[5] H. S. M. Coxeter, *Extreme forms*, Can. J. Math. 3 (1951), p. 391-441.
[6] — and J. A. Todd, *An extreme duodenary form*, Can. J. Math. 5 (1951), p. 384-392.
[7] A. Korkine and G. Zolotareff, *Sur les formes quadratiques positives*, Math. Ann. 11 (1877), p. 242-292.
[8] H. Minkowski, *Diskontinuitätsbereich für arithmetische Äquivalenz*, J. reine angew. Math. 129 (1905), p. 220-274.
[9] L. J. Mordell, *Observation on the minimum of a positive quadratic form in eight variables*, J. Lond. Math. Soc. 19 (1944), p. 3-6.
[10] G. Voronoi, *Sur quelques propriétés des formes quadratiques positives parfaites*, J. reine angew. Math. 133 (1908), p. 97-178.
[11] — *Recherches sur les paralléloèdres primitifs* (Part 1), ibid. 134 (1908), p. 198-287.

UNIVERSITY OF SYDNEY, AUSTRALIA

Reçu par la Rédaction le 10. 11. 1958

ACTA ARITHMETICA
V (1959)

Zur Theorie der algebraischen Gleichungen über endlichen Körpern

von

L. Rédei (Szeged) und P. Turán (Budapest)

Dem Andenken von S. Lubelski, des ersten Herausgebers der Acta Arithmetica gewidmet.

1. Einer der schönsten Sätze der Theorie der Kongruenzen höheren Grades (welche Lubelski selbst mit vielen schönen Forschungen bereichert hat) ist der folgende Satz von König-Rados [2]:

Es sei eine Kongruenz

$$a_0+a_1x+\ldots+a_{p-2}x^{p-2} \equiv 0 \pmod p \qquad (p \nmid a_0) \tag{1.1}$$

vorgelegt (p *Primzahl*, a_ν *ganze rationale Zahl*). *Dann ist die Anzahl der verschiedenen inkongruenten Lösungen von* (1.1) *gleich*

$$p-1-r_p;$$

r_p *bedeutet den Rang* mod p *der zyklischen Matrix*

$$Z_1 = \begin{bmatrix} a_0 & a_1 & a_2 & \ldots & a_{p-2} \\ a_{p-2} & a_0 & a_1 & \ldots & a_{p-3} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_1 & a_2 & a_3 & \ldots & a_0 \end{bmatrix}. \tag{1.2}$$

Ein vereinfachter Beweis dieses Satzes ist in Kronecker's Vorlesungen über die Zahlentheorie ([1], p. 389) gegeben; ein viel einfacherer Beweis und die Erweiterung auf endliche Körper war von dem ersten von uns gefunden ([3]). Er bewies den folgenden Satz:

In einem endlichen Körper K mit q Elementen sei eine Gleichung

$$a_0+a_1x+\ldots+a_{q-2}x^{q-2} = 0 \qquad (a_0 \neq 0) \tag{1.3}$$

vorgelegt ($a_\nu \in K$). *Dann ist die Anzahl der verschiedenen Lösungen von* (1.3) *gleich*

$$q-1-r;$$

r bedeutet den Rang der zyklischen Matrix

$$Z_2 = \begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_{q-2} \\ a_{q-2} & a_0 & a_1 & \dots & a_{q-3} \\ \dots & \dots & \dots & \dots & \dots \\ a_1 & a_2 & a_3 & \dots & a_0 \end{bmatrix}. \tag{1.4}$$

Was die Anwendbarkeit dieser Sätze anbelangt, kennen wir nur zwei Arbeiten von Vandiver ([4] und [5]), wo sie angewendet sind. Die Ursache des Fehlens weiterer Anwendungen liegt offenbar in der Schwierigkeit der Bestimmung des Ranges von Z_1 oder Z_2. Es ist also wünschenswert eine solche Form dieser Sätze zu geben, welche den Anwendungen besser angepasst ist. Ein solcher ist der folgende

Satz. *Die Anzahl der verschiedenen Lösungen der Gleichung* (1.3) *ist gleich*

$$q-1-r_{\text{hms}},$$

wobei r_{hms} den „Hauptminorsummenrang" der Matrix Z_2 in (1.4) *bezeichnet.*

Unter „Hauptminorensummenrang" r_{hms} verstehen wir die maximale ganze rationale Zahl k, für welche die Summe aller Hauptminoren k-ter Ordnung von Z_2 nicht verschwindet. Dieser läßt sich in vielen Fällen einfach berechnen, wo die Bestimmung des gewöhnlichen Ranges ziemlich schwer ist; auf dieses Problem und nebst Anwendungen unseres Satzes werden wir bei einer anderen Gelegenheit zurückkommen.

Wir bemerken noch, daß man nach geeigneter Permutation der Zeilen von Z_2 in (1.4) zu

$$Z_3 = \begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_{q-2} \\ a_1 & a_2 & a_3 & \dots & a_0 \\ a_2 & a_3 & a_4 & \dots & a_1 \\ \dots & \dots & \dots & \dots & \dots \\ a_{q-2} & a_0 & a_1 & \dots & a_{q-3} \end{bmatrix}. \tag{1.5}$$

gelangt, weshalb der Rang r von Z_2 gleich dem von Z_3 ist. Da ferner Z_3 symmetrisch ist, gilt nach einem wohlbekannten Satze

$$r = r_{\text{hm}} \tag{1.6}$$

wobei r_{hm} *den Hauptminorrang* von Z_3, d. h. die größte ganze Zahl k_1 bedeutet, für welche ein nichtverschwindender *Hauptminor* in Z_3 von der Ordnung k_1 existiert. Die Bestimmung von r_{hm} ist im allgemeinen auch viel schwieriger als die von r_{hms}. Ein Vergleich mit dem verallgemeinerten Satz von König-Rados ergibt als Nebenresultat

$$r = r_{\text{hms}}. \tag{1.7}$$

Das ließe sich vielleicht auch direkt beweisen.

2. Nun kehren wir zum kurzen direkten Beweis unseres Satzes. Es sei N die Anzahl der verschiedenen Nullstellen von $f(x)$ in K. Da nach der Annahme $f(0) = a_0 \neq 0$ ist, besagt N, wie oft 0 unter den $q-1$ Elementen

$$f(\gamma), \quad \gamma \in K, \ \gamma \neq 0 \tag{2.1}$$

vorkommt. Wird also der l-te elementar-symmetrische Ausdruck aller Elemente (2.1) durch s_l bezeichnet, d. h. (mit Hilfe einer neuen Unbestimmten z)

$$\prod_{\substack{\gamma \in K \\ \gamma \neq 0}} \left(z + f(\gamma)\right) = \sum_{l=0}^{q-2} s_{q-1-l} z^l + z^{q-1} \tag{2.2}$$

gesetzt, so ist z ein N-facher Faktor dieses Polynoms, d. h.

$$s_{q-1} = s_{q-2} = \dots = s_{q-N} = 0, \quad s_{q-N-1} \neq 0. \tag{2.3}$$

Nun ist aber die linke Seite von (2.2) wegen (1.3) gleich der zyklischen Determinante (siehe [3])

$$\begin{vmatrix} (z+a_0) & a_1 & a_2 & \dots & a_{q-2} \\ a_{q-2} & (z+a_0) & a_1 & \dots & a_{q-3} \\ \dots & \dots & \dots & \dots & \dots \\ a_1 & a_2 & a_3 & \dots & (z+a_0) \end{vmatrix}.$$

Also ist s_l wegen (1.4) gleich der Summe der Hauptminoren l-ter Ordnung der Matrix Z_2. Hiernach besagt (2.3), daß

$$q-N-1 = r_{\text{hms}}$$

ist. Somit ist aber der Satz schon bewiesen.

Zitate

[1] Kronecker, *Vorlesungen über die Zahlentheorie*, Bearbeitet von K. Hensel, Bd. I, Leipzig 1901.

[2] G. Rados, *Zur Theorie der Kongruenzen höheren Grades*, J. für reine und angew. Math. 99 (1886), p. 258-260.

[3] L. Rédei, *Algebra I*, (Ungarisch), Budapest 1954 (Bald erscheint hiervon eine umgearbeitete deutsche Auflage in Leipzig).

[4] Vandiver, *Some theorems in finite field theory with applications to Fermat's last theorem*, Proc. Nat. Acad. USA 30 (1944), p. 362-367.

[5] — *On trinomial congruences and Fermat's last theorem*, Proc. Nat. Acad. USA 30 (1944), p. 367-368.

UNIVERSITÄT SZEGED
UNIVERSITÄT BUDAPEST

Reçu par la Rédaction le 6. 12. 1958