Zur Approximation algebraischer Zahlen. II.

Über die Anzahl der Darstellungen ganzer Zahlen durch Binärformen

Kurt Mahler

Summary. Extending his work in Part I, Mahler now shows that the number of representations of a rational integer g by a binary form $F(x,y)$ is at most $O(|g|^{\varepsilon})$, where ε is any arbitrarily small positive constant.

Acknowledgement. The article

K. Mahler. Zur Approximation algebraischer Zahlen. II. *Math. Ann.*, 108:37–55, 1933.

Zur Approximation algebraischer Zahlen. II.
(Über die Anzahl der Darstellungen ganzer Zahlen durch Binärformen.)

Von

Kurt Mahler in Göttingen.

Im ersten Teil dieser Arbeit wurde gezeigt, *daß sich durch eine irreduzible Binärform* $F(x, y)$ *mit ganzen rationalen Koeffizienten vom Grad* $n \geqq 3$ *höchstens endlichviele Potenzprodukte gegebener endlichvieler Primzahlen eigentlich*, d. h. mit teilerfremden ganzen rationalen Zahlen $x = p$, $y = q$, *darstellen lassen.*

In diesem zweiten Teil wird mittels einiger einfacher Abschätzungen *eine Schranke für die Anzahl dieser darstellbaren Potenzprodukte* gewonnen. Das Ergebnis lautet:

„*Zu der irreduziblen Binärform* $F(x, y)$ *mit ganzen rationalen Koeffizienten vom Grad* $n \geqq 3$ *läßt sich eine positive Zahl* c_4 *angeben mit der folgenden Eigenschaft: Sind* $P_1, P_2, \ldots, P_t$ *irgend endlichviele gegebene Primzahlen, so gibt es höchstens* c_4^{t+1} *verschiedene Paare* p, q *teilerfremder ganzer rationaler Zahlen, für die* $F(p, q)$ *allein durch diese Primzahlen teilbar ist.*"

Aus diesem Satz werden verschiedene Folgerungen gezogen; so ergibt sich z. B., daß *die Anzahl aller Darstellungen großer ganzer rationaler Zahlen* g *durch die Binärform* $F(x, y)$ *höchstens gleich* $O(|g|^{\varepsilon})$ ist, wobei ε eine beliebig kleine positive Konstante bedeuten darf.

I.

1. Im ersten Teil dieser Arbeit wurde folgender Satz bewiesen[1]):

Hilfssatz 1: *Bedeute*:

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

a *die Zahl* $|\overline{f(x)}|$,

ζ *eine reelle Nullstelle von* $f(x)$,

$P_1, P_2, \ldots, P_t$ t *verschiedene Primzahlen*,

ζ_τ *für* $\tau = 1, 2, \ldots, t$ *eine* P_τ*-adische Nullstelle von* $f(x)$,

s *eine natürliche Zahl kleiner als* n,

[1]) Siehe Hilfssatz 3, S. 709 im ersten Teil dieser Arbeit, Math. Annalen **107** (1933), S. 691–730.

ϑ, Θ, k drei positive Zahlen mit

$$\beta = \frac{n}{s+1} + s + \Theta \leqq n, \quad \vartheta \leqq \frac{1}{2}, \quad \vartheta < \frac{\Theta}{\beta}, \qquad k \geqq 1,$$

K die aus ihnen gebildete positive Zahl

$$K = (4a)^{\frac{\left(\frac{n}{s+1}+\vartheta\right)\left(3+\frac{n}{\vartheta}\right)}{\min(1,\,\Theta-\beta\vartheta)}} \, k^{\frac{1-\frac{s}{\beta}+\vartheta}{\Theta-\beta\vartheta}},$$

$\Gamma_1, \Gamma_2, \ldots, \Gamma_t$ im Fall $(0, t)$ t positive Zahlen der Summe Eins,
$\Gamma_0, \Gamma_1, \Gamma_2, \ldots, \Gamma_t$ im Fall $(1, t)$ $t+1$ positive Zahlen der Summe Eins.

Die Paare p, q teilerfremder ganzer rationaler Zahlen, die der Ungleichung

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

bzw. der Ungleichung

$(0, 1)$: $$|p - q\zeta_\tau|_{P_\tau} \leqq k\,|p, q|^{-\beta},$$

bzw. den t Ungleichungen

$(0, t)$: $$|p - q\zeta_\tau|_{P_\tau} \leqq (k\,|p, q|^{-\beta})^{\Gamma_\tau} \qquad (\tau = 1, 2, \ldots, t),$$

bzw. den $t+1$ Ungleichungen

$(1, t)$: $$\left|\frac{p}{q} - \zeta\right| \leqq (k\,|p, q|^{-\beta})^{\Gamma_0}, \quad |p - q\zeta_\tau|_{P_\tau} \leqq (k\,|p, q|^{-\beta})^{\Gamma_\tau} \quad (\tau = 1, 2, \ldots, t)$$

genügen, befriedigen entweder alle die Ungleichung $|p, q| \leqq K$, oder es gibt auch solche Lösungen mit $|p, q| > K$, und wenn p_0, q_0 eine von ihnen mit möglichst kleinem $|p_0, q_0| > K$ ist, so befriedigen alle anderen Lösungen p, q mit $|p, q| > K$ die Ungleichung

$$|p_0, q_0| \leqq |p, q| < \left(k^{-\frac{1}{\beta}}\,|p_0, q_0|\right)^{\frac{2n^3}{\vartheta}}.$$

Es wurde ferner gezeigt[2]):

Hilfssatz 2: *Gelten dieselben Bezeichnungen wie im vorigen Hilfssatz, ist β^* eine positive Zahl größer als β und v eine natürliche Zahl mit*

$$v \geqq \frac{\beta}{\beta^* - \beta}(t+1),$$

so kann jedem Paar teilerfremder ganzer rationaler Zahlen p, q mit $|p, q| > k^{1/\beta}$, das der Ungleichung

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

genügt, auf eindeutige Weise ein System von $t+1$ nichtnegativen ganzen rationalen Zahlen $f_0, f_1, f_2, \ldots, f_t$ mit

$$f_0 + f_1 + f_2 + \cdots + f_t = v$$

[2]) Siehe den Beweis von Satz 1 im ersten Teil dieser Arbeit, S. 710.

zugeordnet werden, so daß auch die Ungleichungen

$$\min\left(1, \left|\frac{p}{q}-\zeta\right|\right) \leqq (k\,|p,q|^{-\beta})^{\frac{f_0}{v}},$$

$$\min(1, |p-q\zeta_\tau|_{P_\tau}) \leqq (k\,|p,q|^{-\beta})^{\frac{f_\tau}{v}} \qquad (\tau = 1, 2, \ldots, t)$$

bestehen. Für das System der Zahlen $f_0, f_1, f_2, \ldots, f_t$ *gibt es genau*

$$\binom{v+t}{t}$$

verschiedene Möglichkeiten.

2. Vermöge dieser beiden Hilfssätze soll eine obere Schranke hergeleitet werden für die Anzahl der gekürzten Brüche $\frac{p}{q}$ mit positivem Nenner, die der Ungleichung

$$(1, 0): \qquad \left|\frac{p}{q}-\zeta\right| \leqq k\,|p,q|^{-\beta}$$

oder der Ungleichung

$$(0, 1): \qquad |p-q\zeta_\tau|_{P_\tau} \leqq k\,|p,q|^{-\beta}$$

oder den t Ungleichungen

$$(0, t): \qquad |p-q\zeta_\tau|_{P_\tau} \leqq (k\,|p,q|^{-\beta})^{\Gamma_\tau} \qquad (\tau = 1, 2, \ldots, t)$$

oder den $t+1$ Ungleichungen

$$(1, t): \left|\frac{p}{q}-\zeta\right| \leqq (k\,|p,q|^{-\beta})^{\Gamma_0}, \quad |p-q\zeta_\tau|_{P_\tau} \leqq (k\,|p,q|^{-\beta})^{\Gamma_\tau} \quad (\tau = 1, 2, \ldots, t)$$

oder schließlich der einen Ungleichung

$$(t+1): \qquad \min\left(1, \left|\frac{p}{q}-\zeta\right|\right) \prod_{\tau=1}^{t} \min(1, |p-q\zeta_\tau|_{P_\tau}) \leqq k\,|p,q|^{-\beta^*}$$

genügen.

Seien $\frac{p_1}{q_1}$ und $\frac{p_2}{q_2}$ zwei verschiedene Lösungen von (1, 0), (0, 1), (0, t) oder (1, t), also ohne Einschränkung

$$(p_1, q_1) = 1, \quad (p_2, q_2) = 1, \quad q_1 > 0, q_2 > 0, \quad \frac{p_1}{q_1} \neq \frac{p_2}{q_2}, \quad |p_1, q_1| \leqq |p_2, q_2|.$$

Dann bestehen die Ungleichungen

$$2\max\left(\left|\frac{p_1}{q_1}-\zeta\right|, \left|\frac{p_2}{q_2}-\zeta\right|\right) \geqq \left|\left(\frac{p_1}{q_1}-\zeta\right)-\left(\frac{p_2}{q_2}-\zeta\right)\right|$$
$$\geqq \frac{|p_1 q_2 - p_2 q_1|}{|p_1, q_1|\,|p_2, q_2|} \geqq \frac{1}{|p_1, q_1|\,|p_2, q_2|},$$

$$\max(|p_1-q_1\zeta_\tau|_{P_\tau}, |p_2-q_2\zeta_\tau|_{P_\tau}) \geqq |q_2(p_1-q_1\zeta_\tau)-q_1(p_2-q_2\zeta_\tau)|_{P_\tau}$$
$$= |p_1 q_2 - p_2 q_1|_{P_\tau} \geqq \frac{1}{2\,|p_1, q_1|\,|p_2, q_2|}.$$

Aus ihnen folgt im Fall (1, 0):

$$\frac{1}{|p_1, q_1|\,|p_2, q_2|} \leqq 2\max\left(\left|\frac{p_1}{q_1}-\zeta\right|, \left|\frac{p_2}{q_2}-\zeta\right|\right)$$
$$\leqq 2\max(k\,|p_1, q_1|^{-\beta}, k\,|p_2, q_2|^{-\beta}) = 2k\,|p_1, q_1|^{-\beta},$$

im Fall (0, 1):

$$\frac{1}{2|p_1, q_1||p_2, q_2|} \leqq \max(|p_1 - q_1\zeta_\tau|_{P_\tau}, |p_2 - q_2\zeta_\tau|_{P_\tau})$$
$$\leqq \max(k|p_1, q_1|^{-\beta}, k|p_2, q_2|^{-\beta}) = k|p_1, q_1|^{-\beta},$$

im Fall (0, t):

$$\frac{1}{2|p_1, q_1||p_2, q_2|} \leqq \prod_{\tau=1}^{t} |p_1 q_2 - p_2 q_1|_{P_\tau}$$
$$\leqq \prod_{\tau=1}^{t} \max(|p_1 - q_1\zeta_\tau|_{P_\tau}, |p_2 - q_2\zeta_\tau|_{P_\tau})$$
$$\leqq \prod_{\tau=1}^{t} \max((k|p_1, q_1|^{-\beta})^{\Gamma_\tau}, (k|p_2, q_2|^{-\beta})^{\Gamma_\tau}) = k|p_1, q_1|^{-\beta},$$

und im Fall (1, t):

$$\frac{1}{|p_1, q_1||p_2, q_2|} \leqq \frac{|p_1 q_2 - p_2 q_1| \prod_{\tau=1}^{t} |p_1 q_2 - p_2 q_1|_{P_\tau}}{|p_1, q_1||p_2, q_2|}$$
$$\leqq 2\max\left(\left|\frac{p_1}{q_1} - \zeta\right|, \left|\frac{p_2}{q_2} - \zeta\right|\right) \prod_{\tau=1}^{t} \max(|p_1 - q_1\zeta_\tau|_{P_\tau}, |p_2 - q_2\zeta_\tau|_{P_\tau})$$
$$\leqq 2\max((k|p_1, q_1|^{-\beta})^{\Gamma_0}, (k|p_2, q_2|^{-\beta})^{\Gamma_0}) \times$$
$$\times \prod_{\tau=1}^{t} \max((k|p_1, q_1|^{-\beta})^{\Gamma_\tau}, (k|p_2, q_2|^{-\beta})^{\Gamma_\tau}) = 2k|p_1, q_1|^{-\beta}.$$

Folglich müssen in allen vier Fällen zwei verschiedene Lösungen $\frac{p_1}{q_1}$ und $\frac{p_2}{q_2}$ durch dieselbe Ungleichung

$$\frac{1}{2|p_1, q_1||p_2, q_2|} \leqq k|p_1, q_1|^{-\beta} \quad \text{oder} \quad |p_2, q_2| \geqq \frac{1}{2k}|p_1, q_1|^{\beta-1}$$

miteinander verknüpft sein.

3. Nach Hilfssatz 1 muß für jeden Lösungsbruch $\frac{p}{q}$ von (1, 0), (0, 1), (0, t) oder (1, t) entweder

$$|p_0, q_0| \leqq |p, q| < (k^{-\frac{1}{\beta}}|p_0, q_0|)^{\frac{2n^2}{\vartheta}} \qquad (|p_0, q_0| > K)$$

oder

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

oder

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

sein. Diese drei Intervalle für $|p, q|$ seien zur Abkürzung der Reihe nach mit J_1, J_2 und J_3 bezeichnet.

Das Intervall J_1 beginnt wegen $|p_0, q_0| > K$ rechts von

$$K \geqq (4a)^{\frac{\left(\frac{n}{s+1}+\vartheta\right)\left(3+\frac{n}{\vartheta}\right)}{\Theta-\beta\vartheta}} k^{\frac{1-\frac{s}{\beta}+\vartheta}{\Theta-\beta\vartheta}};$$

aus

$$\left(\frac{n}{s+1}+\vartheta\right)\left(3+\frac{n}{\vartheta}\right) > \left(\frac{n}{n}+\vartheta\right)(3+0) > 1-\frac{s}{\beta}+\vartheta$$

folgt daher

$$|p_0, q_0| > K > (4ak)^{\frac{1-\frac{s}{\beta}+\vartheta}{\Theta-\beta\vartheta}} > (2k)^{\frac{1-\frac{s}{\beta}+\vartheta}{\Theta-\beta\vartheta}}.$$

Zu den Voraussetzungen von Hilfssatz 1 trete von jetzt ab noch die weitere Annahme

$$\Theta-\beta\vartheta \leqq \frac{1}{2}\left(1-\frac{s}{\beta}+\vartheta\right)(\beta-2).$$

Dann ist

$$|p_0, q_0| > (2k)^{\frac{2}{\beta-2}}, \quad \left(k^{-\frac{1}{\beta}}|p_0, q_0|\right)^{\frac{2n^3}{\vartheta}} \leqq |p_0, q_0|^{\frac{2n^3}{\vartheta}}.$$

Im Intervall J_1 habe jetzt irgend eins der vier Probleme (1, 0), (0, t), (0, t), (1, t) insgesamt die μ Lösungen

$$\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_\mu}{q_\mu}$$

in gekürzten Brüchen mit positivem Nenner. Ohne Einschränkung der Allgemeinheit darf

$$\begin{aligned}(2k)^{\frac{2}{\beta-2}} < |p_0, q_0| \leqq |p_1, q_1| \leqq |p_2, q_2| \leqq \cdots \\ \leqq |p_\mu, q_\mu| < \left(k^{-\frac{1}{\beta}}|p_0, q_0|\right)^{\frac{2n^3}{\vartheta}} \leqq |p_0, q_0|^{\frac{2n^3}{\vartheta}}\end{aligned}$$

angenommen werden. Nach 2. ist aber dann

$$|p_{\lambda+1}, q_{\lambda+1}| \geqq \frac{1}{2k}|p_\lambda, q_\lambda|^{\beta-1} \quad \lambda = 1, 2, \ldots, \mu-1),$$

und demnach besteht die Ungleichung

$$\begin{aligned}|p_\mu, q_\mu| \geqq \left(\frac{1}{2k}\right)^{1+(\beta-1)+\cdots+(\beta-1)^{\mu-2}} |p_1, q_1|^{(\beta-1)^{\mu-1}} \\ > \left((2k)^{-\frac{1}{\beta-2}}|p_1, q_1|\right)^{(\beta-1)^{\mu-1}},\end{aligned}$$

daher erst recht die Ungleichung

$$|p_0, q_0|^{\frac{2n^3}{\vartheta}} > \left((2k)^{-\frac{1}{\beta-2}}|p_0, q_0|\right)^{(\beta-1)^{\mu-1}}$$

und wegen

$$|p_0, q_0| > (2k)^{\frac{2}{\beta-2}}$$

die Ungleichung

$$|p_0, q_0|^{\frac{2n^3}{\vartheta}} > |p_0, q_0|^{\frac{1}{2}(\beta-1)^{\mu-1}}.$$

Hierin ist gewiß $|p_0, q_0|$ größer als Eins und β größer als Zwei, so daß man nach μ auflösen kann und folgende Schranke hierfür bekommt:

$$\mu < 1 + \frac{\log \frac{4n^3}{\vartheta}}{\log(\beta - 1)}.$$

In entsprechender Weise gelangt man zu einer oberen Schranke für die Anzahl der sämtlichen gekürzten Brüche mit positivem Nenner

$$\frac{p_{\mu+1}}{q_{\mu+1}}, \frac{p_{\mu+2}}{q_{\mu+2}}, \ldots, \frac{p_{\mu+\nu}}{q_{\mu+\nu}},$$

für die $|p, q|$ im Intervall J_3 liegt und die einem der vier Probleme (1, 0), (0, 1), (0, t), (1, t) genügen. Ohne Einschränkung der Allgemeinheit darf

$$(4k)^{\frac{1}{\beta-2}} \leqq |p_{\mu+1}, q_{\mu+1}| \leqq |p_{\mu+2}, q_{\mu+2}| \leqq \cdots \leqq |p_{\mu+\nu}, q_{\mu+\nu}| \leqq K$$

vorausgesetzt werden. Dann ist ebenso wie vorhin

$$|p_{\mu+\nu}, q_{\mu+\nu}| > \left((2k)^{-\frac{1}{\beta-2}} |p_{\mu+1}, q_{\mu+1}|\right)^{(\beta-1)^{\nu-1}},$$

also erst recht

$$K > 2^{(\beta-1)^{\nu-1}}$$

und

$$\nu < 1 + \frac{\log \frac{\log K}{\log 2}}{\log(\beta-1)}.$$

Was schließlich die Anzahl o der Lösungen $\frac{p}{q}$ eines der vier Probleme mit $|p, q|$ im Intervall J_3 anbetrifft, so gibt es überhaupt nur höchstens

$$\left(2(4k)^{\frac{1}{\beta-2}} + 1\right)(4k)^{\frac{1}{\beta-2}} < 3(4k)^{\frac{2}{\beta-2}}$$

gekürzte oder ungekürzte Brüche $\frac{p}{q}$ mit

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

folglich ist

$$o < 3(4k)^{\frac{2}{\beta-2}}.$$

4. Damit ist gezeigt, daß *jedes der vier Probleme* (1, 0), (0, 1), (0, t), (1, t) *nicht mehr als*

$$\mu + \nu + o < 2 + \frac{\log \frac{4n^3}{\vartheta} + \log \frac{\log K}{\log 2}}{\log(\beta-1)} + 3(4k)^{\frac{2}{\beta-2}}$$

Lösungen in gekürzten Brüchen $\frac{p}{q}$ *mit positivem Nenner* besitzt. Diese Schranke hat bemerkenswerterweise in allen Fällen denselben Wert und ist vor allem *unabhängig von den Zahlen* Γ.

Hieraus folgt auch eine obere Schranke für die Anzahl der Lösungen der Ungleichung $(t+1)$ in gekürzten Brüchen $\frac{p}{q}$ mit positivem Nenner. An Lösungen mit $|p, q| < (4k)^{\frac{1}{\beta-2}}$ kann auch diese Ungleichung nicht mehr als

$$3(4k)^{\frac{2}{\beta-2}}$$

haben. Es ist aber

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

Aus Hilfssatz 2 folgt also, daß jeder Lösung $\frac{p}{q}$ des Problems mit

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

sich ein System von $t+1$ nichtnegativen ganzen rationalen Zahlen $f_0, f_1, f_2, \ldots, f_t$ der Summe v eindeutig zuordnen läßt, so daß gleichzeitig

$$\min\left(1, \left|\frac{p}{q} - \zeta\right|\right) \leqq (k|p, q|^{-\beta})^{\frac{f_0}{v}},$$

$$\min(1, |p - q\zeta_\tau|_{P_\tau}) \leqq (k|p, q|^{-\beta})^{\frac{f_\tau}{v}} \qquad (\tau = 1, 2, \ldots, t)$$

ist. Möge jetzt eine von den Zahlen f, etwa f_τ, von Null verschieden sein. Dann ist

$$(k|p, q|^{-\beta})^{\frac{f_\tau}{v}} < 1,$$

so daß bei der betreffenden Ungleichung links das Minimum nicht gleich Eins sein kann. Der Bruch $\frac{p}{q}$ muß also einem Problem $(1, 0)$ oder $(0, 1)$ oder $(0, t)$ oder $(1, t)$ genügen, wobei die Zahlen Γ gerade gleich den positiven unter den Zahlen $\frac{f}{v}$ sind. Für das System der Zahlen f gibt es nun genau $\binom{v+t}{t}$ verschiedene Möglichkeiten; einem von soviel verschiedenen Ungleichungssystemen einer der Arten $(1, 0)$, $(0, 1)$, $(0, t)$, $(1, t)$ muß demnach $\frac{p}{q}$ genügen. Aus den oberen Schranken für μ und ν folgt somit, daß *die Ungleichung* $(t+1)$ *höchstens*

$$3(4k)^{\frac{2}{\beta-2}} + \binom{v+t}{t}\left(2 + \frac{\log\frac{4n^3}{\vartheta} + \log\frac{\log K}{\log 2}}{\log(\beta-1)}\right)$$

verschiedene Lösungen in gekürzten Brüchen $\frac{p}{q}$ *mit positivem Nenner* besitzt.

5. Die letzten Schranken können noch auf eine für die Anwendung bequemere Form gebracht werden. Nach C. Siegel genügt die Zahl

$$\alpha = \min_{s=1,2,\ldots,n-1}\left(\frac{n}{s+1} + s\right)$$

der Ungleichung
$$2\sqrt{n}-1 \leqq \alpha \leqq \sqrt{4n+1}-1;$$
ihr Wert wird angenommen an der Stelle
$$s = \left[\frac{\sqrt{4n+1}-1}{2}\right].$$
Über β und Θ werde so verfügt, daß
$$\beta = \alpha + \Theta, \quad 0 < \Theta \leqq \frac{1}{4n}$$
ist. Wegen $n \geqq 3$ hat man dann
$$\alpha - 2 \geqq \tfrac{1}{2}, \quad \alpha - s \geqq 1, \quad \alpha \leqq n,$$
also
$$\Theta - \beta\vartheta < \Theta \leqq \frac{1}{4n} \leqq \frac{(\alpha-2)(\alpha-s)}{2\alpha}$$
$$= \tfrac{1}{2}(\alpha-2)\left(1-\frac{s}{\alpha}\right) < \tfrac{1}{2}(\beta-2)\left(1-\frac{s}{\beta}+\vartheta\right),$$
so daß die zuletzt erhobene Forderung
$$\Theta - \beta\vartheta \leqq \tfrac{1}{2}(\beta-2)\left(1-\frac{s}{\beta}+\vartheta\right)$$
für jedes $\vartheta > 0$ erfüllt ist. Die andere Voraussetzung
$$\Theta - \beta\vartheta > 0$$
wird durch die Wahl
$$\vartheta = \frac{\Theta}{\alpha+1+\Theta}$$
erfüllt, denn es ist
$$\Theta - \beta\vartheta = \vartheta > 0.$$
Die Zahl ϑ liegt im Intervall
$$\frac{\Theta}{\sqrt{4n+1}+\Theta} \leqq \vartheta \leqq \frac{\Theta}{2\sqrt{n}+\Theta}.$$
Da wegen $n \geqq 3$
$$\Theta \leqq \frac{1}{4n} \leqq \frac{1}{12}$$
ist, so gilt demnach
$$\vartheta \leqq \frac{\frac{1}{12}}{2\sqrt{3}} < \frac{1}{24} < \frac{1}{2}.$$
Es ist also
$$\frac{n}{s+1} + \vartheta \leqq \frac{n}{2} + \vartheta = \frac{n+2\vartheta}{2} < \frac{n+1}{2}, \qquad 3 + \frac{n}{\vartheta} = \frac{n+3\vartheta}{\vartheta} < \frac{n+1}{\vartheta}$$
und folglich
$$\frac{\left(\frac{n}{s+1}+\vartheta\right)\left(3+\frac{n}{\vartheta}\right)}{\min(1, \Theta-\beta\vartheta)} < \frac{(n+1)^2}{2\vartheta^2} = \frac{(n+1)^2(\alpha+1+\Theta)^2}{2\Theta^2},$$
ferner
$$1 - \frac{s}{\beta} + \vartheta < 1 - 0 + \frac{1}{2} = \frac{3}{2}$$

und folglich

$$\frac{1-\frac{s}{\beta}+\vartheta}{\Theta-\beta\vartheta}<\frac{3}{2\vartheta}=\frac{3}{2}\,\frac{(\alpha+1+\Theta)}{\Theta}.$$

Endlich ist

$$\frac{4n^3}{\vartheta}=\frac{4n^3(\alpha+1+\Theta)}{\Theta}.$$

Durch Verschlechtern können diese Ausdrücke noch etwas vereinfacht werden. Es ist

$$\alpha-1\geqq 2(\sqrt{n}-1),\quad \alpha-1\geqq\frac{3}{2},$$

also

$$\frac{\alpha+1+\Theta}{\alpha-1}\leqq\frac{\alpha+1+\frac{1}{12}}{\alpha-1}=1+\frac{\frac{35}{12}}{\alpha-1}\leqq 1+\frac{50}{36}<3,$$

$$\frac{n+1}{(\alpha-1)^2}\leqq\frac{n+1}{4(\sqrt{n}+1)^2}=\frac{n+1}{4(n+1-2\sqrt{n})}\leqq\frac{4}{4(4-2\sqrt{3})}<\frac{1}{4-\frac{7}{2}}=2,$$

$$\frac{n}{(\alpha-1)^2}\leqq\frac{n+1}{(\alpha-1)^2}<2.$$

Folglich bestehen die folgenden drei Ungleichungen

$$\frac{\left(\frac{n}{s+1}+\vartheta\right)\left(3+\frac{n}{\vartheta}\right)}{\min(1,\Theta-\beta\vartheta)}<\frac{4(\alpha-1)^4\cdot 9(\alpha-1)^2}{2\Theta^2}=\frac{18(\alpha-1)^6}{\Theta^2},$$

$$\frac{1-\frac{s}{\beta}+\vartheta}{\Theta-\beta\vartheta}<\frac{3}{2}\,\frac{3(\alpha-1)}{\Theta}=\frac{9}{2}\,\frac{(\alpha-1)}{\Theta},$$

$$\frac{4n^3}{\vartheta}<\frac{4\cdot 8(\alpha-1)^6\cdot 3(\alpha-1)}{\Theta}=\frac{96(\alpha-1)^7}{\Theta}.$$

Wegen der numerischen Identitäten

$$2\cdot 18<(\tfrac{3}{2})^{10},\quad 2\cdot\tfrac{9}{2}<(\tfrac{3}{2})^6,\quad 96<(\tfrac{3}{2})^{12},\quad \log 2>0{,}693>(\tfrac{3}{2})^{-1},$$

folgt aus ihnen

$$K<(4a)^{\frac{1}{2}\left(\frac{3}{2}\right)^{10}\frac{(\alpha-1)^6}{\Theta^2}}\,k^{\frac{1}{2}\left(\frac{3}{2}\right)^{6}\frac{\alpha-1}{\Theta}},\qquad \frac{4n^3}{\vartheta}<\frac{(\frac{3}{2})^{12}(\alpha-1)^7}{\Theta},$$

$$\frac{\log\frac{1}{\log 2}}{\log(\beta-1)}<\frac{\log\frac{3}{2}}{\log(\alpha-1)}\leqq 1.$$

In der ersten dieser drei Ungleichungen ist entweder

$$(4a)^{\frac{1}{2}\left(\frac{3}{2}\right)^{10}\frac{(\alpha-1)^6}{\Theta^2}}>k^{\frac{1}{2}\left(\frac{3}{2}\right)^{6}\frac{\alpha-1}{\Theta}},\quad \text{d. h. } K<(4a)^{\left(\frac{3}{2}\right)^{10}\frac{(\alpha-1)^6}{\Theta^2}};$$

dann erhält man

$$\frac{\log\log K}{\log(\beta-1)}<\frac{\log\log K}{\log(\alpha-1)}<\frac{\log(\frac{3}{2})^{10}}{\log(\frac{3}{2})}+\frac{\log(\alpha-1)^6}{\log(\alpha-1)}+\frac{\log\log(4a)}{\log(\alpha-1)}+\frac{2\log\frac{1}{\Theta}}{\log(\alpha-1)}$$

oder

$$\frac{\log\frac{\log K}{\log 2}}{\log(\beta-1)}<17+\frac{\log\log(4a)+2\log\frac{1}{\Theta}}{\log(\alpha-1)}.$$

Oder es ist

$$(4a)^{\frac{1}{2}\left(\frac{3}{2}\right)^{10}\frac{(\alpha-1)^6}{\vartheta^2}} \leqq k^{\frac{1}{2}\left(\frac{3}{2}\right)^6\frac{\alpha-1}{\vartheta}}, \quad \text{d. h. } K < k^{\left(\frac{3}{2}\right)^6\frac{\alpha-1}{\vartheta}},$$

und man bekommt

$$\frac{\log\log K}{\log(\beta-1)} < \frac{\log\log K}{\log(\alpha-1)} < \frac{\log\left(\frac{3}{2}\right)^6}{\log\left(\frac{3}{2}\right)} + \frac{\log(\alpha-1)}{\log(\alpha-1)} + \frac{\log\frac{1}{\Theta}}{\log(\alpha-1)} + \frac{\log\log k}{\log(\alpha-1)}$$

oder

$$\frac{\log\frac{\log K}{\log 2}}{\log(\beta-1)} < 8 + \frac{\log\log k + \log\frac{1}{\Theta}}{\log(\alpha-1)}.$$

Aus der zweiten Ungleichung erhält man entsprechenderweise

$$\frac{\log\frac{4n^3}{\vartheta}}{\log(\beta-1)} < 19 + \frac{\log\frac{1}{\Theta}}{\log(\alpha-1)}.$$

Faßt man die letzten Ungleichungen zusammen, so kommt man also zu den beiden Ungleichungen

$$2 + \frac{\log\frac{4n^3}{\vartheta} + \log\frac{\log K}{\log 2}}{\log(\beta-1)} + 3(4k)^{\frac{2}{\beta-2}}$$

$$< 3(4k)^{\frac{2}{\beta-2}} + \max\left(38 + \frac{\log\log(4a) + 3\log\frac{1}{\Theta}}{\log(\alpha-1)},\ 29 + \frac{\log\log k + 2\log\frac{1}{\Theta}}{\log(\alpha-1)}\right)$$

und

$$3(4k)^{\frac{2}{\beta-2}} + \binom{v+t}{t}\left(2 + \frac{\log\frac{4n^3}{\vartheta} + \log\frac{\log K}{\log 2}}{\log(\beta-1)}\right)$$

$$< 3(4k)^{\frac{2}{\beta-2}} + \binom{v+t}{t}\max\left(38 + \frac{\log\log(4a) + 3\log\frac{1}{\Theta}}{\log(\alpha-1)},\ 29 + \frac{\log\log k + 2\log\frac{1}{\Theta}}{\log(\alpha-1)}\right).$$

Die rechte Seite der ersten Ungleichung liefert eine obere Schranke für die Anzahl der gekürzten Brüche $\frac{p}{q}$ mit positivem Nenner, die einem der Probleme (1, 0), (0, 1), (0, t), (1, t) genügen, die rechte Seite der zweiten Ungleichung eine obere Schranke für die Anzahl der gekürzten Brüche $\frac{p}{q}$ mit positivem Nenner, die dem Problem ($t+1$) genügen. Damit ist bewiesen[8]):

Hilfssatz 3: *Bedeute:*

$f(x)$ ein irreduzibles Polynom mit ganzen rationalen Koeffizienten vom Grad $n \geqq 3$ und mit $a = |\overline{f(x)}|$,

---

[8]) In ähnlicher Weise kann für $\beta = n$ gezeigt werden, daß das Ungleichungssystem $[t+1]$ höchstens

$$(4(2k)^{\frac{1}{n-2}} + 1)^2 + \max\left(24 + \frac{\log\log(4a)}{\log(n-1)},\ 16 + \frac{\log\log k}{\log(n-1)}\right)$$

Lösungen besitzt.

ζ *eine reelle Nullstelle von* $f(x)$,
$P_1, P_2, \ldots, P_t$ *endlichviele verschiedene Primzahlen*,
ζ_τ *für* $\tau = 1, 2, \ldots, t$ *eine* P_τ*-adische Nullstelle von* $f(x)$,
$\Gamma_0, \Gamma_1, \Gamma_2, \ldots, \Gamma_t$ $t+1$ *nichtnegative Zahlen der Summe Eins*,
$\alpha, \Theta, \beta, \beta^*, k$ *positive Zahlen mit*

$$\alpha = \min_{s=1,2,\ldots,n-1}\left(\frac{n}{s+1}+s\right),\ 0<\Theta\leqq\frac{1}{4n},\ \beta=\alpha+\Theta,\ \beta^*>\beta,\ k\geqq 1,$$

v *eine natürliche Zahl mit*

$$v \geqq \frac{\beta}{\beta^*-\beta}(t+1).$$

Dann gibt es höchstens

$$3(4k)^{\frac{2}{\beta-2}} + \max\left(38+\frac{\log\log(4a)+3\log\frac{1}{\Theta}}{\log(\alpha-1)},\ 29+\frac{\log\log k+2\log\frac{1}{\Theta}}{\log(\alpha-1)}\right)$$

verschiedene gekürzte Brüche mit positivem Nenner, die den Ungleichungen

$$[t+1]:\qquad \begin{aligned}&\min\left(1, \left|\frac{p}{q}-\zeta\right|\right) \leqq (k|p, q|^{-\beta})^{\Gamma_0},\\ &\min(1, |p-q\zeta_\tau|_{P_\tau}) \leqq (k|p, q|^{-\beta})^{\Gamma_\tau}, \qquad (\tau = 1, 2, \ldots, t)\end{aligned}$$

genügen; ebenso gibt es höchstens

$$3(4k)^{\frac{2}{\beta-2}} + \binom{v+t}{t}\max\left(38+\frac{\log\log(4a)+3\log\frac{1}{\Theta}}{\log(\alpha-1)},\ 29+\frac{\log\log k+2\log\frac{1}{\Theta}}{\log(\alpha-1)}\right)$$

verschiedene gekürzte Brüche mit positivem Nenner, für die

$$(t+1):\quad \min\left(1, \left|\frac{p}{q}-\zeta\right|\right)\prod_{\tau=1}^{t}\min(1, |p-q\zeta_\tau|_{P_\tau}) \leqq k|p, q|^{-\beta^*}$$

ist.

Dieser Satz gibt eine Übersicht über die Abhängigkeit der Lösungsanzahlen der Probleme $[t+1]$ und $(t+1)$ von den auftretenden Parametern. Nach ihm sind die beiden Lösungsanzahlen als Funktion von k von der Größenordnung

$$O(k^{\frac{2}{\beta-2}}),$$

als Funktion von ζ, d.h. von $f(x)$, von der Größenordnung

$$O(\log\log(4a)).$$

Im folgenden wird aber vor allem die Abhängigkeit der Lösungsanzahl des Problems $(t+1)$ von der Anzahl t der betrachteten Primzahlen $P_1, P_2, \ldots, P_t$ zu untersuchen sein. Dazu werde v als Funktion von t durch die Ungleichung

$$\frac{\beta}{\beta^*-\beta}(t+1) \leqq v < \frac{\beta}{\beta^*-\beta}(t+1)+1$$

eindeutig festgelegt, so daß

$$\frac{\beta^*}{\beta^*-\beta}t + \frac{\beta}{\beta^*-\beta} \leqq v+t < \frac{\beta^*}{\beta^*-\beta}(t+1)$$

und demnach
$$\binom{v+t}{t} \leqq \sum_{l=0}^{v+t} \binom{v+t}{l} = 2^{v+t} \leqq 2^{\frac{\beta^*}{\beta^*-\beta}(t+1)}$$
ist. Die Anzahl der Lösungen von $(t+1)$ ist also kleiner als
$$3\,(4\,k)^{\frac{2}{\beta-2}} + 2^{\frac{\beta^*}{\beta^*-\beta}(t+1)} \max\left(38 + \frac{\log\log(4\,a) + 3\log\frac{1}{\Theta}}{\log(\alpha-1)},\ 29 + \frac{\log\log k + 2\log\frac{1}{\Theta}}{\log(\alpha-1)}\right).$$
Jetzt werde eine beliebige, aber hinreichend kleine positive Zahl ε vorgegeben; dann kann man eine positive Zahl $\Theta \leqq \frac{1}{4n}$ bestimmen, so daß
$$\frac{\beta^*}{\beta^*-\beta} = \frac{\beta^*}{\beta^*-\alpha}(1+\varepsilon)$$
ist. Durch diese Wahl wird der vorige Ausdruck kleiner als
$$c_0 \,.\, 2^{\frac{\beta^*}{\beta^*-\alpha}(1+\varepsilon)\,t},$$
wobei c_0 eine positive Zahl bedeutet, die wohl von n, a, β^*, ε und k abhängt, nicht aber von den Primzahlen $P_1, P_2, \ldots, P_t$ und ihrer Anzahl t.

Indem statt β^* wieder β geschrieben wird, läßt sich dies Ergebnis folgendermaßen aussprechen:

Satz 4: *Bedeute:*

$f(x)$ ein irreduzibles Polynom mit ganzen rationalen Koeffizienten vom Grad $n \geqq 3$ und mit $a = \overline{|f(x)|}$,

ζ eine reelle Nullstelle von $f(x)$,

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

ζ_τ für $\tau = 1, 2, \ldots, t$ eine P_τ-adische Nullstelle von $f(x)$,

α und β zwei positive Zahlen mit
$$\alpha = \min_{s=1,2,\ldots,n-1}\left(\frac{n}{s+1}+s\right),\quad \beta > \alpha,\quad \beta \leqq n,$$
ε und k zwei positive Zahlen.

Dann gibt es eine positive Zahl c_0, die allein von n, a, β, ε und k abhängt, nicht aber von den Primzahlen $P_1, P_2, \ldots, P_t$ und ihrer Anzahl t, so daß die Ungleichung
$$\min\left(1, \left|\frac{p}{q}-\zeta\right|\right) \prod_{\tau=1}^{t} \min(1, |p - q\,\zeta_\tau|_{P_\tau}) \leqq k\,|p, q|^{-\beta}$$
durch höchstens
$$c_0 \,.\, 2^{\frac{\beta}{\beta-\alpha}(1+\varepsilon)\,t}$$
verschiedene gekürzte Brüche $\frac{p}{q}$ mit positivem Nenner befriedigt wird.

(Die beim Beweis dieses Satzes gemachten Einschränkungen, daß ε hinreichend klein und $k \geqq 1$ ist, sind offenbar überflüssig bei der Fassung, die für ihn gewählt ist.)

II.

6. Im ersten Teil dieser Arbeit wurde folgender Satz bewiesen[4]):

Hilfssatz 5: *Bedeute:*

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

$\zeta, \zeta', \ldots, \zeta^{(\nu-1)}$ die sämtlichen reellen Nullstellen von $f(x) \equiv F(x, 1)$,

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

$\zeta_\tau, \zeta'_\tau, \ldots, \zeta_\tau^{(\nu_\tau-1)}$ für $\tau = 1, 2, \ldots, t$ die sämtlichen P_τ-adischen Nullstellen des Polygoms $f(x)$,

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

$Q(p, q)$ das größte Potenzprodukt der Primzahlen P_τ, das in der Zahl $F(p, q)$ aufgeht.

Dann gibt es eine positive Konstante c_1, die wohl von der Binärform $F(x, y)$ abhängt, nicht aber von den Primzahlen $P_1, P_2, \ldots, P_t$ und ihrer Anzahl t, so daß stets

$$\frac{|F(p,q)|}{Q(p,q)} \geqq c_1 |p, q|^n \min\left(1, \left|\frac{p}{q} - \zeta\right|, \left|\frac{p}{q} - \zeta'\right|, \ldots, \left|\frac{p}{q} - \zeta^{(\nu-1)}\right|\right) \times$$
$$\times \prod_{\tau=1}^{t} \min\left(1, |p - q\zeta_\tau|_{P_\tau}, |p - q\zeta'_\tau|_{P_\tau}, \ldots, |p - q\zeta_\tau^{(\nu_\tau-1)}|_{P_\tau}\right)$$

ist.

Dieser Satz, zusammen mit Satz 4, führt zu weiteren Ergebnissen über die Anzahl der Darstellungen ganzer rationaler Zahlen durch die Binärform $F(x, y)$.

Dazu werde die Menge der Primzahlen $P_1, P_2, \ldots, P_t$ in zwei Teilmengen

$$P_1, P_2, \ldots, P_r \text{ und } P_{r+1}, P_{r+2}, \ldots, P_{r+s} \qquad (r + s = t$$

zerlegt, so daß für $\tau = 1, 2, \ldots, r$ die Zahl ν_τ mindestens gleich Eins und natürlich höchstens gleich n ist, für $\tau = r+1, r+2, \ldots, r+s$ dagegen $\nu_\tau = 0$ gilt. Dies ist durch geeignete Numerierung immer möglich. Die Faktoren

$$\min\left(1, |p - q\zeta_\tau|_{P_\tau}, |p - q\zeta'_\tau|_{P_\tau}, \ldots, |p - q\zeta_\tau^{(\nu_\tau-1)}|_{P_\tau}\right) = 1$$

können in der Ungleichung des letzten Satzes fortgelassen werden und es muß daher auch die Ungleichung

$$\frac{|F(p,q)|}{Q(p,q)} \geqq c_1 |p, q|^n \min\left(1, \left|\frac{p}{q} - \zeta\right|, \left|\frac{p}{q} - \zeta'\right|, \ldots, \left|\frac{p}{q} - \zeta^{(\nu-1)}\right|\right) \times$$
$$\times \prod_{\tau=1}^{r} \min\left(1, |p - q\zeta_\tau|_{P_\tau}, |p - q\zeta'_\tau|_{P_\tau}, \ldots, |p - q\zeta_\tau^{(\nu_\tau-1)}|_{P_\tau}\right)$$

---

[4]) Siehe Teil 1, Hilfssatz 5, S. 722.

stets gelten. Ist auch $\nu = 0$, so darf rechts der Faktor

$$\min\left(1, \left|\frac{p}{q} - \zeta\right|, \left|\frac{p}{q} - \zeta'\right|, \ldots, \left|\frac{p}{q} - \zeta^{(\nu-1)}\right|\right) = 1$$

gleichfalls fortgelassen werden.

In Satz 4 werde nun die Zahl k gleich

$$k = \frac{1}{c_1}$$

gewählt. Nach diesem Satz hat jede Ungleichung

$$\min\left(1, \left|\frac{p}{q} - \zeta^{(\mu)}\right|\right) \prod_{\tau=1}^{r} \min(1, |p - q\zeta_\tau^{(\mu_\tau)}|_{P_\tau}) \leqq k\,|p, q|^{-\beta}$$

höchstens

$$c_2 \cdot 2^{\frac{\beta}{\beta-\alpha}(1+\varepsilon)r}$$

verschiedene Lösungen in teilerfremden ganzen rationalen Zahlen p, q mit $q \neq 0$, wenn μ_τ für jedes $\tau = 1, 2, \ldots, r$ irgendeiner der Indizes $0, 1, \ldots, \nu_\tau - 1$ und μ einer der Indizes $0, 1, \ldots, \nu - 1$ ist, ferner c_2 eine gewisse positive Zahl bedeutet, die nicht von den Primzahlen P_1, $P_2, \ldots, P_t$ oder von den Anzahlen r, s, t abhängt. Dieselbe Ungleichung für die Lösungsanzahl bleibt auch noch bestehen, wenn $\nu = 0$ sein sollte, also $f(x)$ gar keine reelle Nullstellen hat, so daß

$$\min\left(1, \left|\frac{p}{q} - \zeta^{(\mu)}\right|\right) \text{ durch } 1$$

zu ersetzen ist.

Nun können für jede der Zahlen μ_τ höchstens ν_τ verschiedene Indizes gewählt werden, ebenso, wenn $\nu \neq 0$ ist, für die Zahl μ höchstens ν. Also hat für $\nu \geqq 1$ die Ungleichung

$$\begin{aligned}\min\left(1, \left|\frac{p}{q} - \zeta\right|, \left|\frac{p}{q} - \zeta'\right|, \ldots, \left|\frac{p}{q} - \zeta^{(\nu-1)}\right|\right) \times \\ \times \prod_{\tau=1}^{r} \min(1, |p - q\zeta_\tau|_{P_\tau}, |p - q\zeta'_\tau|_{P_\tau}, \ldots, |p - q\zeta_\tau^{(\nu_\tau-1)}|_{P_\tau}) \\ \leqq k\,|p, q|^{-\beta}\end{aligned}$$

höchstens

$$c_2 \cdot 2^{\frac{\beta}{\beta-\alpha}(1+\varepsilon)r}\, \nu\, \nu_1 \ldots \nu_r$$

und für $\nu = 0$ die Ungleichung

$$\prod_{\tau=1}^{r} \min(1, |p - q\zeta_\tau|_{P_\tau}, |p - q\zeta'_\tau|_{P_\tau}, \ldots, |p - q\zeta_\tau^{(\nu_\tau-1)}|_{P_\tau}) \leqq k\,|p, q|^{-\beta}$$

höchstens

$$c_2 \cdot 2^{\frac{\beta}{\beta-\alpha}(1+\varepsilon)r}\, \nu_1 \nu_2 \ldots \nu_r$$

verschiedene Lösungen in teilerfremden ganzen rationalen Zahlen p, q mit $q \neq 0$. Diese beiden Ergebnisse lassen sich zu der Aussage zusammenfassen, daß die Ungleichung

$$\min\left(1, \left|\frac{p}{q}-\zeta\right|, \left|\frac{p}{q}-\zeta'\right|, \ldots, \left|\frac{p}{q}-\zeta^{(\nu-1)}\right|\right) \times$$
$$\times \prod_{\tau=1}^{t} \min\left(1, |p-q\zeta_\tau|_{P_\tau}, |p-q\zeta'_\tau|_{P_\tau}, \ldots, |p-q\zeta_\tau^{(\nu_\tau-1)}|_{P_\tau}\right)$$
$$\leqq k\,|p, q|^{-\beta}$$

höchstens

$$c_2 \cdot 2^{\frac{\beta}{\beta-\alpha}(1+s)r} \max(1, \nu) \prod_{\tau=1}^{t} \max(1, \nu_\tau)$$

verschiedene Lösungen in ganzen rationalen teilerfremden Zahlen p, q mit $q \neq 0$ besitzt.

Für alle Zahlpaare p, q, die dieser Ungleichung nicht genügen, besteht aber nach Hilfssatz 5 die Ungleichung

$$\frac{|F(p, q)|}{Q(p, q)} > c_1 |p, q|^n \cdot k\,|p, q|^{-\beta} = |p, q|^{n-\beta}.$$

Es gibt ferner an Paaren p, q teilerfremder ganzer rationaler Zahlen mit $q = 0$ nur die beiden $1, 0$ und $-1, 0$. Indem man auch diese noch dadurch mitberücksichtigt, daß man von c_2 zu einer geeigneten größeren Zahl c_3 übergeht, folgt schließlich:

Satz 6: *Bedeute*:

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

ν die Anzahl der reellen Nullstellen des Polynoms $f(x) \equiv F(x, 1)$,

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

ν_τ für $\tau = 1, 2, \ldots, t$ die Anzahl der P_τ-adischen Nullstellen des Polynoms $f(x)$,

r die Anzahl derjenigen unter den Zahlen $\nu_1, \nu_2, \ldots, \nu_t$, die nicht verschwinden,

p und q zwei beliebige teilerfremde ganze rationale Zahlen,

$Q(p, q)$ das größte Potenzprodukt der Primzahlen P_τ, das in der Zahl $F(p, q)$ aufgeht,

α, β zwei positive Zahlen mit

$$\alpha = \min_{s=1, 2, \ldots, n-1} \left(\frac{n}{s+1} + s\right), \quad \beta > \alpha, \quad \beta \leqq n,$$

ε eine positive Zahl.

4*

Dann gibt es eine positive Zahl c_3, die wohl von der Binärform $F(x, y)$, von β und ε, nicht aber von den Primzahlen $P_1, P_2, \ldots, P_t$ und den Anzahlen t und r abhängt, so daß die Ungleichung

$$\frac{|F(p, q)|}{Q(p, q)} \leqq |p, q|^{n-\beta}$$

durch höchstens

$$c_3 \, . \, 2^{\frac{\beta}{\beta-\alpha}(1+\varepsilon) r} \max(1, \nu) \prod_{\tau=1}^{t} \max(1, \nu_\tau)$$

Paare p, q befriedigt wird.

7. Aus Satz 6 lassen sich mehrere Folgerungen über die Darstellung von ganzen rationalen Zahlen durch die Form $F(x, y)$ herleiten.

Es ist trivialerweise

$$\nu \leqq n, \quad \nu_\tau \leqq n \qquad (\tau = 1, 2, \ldots, t),$$

also für $\varepsilon = 1$, $\beta = n$, und mit t statt r

$$c_3 \, . \, 2^{\frac{\beta}{\beta-\alpha}(1+\varepsilon) r} \max(1, \nu) \prod_{\tau=1}^{t} \max(1, \nu_\tau) \leqq c_4^{t+1},$$

wo c_4 eine positive Zahl ist, die nur noch von der Binärform $F(x, y)$ abhängt. Die Anzahl der teilerfremden ganzen rationalen Zahlpaare p, q mit

$$|F(p, q)| \leqq Q(p, q), \quad \text{also} \quad |F(p, q)| = Q(p, q),$$

d. h. derjenigen Paare, für die $F(p, q)$ allein aus den t Primzahlen $P_1, P_2, \ldots, P_t$ zusammengesetzt ist, ist demnach höchstens gleich c_4^{t+1}. Diese Aussage läßt sich auf zwei verschiedene Weisen interpretieren. Erstens ergibt sich:

Folgerung 1: *Zu der irreduziblen Binärform $F(x, y)$ mit ganzen rationalen Koeffizienten vom Grad $n \geqq 3$ läßt sich eine nur von ihr abhängige positive Zahl c_4 angeben mit folgender Eigenschaft: Sind irgendwelche endlichvielen verschiedenen Primzahlen gegeben, etwa mit der Anzahl t, so gibt es höchstens c_4^{t+1} verschiedene ganze rationale Zahlen g, die allein durch diese Primzahlen teilbar sind und sich durch die Binärform $F(x, y)$ eigentlich,* d. h. mit teilerfremden ganzen rationalen Zahlen $x = p$, $y = q$, *darstellen lassen.*

Zweitens ergibt sich:

Folgerung 2: *Zu der irreduziblen Binärform $F(x, y)$ mit ganzen rationalen Koeffizienten vom Grad $n \geqq 3$ läßt sich eine nur von ihr abhängige positive Zahl c_4 angeben mit folgender Eigenschaft: Ist g irgendeine ganze rationale und von Null verschiedene Zahl, in der etwa genau t verschiedene*

Primzahlen aufgehen, so läßt sich g auf höchstens c_4^{t+1} verschiedene Arten eigentlich durch die Binärform $F(x, y)$ darstellen.

Ist g selbst eine Primzahl, so sind offenbar alle Darstellungen dieser Zahl durch die Binärform von selbst eigentlich; man erhält also das merkwürdige Ergebnis, daß die *Anzahl der Darstellungen dieser Primzahl durch $F(x, y)$ unterhalb einer Schranke liegt, die allein von der Binärform abhängt.*

8. Die Folgerung 2 führt weiter zu einer einfachen oberen Schranke für die Anzahl der sämtlichen Darstellungen der großen ganzen rationalen Zahl g durch die feste Binärform $F(x, y)$. Sei diese Anzahl zur Abkürzung mit $A(g)$ bezeichnet; sei ferner $a(g)$ die Anzahl der sämtlichen eigentlichen Darstellungen von g durch die Binärform. Offenbar besteht dann die Formel

$$A(g) = \sum_{\substack{d=1 \\ d^n \mid g}}^{\infty} a\left(\frac{g}{d^n}\right),$$

wo die Summe über alle natürlichen Zahlen d zu erstrecken ist, deren n-te Potenz in g aufgeht. Ist nun t die Anzahl der in g aufgehenden Primzahlen und daher nicht kleiner als die Anzahl der in den Zahlen $\frac{g}{d^n}$ aufgehenden Primzahlen, so ist nach Folgerung 2:

$$a\left(\frac{g}{d^n}\right) \leqq c_4^{t+1} \qquad \left(\begin{matrix} d = 1, 2, 3, \dots \\ d^n \mid g \end{matrix}\right).$$

Da d^n in g aufgehen muß, so gibt es ferner für d höchstens $\tau(|g|)$ Möglichkeiten, wenn $\tau(|g|)$ die Anzahl der positiven Teiler von g bedeutet. Die Identität für $A(g)$ ergibt demnach

$$A(g) \leqq \tau(|g|)\, c_4^{t+1}.$$

Nach bekannten elementaren Sätzen über Primzahlen ist aber für alle großen natürlichen Zahlen g[5]):

$$\log \tau(|g|) = O\left(\frac{\log |g|}{\log\log |g|}\right), \quad t = O\left(\frac{\log |g|}{\log\log |g|}\right)$$

und folglich

$$\log A(g) \leqq O\left(\frac{\log |g|}{\log\log |g|}\right).$$

Damit ist folgender Satz bewiesen:

Folgerung 3: Zu der irreduziblen Binärform $F(x, y)$ mit ganzen rationalen Koeffizienten vom Grad $n \geqq 3$ läßt sich eine nur von ihr ab-

[5]) Vgl. E. Landau, Handbuch der Lehre von der Verteilung der Primzahlen, Bd. 1 (1909), B. G. Teubner, Leipzig, S. 220—222, wo sogar viel mehr bewiesen wird.

hängige positive Zahl c_5 *angeben mit folgender Eigenschaft: Ist g eine ganze rationale Zahl mit hinreichend großem Absolutbetrag, so ist die Anzahl der Darstellungen von g in der Gestalt*

$$g = F(p, q)$$

mit ganzen rationalen nicht notwendig teilerfremden Zahlen p und q höchstens gleich

$$c_5^{\frac{\log |g|}{\log \log |g|}},$$

also insbesondere für jede positive Zahl ε von der Größenordnung

$$O(|g|^{\varepsilon}).$$

In diesem Satz ist enthalten, daß die Konvergenzabszisse der Dirichletschen Reihe

$$\sum_{\substack{g=-\infty \\ g \neq 0}}^{+\infty} \frac{A(g)}{|g|^{s}} = \sum_{p=-\infty}^{+\infty} \sum_{\substack{q=-\infty \\ p^2+q^2 \neq 0}}^{+\infty} |F(p, q)|^{-s}$$

nicht größer als Eins ist; der genaue Wert ist nach C. Siegel (1925) gleich $\frac{2}{n}$, also kleiner.

9. Nach Trygve Nagell strebt für großes p die größte Primzahl, die in dem Produkt

$$f(1) f(2) \ldots f(p)$$

aufgeht, zu einer höheren Größenordnung gegen Unendlich, als p; dabei bedeutet $f(x)$ ein Polynom mit ganzen rationalen Koeffizienten, das mindestens eine irrationale Nullstelle hat[6]). Ein ähnliches, aber nicht so scharfes Ergebnis für Binärformen läßt sich aus Folgerung 2 herleiten. Es gilt folgender Satz:

Folgerung 4: Zu der irreduziblen Binärform $F(x, y)$ *mit ganzen rationalen Koeffizienten vom Grad* $n \geqq 3$ *läßt sich eine nur von ihr abhängige positive Zahl* c_6 *angeben mit folgender Eigenschaft: Ist m eine genügend große natürliche Zahl und sind*

$$p_1, q_1;\ p_2, q_2;\ \ldots;\ p_m, q_m$$

m verschiedene Paare teilerfremder ganzer rationaler Zahlen, so ist die größte Primzahl, die in dem Produkt

$$F(p_1, q_1) F(p_2, q_2) \ldots F(p_m, q_m)$$

aufgeht, größer als $c_6 \log m \log \log m$.

[6]) Siehe Tr. Nagell, „Zur Arithmetik der Polynome", Abhandlungen aus dem math. Seminar der Hamburgischen Universität 1, S. 179 (1922).

Beweis: Bedeute c_4 die Konstante aus Folgerung 1; ohne Einschränkung ist sie größer als Eins. Zu der großen natürlichen Zahl m läßt sich eindeutig eine natürliche Zahl t bestimmen, die der Ungleichung

$$c_4^t + 1 \leqq m < c_4^{t+1} + 1$$

genügt. Dann können nach Folgerung 1 die Zahlen

$$F(p_1, q_1), F(p_2, q_2), \ldots, F(p_m, q_m)$$

nicht alle nur aus den $t-1$ ersten Primzahlen zusammengesetzt sein, denn ihre Anzahl m ist größer als c_4^t. Also muß in ihrem Produkt eine Primzahl aufgehen, die größer oder gleich der t-ten Primzahl ist. Nach bekannten Sätzen über Primzahlen ist jedoch die t-te Primzahl größer als $\frac{1}{2} t \log t$, wenn t genügend groß ist[7]). Ferner ist nach Definition

$$t > \frac{\log (m-1)}{\log c_4} - 1,$$

und daraus folgt die Behauptung.

[7]) Siehe [5]), S. 214.

(Eingegangen am 4. 6. 1932.)