EINE ARITHMETISCHE EIGENSCHAFT DER REKURRIERENDEN REIHEN.

VON

KURT MAHLER.

(In Groningen).

---

1. Sei

$$F(x, y) = x^2 + pxy + qy^2$$

eine quadratische Binärform mit ganzen rationalen Koeffizienten und

$$\Delta = p^2 - 4q \neq 0, \quad q \neq 0, \quad (p, q) = 1.$$

Die beiden Wurzeln

$$\xi = \frac{-p + \sqrt{\Delta}}{2}, \qquad \eta = \frac{-p - \sqrt{\Delta}}{2}$$

der zugehörigen quadratischen Gleichung

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

sind also von einander und von Null verschieden.

Unter einer zu $F(x, y)$ gehörigen rekurrierenden Reihe werde jede Folge

$$w_k \qquad (k = 1, 2, 3, \ldots.)$$

ganzer rationalen Zahlen verstanden, die derselben Rekursionsformel

$$w_{k+2} + pw_{k+1} + qw_k = 0 \qquad (k = 1, 2, 3, \ldots)$$

genügt; eine solche Folge ist vollständig durch die beiden Anfangsglieder w_1 und w_2 bestimmt.

Durch

$$u_k = \frac{\xi^k - \eta^k}{\xi - \eta}, \quad v_k = \xi^k + \eta^k \qquad (k = 1, 2, 3, \ldots.)$$

werden zwei spezielle zu $F(x, y)$ gehörige rekurrierende Reihen definiert; sie haben die Anfangsglieder

$$u_1 = 1, \quad u_2 = -p \quad \text{und} \quad v_1 = -p, \quad v_2 = p^2 - 2q.$$

Diese beiden Reihen sind mit einander durch die Identitäten

$$v_k^2 - \Delta u_k^2 = 4q^k \qquad (k = 1, 2, 3, \ldots.)$$

verknüpft; wegen $(p, q) = 1$ ist demnach (u_k, v_k) ein Teiler von 2.

2. Da die Determinante
$$u_1 v_2 - u_2 v_1 = -2q$$
nach Voraussetzung nicht verschwindet, so gibt es drei ganze rationale Zahlen U, V, W mit $W \neq 0$, so dass
$$W w_k = U u_k + V v_k$$
für $k = 1$ und $k = 2$ ist, wegen der Rekursionsformeln für u_k, v_k, w_k also für jedes natürliche k gilt.

Wit schliessen den trivialen Fall
$$w_1 = w_2 = w_3 = \ldots . = 0$$
im Folgenden aus; mindestens eine der beiden Zahlen U und V ist demnach von Null verschieden. Wir setzen ferner voraus, dass keiner der beiden Quotienten
$$\frac{w_k}{\xi^k} \quad \text{und} \quad \frac{w_k}{\eta^k}$$
für alle k einen von k unabhängigen Wert besitzt; demnach ist
$$\frac{U}{V} \neq + \sqrt{\Delta} \quad \text{und} \quad \frac{U}{V} \neq - \sqrt{\Delta}.$$
Die kubische Binärform mit ganzen rationalen Koeffizienten
$$G(x, y) = (y^2 - \Delta x^2)\ (Ux + Uy)$$
verschwindet demnach nicht identisch, und die drei Nullstellen
$$+\frac{1}{\sqrt{\Delta}},\ -\frac{1}{\sqrt{\Delta}},\ -\frac{V}{U}$$
des zugeordneten Polynoms
$$G(x, 1) = (1 - \Delta x^2)\ (Ux + V)$$
sind alle von einander verschieden.

3. In meiner Arbeit: „*Zur Approximation algebraischer Zahlen*, Teil I'' (Math. Annalen 107 (1933), 691—730) bewies ich folgenden Satz: „*Die Binärform* $H(x, y) \not\equiv 0$ *habe ganze rationale Koeffizienten, uud das zugehörige Polynom* $H(x, 1)$ *besitze mindestens drei verschiedene Nullstellen, wobei auch eine etwaige Nullstelle* ∞ *mitzuzählen ist. Sind dann* x *und* y *teilerfremde ganze rationale Zahlen und strebt max* $(|x|, |y|)$ *über alle Grenzen, so wächst auch die grösste in* $H(x, y)$ *aufgehende Primzahl gegen Unendlich.*''

Dieser Satz werde speziell auf die Form $G(x, y)$ angewandt. Man hat
$$G(u_k, v_k) = 4q^k \,.\, W w_k \qquad (k = 1, 2, 3, \ldots .)$$

und es gilt

$$\delta_k = (u_k, v_k) = 1 \text{ oder } = 2 \qquad (k = 1, 2, 3, \ldots .).$$

Falls für $k \to \infty$

$$\lim_{k \to \infty} \max (|u_k|, |v_k|) = \infty$$

ist, muss also die grösste in

$$G\left(\frac{u_k}{\delta_k}, \frac{v_k}{\delta_k}\right) = \frac{4q^k \,.\, Ww_k}{{\delta_k}^3}$$

und also auch die grösste in w_k aufgehende Primzahl und demnach erst recht $|w_k|$ selbst über alle Grenzen wachsen.

Nun kann offenbar nur dann für eine unendliche Folge

$$k = k_1, k_2, k_3, \ldots\ldots$$

jede der beiden Zahlen

$$u_k, \quad v_k$$

absolut beschränkt sein, wenn auch die beiden Zahlen

$$\xi^k, \quad \eta^k$$

absolut beschränkt sind; dies verlangt, dass

$$|\xi| \leq 1 \quad \text{und} \quad |\eta| \leq 1$$

sei. Demnach muss sogar

$$|\xi| = |\eta| = 1, \quad q = \mp 1$$

sein. Damit diese Bedingungen erfüllt sind, muss die rekurrierende Folge w_k notwendigerweise zu einer der Binärformen

$$x^2 - y^2, \quad x^2 + y^2, \quad x^2 \mp xy + y^2$$

gehören, und dies ist natürlich auch hinreichend. Von diesen vier uninteressanten Fällen werde abgesehen; dann ergibt sich der folgende Satz:

,,*Die quadratische Binarform*

$$F(x, y) = x^2 + pxy + qy^2$$

habe ganz rationale Koeffizienten mit

$$\Delta = p^2 - 4q \neq 0, \quad q \neq 0, \quad (p, q) = 1,$$

und sie sei verschieden von den vier Formen

$$x^2 - y^2, \quad x^2 + y^2, \quad x^2 \mp xy + y^2.$$

Die Folge ganzer rationaler Zahlen

$$w_1, w_2, w_3, \ldots\ldots\ldots$$

genüge den Rekursionsformeln

$$w_{k+2} + pw_{k+1} + qw_k = 0 \qquad (k = 1, 2, 3, \ldots .)$$

und es besitze keiner der beiden Ausdrucke

$$w_k\left(\frac{-p + \sqrt{\Delta}}{2}\right)^{-k} \quad \text{und} \quad w_k\left(\frac{-p - \sqrt{\Delta}}{2}\right)^{-k}$$

für alle k einen von k unabhängigen Wert. Mit wachsendem k strebt dann $|w_k|$ und sogar die grosste in w_k aufgehende Primzahl über alle Grenzen.''

4. Das Beweisverfahren in 3. lässt sich verallgemeinern. Man wendet den allgemeinen Primteilersatz zu diesem Zweck nicht auf

$$(y^2 - \Delta x^2)\ (\mathrm{U}x + \mathrm{V}y),$$

sondern auf die Binärform

$$(y^2 - \Delta x^2)\ \mathrm{K}(x, y)$$

an, wobei $\mathrm{K}(x, y) \not\equiv 0$ eine Binärform mit ganzen rationalen Koeffizienten bedeutet, die teilerfremd zu der speziellen Form

$$y^2 - \Delta x^2$$

ist. Unter den an $\mathrm{F}(x, y)$ gemachten Voraussetzungen strebt dann die grösste in

$$\mathrm{K}(v_k,\ u_k) = z_k \qquad (k = 1, 2, 3, \ldots .)$$

aufgehende Primzahl mit k über alle Grenzen, und hier bilden die z_k, wie man leicht zeigt, eine rekurrierende Reihe, jedoch natürlich von höherer als zweiter Ordnung.

Es wäre von Interesse, die erhaltenen Ergebnisse mit elementareren Mitteln als der hier benutzten Verallgemeinerung des Thue-Siegelschen Satzes abzuleiten. Falls man statt w_k eine der beiden speziellen Folgen u_k und v_k nimmt, wird dies vielleicht möglich sein mittels der bekannten einfachen Teilbarkeitsgesetze dieser beiden Reihen. Siehe hierzu die schöne Darstellung der Theorie der rekurrierenden Reihen von Bessel—Hagen in Pascals Repertorium I 3 (1929), Kapitel XXVII, § 19.

Krefeld, 1. September 1934.