^{2/n} + \begin{cases} O(k^{\frac{1}{n}}) & \text{für } t_0 = 0, \\ O(k^{\frac{1}{n-1}} (\log k)^{t_0-1}) & \text{für } t_0 \geq 1. \end{cases}$$

26. Um zu einer entsprechenden Formel auch für  $A'(k)$  zu gelangen, machen wir Gebrauch von der bekannten Formel

$$\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

Aus derselben folgt leicht die weitere Gleichung

$$\sum_{\substack{d=1 \\ (d, P_1 P_2 \dots P_t)=1}}^{\infty} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2} \prod_{\tau=1}^t (1 - P_{\tau}^{-2})^{-1}.$$

Der Rest dieser Reihe genügt ferner der Ungleichung

$$\left| \sum_{\substack{d > k^{1/n} \\ (d, P_1 P_2 \dots P_t)=1}} \frac{\mu(d)}{d^2} \right| \leq \sum_{d > k^{1/n}} \frac{1}{d^2} = O(k^{-1/n})$$

und somit ist

$$\sum_{\substack{d \leq k^{1/n} \\ (d, P_1 P_2 \dots P_t)=1}} \mu(d) \sigma \prod_{\tau=1}^t \sigma(P_{\tau}) \left(\frac{k}{d^n}\right)^{2/n} = \frac{6\sigma}{\pi^2} \prod_{\tau=1}^t \frac{\sigma(P_{\tau})}{1 - P_{\tau}^{-2}} \cdot k^{2/n} + O(k^{1/n}).$$

Weiter bestehen die beiden Ungleichungen

$$\sum_{d \leq k^{1/n}} \left(\frac{k}{d^n}\right)^{1, n} = O(k^{1/n} \log k),$$

und

$$\sum_{d \leq k^{1/n}} \left\{ \left(\frac{k}{d^n}\right)^{\frac{1}{n-1}} \left(\log \frac{2k}{d^n}\right)^{t_0-1} \right\} = O(k^{n-1} (\log k)^{t_0-1}).$$

Führt man die Abkürzungen

$$\sigma' = \frac{6\sigma}{\pi^2}, \quad \sigma'(P_{\tau}) = \frac{\sigma(P_{\tau})}{1 - P_{\tau}^{-2}}$$

ein und beachtet man, dass nach dem ersten Ergebnis für  $k \geq 1$

$$\left| A(k) - \sigma \prod_{\tau=1}^t \sigma(P_{\tau}) \cdot k^{2/n} \right| \leq \begin{cases} C_6 k^{\frac{1}{n}} & \text{für } t_0 = 0, \\ C_6 k^{n-1} (\log 2k)^{t_0-1} & \text{für } t_0 \geq 1 \end{cases}$$

ist mit einer von  $k$  unabhängigen positiven Konstanten  $C_6$ , berücksichtigt man ferner die Identität

$$A'(k) = \sum_{\substack{d \leq k^{1/n} \\ (d, P_1 P_2 \dots P_t)=1}} \mu(d) A\left(\frac{k}{d^n}\right),$$

so ergibt sich der gesuchte Satz:

**2. Ergebnis:** Die Anzahl  $A'(k)$  der Lösungspaare  $p, q$  der beiden Bedingungen

$$\left| \frac{F(p, q)}{Q(p, q)} \right| \leq k, \quad (p, q) = 1$$

ist für grosses  $k$  gleich

$$A'(k) = \sigma' \prod_{\tau=1}^t \sigma'(P_\tau) \cdot k^{2/n} + \begin{cases} O(k^{\frac{1}{n}}) & \text{für } t_0 = 0, \\ O(k^{\frac{1}{n-1}} (\log k)^{t_0-1}) & \text{für } t_0 \geq 1. \end{cases}$$

Es ist bemerkenswert, dass man für die beiden Grenzwerte

$$\lim_{k \rightarrow \infty} \frac{A(k)}{k^{2/n}} = \sigma \prod_{\tau=1}^t \sigma(P_\tau) \quad \text{und} \quad \lim_{k \rightarrow \infty} \frac{A'(k)}{k^{2/n}} = \sigma' \prod_{\tau=1}^t \sigma'(P_\tau)$$

zu fast gleichartigen Ausdrücken kommt; neben einem Faktor  $\sigma$  bzw.  $\sigma'$ , der gewissermassen die Absolutbetrag-Bewertung repräsentiert, treten Faktoren  $\sigma(P_\tau)$  bzw.  $\sigma'(P_\tau)$  auf, die jeder der  $P_\tau$ -adischen Bewertungen zugeordnet sind. Weiter ist interessant, dass nach diesen Formeln gewissermassen nur 0 % aller Zahlen sich durch die Binärform  $F(x, y)$  darstellen lassen, denn es ist ja

$$A(k) = o(k), \quad A'(k) = o(k),$$

wenn  $k$  über alle Grenzen wächst.

Aus den Ergebnissen 1 und 2 folgt noch:

**3. Ergebnis:** Die Dirichletsche Reihe

$$Z(s) = \sum_{\substack{p=-\infty \\ (p, q, P_1 P_2 \dots P_t)=1}}^{+\infty} \sum_{\substack{q=-\infty \\ (p, q, P_1 P_2 \dots P_t)=1}}^{+\infty} \left( \left| \frac{F(p, q)}{Q(p, q)} \right| \right)^{-s} \quad (s = \sigma_0 + ti)$$

konvergiert für  $\sigma_0 > 2/n$ ; die durch sie dargestellte analytische Funktion hat bei  $s = 2/n$  einen einfachen Pol mit dem Residuum

$$\frac{2}{n} \sigma \prod_{\tau=1}^t \sigma(P_\tau)$$

und lässt sich bis in die Halbebene  $\sigma_0 > 1/n - 1$  fortsetzen, falls  $t_0 \geq 1$  ist, und sogar in die Halbebene  $\sigma_0 > 1/n$ , wenn  $t_0$  den Wert 0 hat.

## 4. Ergebnis: Die Dirichletsche Reihe

$$Z'(s) = \sum_{\substack{p=-\infty \\ (p,q)=1}}^{+\infty} \sum_{q=-\infty}^{+\infty} \left\{ \frac{|F(p,q)|}{Q(p,q)} \right\}^{-s} \quad (s = \sigma_0 + ti)$$

konvergiert für  $\sigma_0 > 2/n$ ; die durch sie dargestellte Funktion hat bei  $s = 2/n$  einen einfachen Pol mit dem Residuum

$$\frac{2}{n} \sigma' \prod_{\tau=1}^t \sigma(P_\tau)$$

und lässt sich bis in die Halbebene  $\sigma_0 > 1/n - 1$  fortsetzen, falls  $t_0 \geq 1$  ist, und bis in die Halbebene  $\sigma_0 > 1/n$ , wenn  $t_0 = 0$  ist.

Es wäre von grossem Interesse, das genaue Existenzgebiet der durch diese Reihen  $Z(s)$  und  $Z'(s)$  definierten Funktionen zu bestimmen; dies wird aber wahrscheinlich nicht leicht sein. Vielleicht lassen sich diese Reihen für die analytische Theorie der Binärformen höheren Grades heranziehen und gelingt es, mit ihrer Hilfe ein Analogon zur Klassenzahlformel von Gauss-Dirichlet für die quadratischen Formen im Gebiete der Formen höheren Grades nachzuweisen.

Amsterdam, im Juni 1933.

