Kurzer Beweis eines Satzes von Vandiver über endliche Körper.

Von L. RÉDEI in Szeged.

Bezeichne $F(q)$ den endlichen Körper mit q Elementen (q Primzahlpotenz), $m\,(>1)$ einen Teiler von $q-1$ und es werde

$$q=1+mc \tag{1}$$

gesetzt. VANDIVER[1]) bewies kürzlich einen interessanten Satz über die Anzahl der Paare x^m, y^m $(\neq 0)$ mit

$$1+ax^m=by^m \qquad (a,b,x,y\in F(q);\ ab\neq 0).$$

Statt dieser betrachtet er bequemer die Gleichung

$$1+g^{i+rm}=g^{j+sm} \qquad (r,s=0,\ldots,c-1), \tag{2}$$

wobei g ein festgewähltes erzeugendes Element der multiplikativen (zyklischen) Gruppe der Elemente $(\neq 0)$ von $F(q)$ ist, und i,j feste ganze Zahlen sind. Er bezeichnet mit (i,j) die Anzahl der Lösungen r,s von (2), dabei hängt (i,j) nur von den Restklassen i,j mod m an. VANDIVERs Satz lautet so:

Wird

$$A_{hk}=\sum_{i,j=0}^{m-1}(i,j)\,(i+h,\ j+k) \tag{3}$$

gesetzt, so gilt

$$A_{hk}=\begin{cases}(c-1)^2+c\,(m-1) & \text{für } m\mid h,k,\\ c^2 & \text{für } m\nmid h,k,h-k,\\ c^2-c & \text{sonst.}\end{cases} \tag{4}$$

Für eine ganze Zahl i setzen wir $\bar{i}=1$ bzw. $\bar{i}=0$, je nachdem $m\mid i$ oder $m\nmid i$ gilt. Dann schreibt sich VANDIVERs Satz wegen (1) so:

$$A_{hk}=c^2+q\,\bar{h}\bar{k}-c\,(\bar{h}+\bar{k}+\overline{h-k}). \tag{4'}$$

VANDIVER stellt in seiner Arbeit auch Anwendungen für die obere und untere Grenze der Lösungsanzahl der Gleichung in $F(q)$

$$c_1x_1^{a_1}+\ldots+c_sx^{a_s}+c_{s+1}=0$$

in Aussicht, und das erhöht die Wichtigkeit von (4).

---

[1]) H. S. VANDIVER: Limits for the number of solutions of certain general types of equations in a finite field. *Proc. Nat. Acad. Sci. USA* **33** (1947), 236–242.

Im folgenden verkürzen wir den Beweis von (4). Mit VANDIVER setzen wir

$$C_{uv}=\sum_{h,k=0}^{m-1} A_{hk}\,\alpha^{-uh+vk}, \tag{5}$$

wobei α eine feste primitive m-te (komplexe) Einheitswurzel bezeichnet. Die Formeln (6), (9), (10), (11), (13) in der Arbeit von VANDIVER lassen sich so schreiben:

$$C_{uv}=q+(q-1)^2\,\bar{u}\,\bar{v}-(q-1)\,(\bar{u}+\bar{v}+\overline{u-v}). \tag{6}$$

Hiervon stimmt nämlich der fall $\bar{u}=\bar{v}=\overline{u-v}=0$ mit der Formel

$$\psi_{uv}(\alpha)\,\psi_{uv}(\alpha^{-1})=q \qquad \left(\psi_{uv}(\alpha)=\sum_{i,j=0}^{m-1}(i,j)\,\alpha^{-ui+vj}\right)$$

von MITCHELL[2]) überein (vgl. (4b) in der Arbeit von VANDIVER), die übrigen Fälle sind Trivialitäten.

Von (6) zu (4′) kommt man einfach so. Wegen (5) gilt

$$\sum_{u,v=0}^{m-1} C_{uv}\alpha^{ur-vs}=\sum_{h,k=0}^{m-1}\left(A_{hk}\left(\sum_{u=0}^{m-1}\alpha^{u(r-h)}\right)\left(\sum_{v=0}^{m-1}\alpha^{v(k-s)}\right)\right)=m^2 A_{rs},$$

und so folgt aus (6)

$$m^2 A_{rs}=\sum_{u,v=0}^{m-1}(q+(q-1)^2\bar{u}\,\bar{v}-(q-1)\,(\bar{u}+\bar{v}+\overline{u-v}))\,\alpha^{ur-vs} \tag{7}$$

Es gilt nun mit der Abkürzung $\omega=\alpha^{ur-vs}$, $\sum=\sum_{u,v=0}^{m-1}$:

$$\Sigma\,\omega=m^2\bar{r}\,\bar{s},\quad \Sigma\,\bar{u}\,\bar{v}\,\omega=1,\quad \Sigma\,\bar{u}\,\omega=m\bar{s},\quad \Sigma\,\bar{v}\,\omega=m\bar{v},$$

$$\sum\overline{u-v}\,\omega=\sum_{v=0}^{m-1}\alpha^{vr-vs}=m\overline{r-s},$$

und so folgt aus (7):

$$m^2 A_{rs}=q\,m^2\,\bar{r}\,\bar{s}+(q-1)^2-(q-1)\,m\,(\bar{s}+\bar{r}+\overline{r-s})$$

Wegen (1) stimmt dies mit (4′) überein, womit wir VANDIVERS Satz bewiesen haben.

(Eingegangen am 15. Oktober 1949.)

---

[2]) H. H. MITCHELL: Generalised Jacobi-Kummer cyclotomic Function. *Trans. Amer Math. Soc.*, **17** (1916), 165—177, insb. S. 167, (5).