Ein Gleichverteilungssatz für Systeme homogener Linearformen modulo p

Von L. RÉDEI in Szeged und H. J. WEINERT in Potsdam

Professor Ott-Heinrich Keller zum 60. Geburtstag gewidmet

1. Es sei p eine Primzahl und $R=\mathfrak{Z}/(p)$ der Restklassenring des Ringes $\mathfrak{Z}$ der ganzen Zahlen modulo p, für dessen Elemente wir der Kürze halber oft einfach $0, 1, \ldots, p-1$ schreiben. Ein System von r homogenen Linearformen in n Unbestimmten

$$L_\varrho(x_1, x_2, \ldots, x_n) = \sum_{\nu=1}^{n} a_{\varrho,\nu} x_\nu \in R[x_1, x_2, \ldots, x_n] \qquad (\varrho = 1, \ldots, r) \tag{1}$$

nennen wir (modulo p) *gleichverteilt*, wenn $p|r$ gilt und für jedes n-tupel

$$(\xi_1, \xi_2, \ldots, \xi_n) \neq (0, 0, \ldots, 0) \quad \text{aus} \quad R^{[n]} = R \times R \times \ldots \times R \tag{2}$$

die r Werte

$$L_\varrho(\xi_1, \xi_2, \ldots, \xi_n) = \sum_{\nu=1}^{n} a_{\varrho,\nu} \xi_\nu \qquad (\varrho = 1, \ldots, r) \tag{3}$$

gleichverteilt sind, d. h. alle Restklassen modulo p gerade $\frac{r}{p}$-mal ergeben. Weiterhin bezeichnen wir als *volles System* in n Unbestimmten das aus allen $r=p^n$ paarweise voneinander verschiedenen Linearformen bestehende System

$$L_{i_1 i_2 \ldots i_n}(x_1, x_2, \ldots, x_n) = i_1 x_1 + i_2 x_2 + \ldots + i_n x_n, \tag{4}$$

wobei also $(i_1, i_2, \ldots, i_n)$ die Produktmenge $R^{[n]}$ durchläuft.

Es ist klar, daß das volle System (4) gleichverteilt ist. Ausgangspunkt der vorliegenden Note war die Frage, ob umgekehrt ein gleichverteiltes System (1) von $r=p^n$ Linearformen das volle System sein muß. In der Tat gilt sogar der folgende, etwas schärfere

Satz. *Ein System* (1) *von r homogenen Linearformen in n Unbestimmten modulo p ist genau dann gleichverteilt, wenn $p^n|r$ gilt und es aus $s=\frac{r}{p^n}$ vollen Systemen besteht.*

Darüber hinaus zeigen wir, daß dieser Satz weder durch eine (wesentliche) Abschwächung der Gleichverteilung noch durch eine Ausdehnung auf andere Polynome aus $R[x_1, \ldots, x_n]$ verallgemeinert werden kann. Schließlich bemerken wir, daß sich unser Satz offenbar auch in die folgende Aussage überführen läßt:

Zwei Systeme (1) von je r Linearformen modulo p liefern genau dann für jedes n-tupel (2) die gleichen Werte, wenn diese Systeme übereinstimmen.

2. Beweis des Satzes. Wir brauchen nur zu zeigen, daß jedes gleichverteilte System aus einem oder mehreren vollen Systemen besteht. Für $n=1$ ist diese Behauptung trivial; wir zeigen, daß sie für ein System (1) in $n\geqq 2$ Unbestimmten richtig ist, falls sie für Systeme in $n-1$ Unbestimmten zutrifft. Die Einsetzung von $(1, 0, \ldots, 0)$ in (1) lehrt zunähst, daß die Koeffizienten $a_{\varrho,1}$ gleichverteilt sind; ohne Beschränkung der Allgemeinheit können wir daher das System (1) in der Form

$$L_\tau^{(i)}(x_1, x_2, \ldots, x_n) = ix_1 + \sum_{\nu=2}^{n} a_{\tau,\nu}^{(i)} x_\nu \tag{5}$$

schreiben, wobei i die Klassen $0, 1, \ldots, p-1$ und τ jeweils alle Werte $1, \ldots, t$ mit $r=pt$ durchläuft. Wir betrachten nun für jedes feste $(n-1)$-tupel $(\xi_2, \ldots, \xi_n) \neq (0, \ldots, 0)$ die p^2t Werte

$$L_\tau^{(i)}(\xi_1, \xi_2, \ldots, \xi_n) = i\xi_1 + \sum_{\nu=2}^{n} a_{\tau,\nu}^{(i)} \xi_\nu \tag{6}$$

für alle i, alle τ und alle $\xi_1 \in R$, die nach Voraussetzung für jeden Wert von ξ_1, also auch insgesamt gleichverteilt sind. Ist $c \in R$ fest gewählt, so trifft die gleiche Feststellung für die p^2t Werte

$$L_\tau^{(i)}(\xi_1, \xi_2, \ldots, \xi_n) - c\xi_1 = (i-c)\xi_1 + \sum_{\nu=2}^{n} a_{\tau,\nu}^{(i)} = F(i, \tau, \xi_1) \tag{6'}$$

zu. Nun sind aber für jedes τ und jedes $i \neq c$ die p Werte $F(i, \tau, \xi_1)$ mit $\xi_1 = 0, 1, \ldots, \ldots, p-1$ gleichverteilt. Wir streichen sie alle aus (6'), womit auch die aus pt Werten bestehende Restmenge

$$F(c, \tau, \xi_1) = 0\xi_1 + \sum_{\nu=2}^{n} a_{\tau,\nu}^{(c)} \xi_\nu \tag{6''}$$

gleichverteilt ist. Da aber diese Werte von ξ_1 gar nicht mehr abhängen, so folgt, daß für jedes $c \in R$ die t Linearformen in $n-1$ Unbestimmten

$$\sum_{\nu=2}^{n} a_{\tau,\nu}^{(c)} x_\nu \qquad (\tau = 1, \ldots, t)$$

gleichverteilt sind. Nach Induktionsvoraussetzung bestehen sie also jeweils aus $s = \frac{t}{p^{n-1}}$ vollen Systemen in $n-1$ Unbestimmten und damit (5) aus $s = \frac{pt}{p^n} = \frac{r}{p^n}$ vollen Systemen in n Unbestimmten, wie zu beweisen war.

3. Für die weiteren Bemerkungen stellen wir zunächst fest, daß ersichtlich nicht alle $p^n - 1$ n-tupel (2) eingesetzt werden müssen, um nachzuprüfen, ob ein System (1) gleichverteilt ist. Vielmehr kann man sich (auf die verschiedenen Punkte des $n-1$-dimensionalen projektiven Raumes über R d.h.) etwa auf die folgenden

$1+p+\ldots+p^{n-1}=\dfrac{p^n-1}{p-1}$ n-tupel beschränken:

$$\left.\begin{array}{l}(1\ ,0,0,\ldots\ldots\ldots,0,\ 0)\\(\xi_1,1,0,\ldots\ldots\ldots,0,\ 0)\\\ldots\ldots\ldots\ldots\ldots\ldots\ldots\end{array}\right\}\quad a)$$

(7)
$$(\xi_1,\ldots,\xi_k,1,0,\ldots,0)\quad b)$$

$$\left.\begin{array}{l}\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\(\xi_1,\xi_2,\xi_3,\ldots,1\ \ ,0)\\(\xi_1,\xi_2,\xi_3,\ldots,\xi_{n-1},1)\end{array}\right\}\quad c)$$

Dagegen gilt unser Satz nicht mehr, wenn von diesen (oder auf andere Weise normierten) wesentlichen Einsetzungen eine weggelassen wird:

Zusatz. *Für jedes feste n-tupel $\eta=(\eta_1,\ldots,\eta_k,1,0,\ldots,0)$ von* (7) *gibt es stets ein System* (1) *von $r=p^{n-1}$ Linearformen in n Unbestimmten, welches beim Einsetzen von jedem n-tupel* (7) *mit Ausnahme von η gleichverteilte Werte liefert, nämlich etwa*

(8)
$$i_1x_1+\ldots+i_kx_k-(i_1\eta_1+\ldots+i_k\eta_k)x_{k+1}+i_{k+2}x_{k+2}+\ldots+i_nx_n$$

mit allen $(i_1,\ldots,i_k,i_{k+2},\ldots,i_n)\in R^{[n-1]}$.

Beweis. Beim Einsetzen der in (7) unter a) bzw. c) zusammengefaßten n-tupel in (8) erhält man ersichtlich immer gleichverteilte Werte. Im Falle b) ergeben sich aus (8) mehrfach die Werte

$$i_1(\xi_1-\eta_1)+\ldots\ i_k(\xi_k-\eta_k),$$

die genau dann glechverteilt sind, wenn wenigstens für eine Differenz $\xi_\nu-\eta_\nu\neq 0$ gilt.

Aus diesem Zusammenhang folgt sofort, daß kein entsprechender Gleichverteilungssatz für inhomogene Linearformen oder Systeme von Polynomen höheren Grades gilt[1]). Jedem solchen System kann nämlich nach der Anzahl n der auftretenden Koeffizienten ein System (1) von homogenen Linearformen in n Unbestimmten zugeordnet werden, wobei jedoch wenigstens für eine Unbestimmte nicht mehr alle p Werte aus R eingesetzt werden können oder die Einsetzungsmöglichkeiten für verschiedene Unbestimmte nicht mehr unabhängig voneinander sind. Eine einzige (wesentliche) Ausnahme beim Einsetzen macht aber nach unserem Zusatz die Aussage des Gleichverteilungssatzes bereits falsch.

(Eingegangen am 3. Februar 1965)

[1]) Von Umschreibungen wie x^p für x usw., die beim Einsetzen modulo p trivialer Weise den gleichen Wert liefern, hat man dabei natürlich abzusehen.