ACTA ARITHMETICA
XLV (1985)

Über die Fixpunkte von durch Dicksonpolynome dargestellten Permutationen

von

RUPERT NÖBAUER (Klagenfurt)

1. Einleitung. Ein Polynom $f(x)$ über einem kommutativen Ring R mit Einselement heißt *Permutationspolynom* von R, wenn die Abbildung Π: $a \to f(a)$ von R in sich eine Permutation ist (vgl. [3]). Man sagt dann, daß die Abbildung Π durch f dargestellt wird und nennt Π Polynompermutation. Gewissen Klassen von Polynompermutationen kommt insofern auch praktische Bedeutung zu, als sie zur Konstruktion von Public-Key Cryptosystemen (vgl. [1]) herangezogen werden können: So liegen dem RSA-Schema (vgl. [9]) Potenzpermutationen $x \to x^k$ des Restklassenringes Z_m, m quadratfreie natürliche Zahl (in der Praxis: $m = p \cdot q$; p, q zwei große Primzahlen), zugrunde, und W. B. Müller und W. Nöbauer [5] schlagen ein Public-Key System vor, das auf durch Dicksonpolynome $g_k(a, x)$, $a = \pm 1$, dargestellten Permutationen von Z_m beruht. Dabei ist das Dicksonpolynom $g_k(a, x)$ mit beliebigem, ganzzahligen a gegeben durch

$$g_k(a, x) = \sum_{t=0}^{[k/2]} \frac{k}{k-t} \cdot \binom{k-t}{t} \cdot (-a)^t \cdot x^{k-2t}$$

(vgl. [2], [4]).

Ist $m = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ die Faktorisierung von m in Primzahlpotenzen, bezeichnet φ die Eulersche φ-Funktion, und setzt man $v := \varphi(m)(p_1+1) \times \times (p_2+1) \dots (p_r+1)$, so ist $g_k(a, x)$, $a = \pm 1$, genau dann Permutationspolynom von Z_m, wenn gilt $(k, v) = 1$ (vgl. [7]).

Beim Verschlüsseln mit Hilfe einer Polynompermutation wirken Fixpunkte dieser Permutation als störend, und es erscheint daher von Interesse, die Fixpunkte von zur Chiffrierung in Frage kommenden Polynompermutationen zu studieren. Für Potenzpermutationen von Z_m wurde eine derartige Untersuchung bereits von W. B. Müller und W. Nöbauer [6] durchgeführt, und in der vorliegenden Arbeit sollen nun die Fixpunkte von durch Dicksonpolynome $g_k(a, x)$, $a = \pm 1$, dargestellten Permutationen untersucht werden, wobei wesentlich von zahlentheoretischen Methoden Gebrauch gemacht wird.

2. Sei Q ein Galoisfeld der Ordnung q, $a\in Q$, $a\neq 0$ und k eine natürliche Zahl. In $Q(z)$, dem rationalen Funktionenkörper über Q, gilt die im Verlauf der Arbeit öfter benötigte Formel

$$g_k\left(a,\ z+\frac{a}{z}\right)=z^k+\left(\frac{a}{z}\right)^k \tag{1}$$

(vgl. [8]). Es ist $g_k(a, x)$ genau dann Permutationspolynom von Q, wenn gilt: $(k, q^2-1)=1$ (vgl. [8]). Schließlich sei noch die folgende, ebenfalls in [8] gezeigte Aussage vermerkt: Die Menge $\mathcal{M}(a)$ aller Lösungen der q Gleichungen

$$z+\frac{a}{z}=\varrho,\qquad \varrho\in Q, \tag{2}$$

also der q quadratischen Gleichungen $z^2-\varrho z+a=0$ in E, dem Galoisfeld der Ordnung q^2 (jede dieser Gleichungen ist in E tatsächlich lösbar), ist gegeben durch $\mathcal{M}(a)=\mathcal{M}_1(a)\cup\mathcal{M}_2(a)$, wobei

$$\begin{aligned}\mathcal{M}_1(a)&=\{u\in E|\ u^{q+1}=a\},\\ \mathcal{M}_2(a)&=\{u\in E|\ u^{q-1}=1\}.\end{aligned} \tag{3}$$

Ist R ein kommutativer Ring mit Einselement, dann werde im folgenden die Anzahl der Fixpunkte der durch $g_k(a, x)$ auf R dargestellten Abbildung mit $f(R, k, a)$ bezeichnet. Wir zeigen nun

SATZ 1. *Sei Q ein Galoisfeld der Ordnung q, und sei k eine natürliche Zahl. Sei ε_1 definiert durch*

$$\varepsilon_1=\begin{cases}1 & \text{falls char } Q=2 \text{ oder}\\ & \text{char } Q\neq 2 \text{ und } k \text{ gerade},\\ 2 & \text{falls char } Q\neq 2 \text{ und } k \text{ ungerade}.\end{cases}$$

Dann gilt:

$$f(Q, k, 1)=\tfrac{1}{2}[(k+1, q+1)+(k+1, q-1)+(k-1, q+1)+(k-1, q-1)]-\varepsilon_1.$$

Beweis. Ist w Primitivwurzel von E, so gilt

$$\begin{aligned}\mathcal{M}_1(1)&=\{w^{(q-1)r}|\ r=0, 1, \ldots, q\},\\ \mathcal{M}_2(1)&=\{w^{(q+1)s}|\ s=0, 1, \ldots, q-2\}.\end{aligned} \tag{4}$$

Für $u\in\mathcal{M}_1(1)\cap\mathcal{M}_2(1)$ haben wir $u^{q+1}=u^{q-1}=1$, also $u^2=1$ und somit $u=\pm 1$. Umgekehrt gilt für $u=\pm 1$ $u\in\mathcal{M}_1(1)\cap\mathcal{M}_2(1)$, und zwar im Fall char $Q=2$ wegen $-1=+1$. Setzt man $\mathcal{N}_3(1)=\{1\}$ im Fall char $Q=2$, $\mathcal{N}_3(1)=\{-1, +1\}$ im Fall char $Q\neq 2$, weiters $\mathcal{N}_1(1)=\mathcal{M}_1(1)\setminus\mathcal{N}_3(1)$ und $\mathcal{N}_2(1)=\mathcal{M}_2(1)\setminus\mathcal{N}_3(1)$, dann läßt sich $\mathcal{M}(1)$ folgendermaßen als Vereinigung disjunkter Mengen darstellen:

$$\mathcal{M}(1)=\mathcal{N}_1(1)\cup\mathcal{N}_2(1)\cup\mathcal{N}_3(1).$$

Für jede Gleichung $z+1/z=\varrho$ ist mit u auch $1/u$ Lösung, und die Werte u und $1/u$ fallen genau für $u^2=1$, also für $u\in\mathcal{N}_3(1)$ zusammen.

Es ist $\varrho\in Q$ genau dann Fixpunkt von $g_k(1, x)$, wenn gilt $g_k(1, \varrho)=\varrho$, also mit $\varrho=u+1/u$ nach (1) genau dann, wenn gilt $u^k+1/u^k=u+1/u$. Dies ist äquivalent zu $u^{2k}-u^{k+1}-u^{k-1}+1=0$, also zu

$$(u^{k+1}-1)(u^{k-1}-1)=0. \tag{5}$$

Wir haben alle Lösungen von (5) über $\mathcal{M}(1)$ zu bestimmen, also alle Lösungen jeder der beiden Gleichungen $u^{k+1}=1$ und $u^{k-1}=1$ über jeder der drei Mengen $\mathcal{N}_1(1)$, $\mathcal{N}_2(1)$ und $\mathcal{N}_3(1)$. Da eine Lösung v von (5) genau dann Lösung beider Gleichungen $u^{k+1}=1$ und $u^{k-1}=1$ ist, wenn gilt $v^2=1$, also wenn $v\in\mathcal{N}_3(1)$, ist die Anzahl der Lösungen von Gleichung (5) über $\mathcal{M}(1)$ gleich der Summe der Anzahlen der Lösungen jeder der beiden Gleichungen $u^{k+1}=1$ und $u^{k-1}=1$ über jeder der beiden Mengen $\mathcal{N}_1(1)$ und $\mathcal{N}_2(1)$ plus der Anzahl der Lösungen von (5) über $\mathcal{N}_3(1)$. Es ist $v\in\mathcal{M}_1(1)$ genau dann Lösung von $u^{k+1}=1$, wenn gilt $w^{(q-1)r(k+1)}=1$, also wenn $(q-1)r(k+1)\equiv 0 \bmod (q+1)(q-1)$, d.h. wenn $r(k+1)\equiv 0 \bmod (q+1)$. Diese Kongruenz hat $(k+1, q+1)$ inkongruente Lösungen, und daher hat $u^{k+1}=1$ genau $(k+1, q+1)$ Lösungen über $\mathcal{M}_1(1)$. Ebenso zeigt man: $u^{k+1}=1$ hat genau $(k+1, q-1)$ Lösungen über $\mathcal{M}_2(1)$, $u^{k-1}=1$ hat genau $(k-1, q+1)$ Lösungen über $\mathcal{M}_1(1)$ und $u^{k-1}=1$ hat genau $(k-1, q-1)$ Lösungen über $\mathcal{M}_2(1)$. (5) hat über $\mathcal{N}_3(1)$ in den Fällen char $K=2$ sowie char $K\neq 2$ und k gerade genau eine Lösung, im Fall char $K\neq 2$ und k ungerade genau zwei Lösungen, also stets genau ε_1 Lösungen. Beachtet man, daß mit u jeweils auch $1/u$ Lösung von $u^{k+1}=1$ bzw. $u^{k-1}=1$ ist, so erhält man unter Berücksichtigung des über die Lösungen von $u+1/u=\varrho$ Gesagten

$$f(Q, k, 1)=\tfrac{1}{2}[(k+1, q+1)+(k+1, q-1)+(k-1, q+1)+(k-1, q-1)]-\varepsilon_1,$$

und dies ergibt gerade die Behauptung.

Bemerkung. Satz 1 enthält keinerlei Einschränkungen über k und beinhaltet daher für beliebige von Polynomen der Gestalt $g_k(1, x)$ dargestellte Abbildungen eine Aussage über die Fixpunkteanzahl und nicht nur für Permutationen.

Es soll nun die Anzahl der Fixpunkte der durch $g_k(-1, x)$, k ungerade, dargestellten Abbildungen von Q bestimmt werden. Da im Fall char $Q=2$ gilt: $g_k(-1, x)=g_k(1, x)$, können wir uns dabei auf Körper ungerader Charakteristik beschränken. Im folgenden sei $v_p(m)$ für $m\in Z\setminus\{0\}$ die Vielfachheit, mit der p in der Faktorzerlegung von m auftritt, und $v_p(0)=\infty$. Klarerweise gelten die Rechenregeln $v_p((a, b))=\min\{v_p(a), v_p(b)\}$, $v_p(a\cdot b)=v_p(a)+v_p(b)$ und $a|b\Rightarrow v_p(b/a)=v_p(b)-v_p(a)$, und zwar mit den Festsetzungen $c<\infty$ und $\infty+c=\infty-c=\infty$ sogar für beliebige ganze Zahlen a und b. Wir zeigen nun folgenden

SATZ 2. *Sei Q ein Galoisfeld ungerader Ordnung q, und sei k eine ungerade natürliche Zahl. Sei*

$$\varepsilon_{-1} = \begin{cases} 2 & \text{für } k \equiv 1 \bmod 4 \text{ und } q \equiv 1 \bmod 4, \\ 0 & \text{sonst.} \end{cases}$$

Dann gilt

$$f(Q, k, -1) = \tfrac{1}{2}\big[a_1 \cdot (k+1, 2(q+1)) + a_2 \cdot (k+1, q-1) + a_3 \cdot ((k-1)/2, q+1) + 1 \cdot (k-1, q-1)\big] - \varepsilon_{-1},$$

wobei

$$a_1 = \begin{cases} 1 & \text{für } v_2(k+1) = v_2(q+1), \\ 0 & \text{sonst,} \end{cases}$$

$$a_2 = \begin{cases} 1 & \text{für } v_2(k+1) < v_2(q-1), \\ 0 & \text{sonst,} \end{cases}$$

$$a_3 = \begin{cases} 1 & \text{für } v_2(k-1) > v_2(q+1), \\ 0 & \text{sonst.} \end{cases}$$

Beweis. Es gilt

$$\mathscr{M}_1(-1) = \{w^{((q-1)/2)\cdot r} \mid r = 1, 3, \ldots, 2q+1\},$$
$$\mathscr{M}_2(-1) = \{w^{(q+1)\cdot s} \mid s = 0, 1, \ldots, q-2\}. \tag{6}$$

Für das folgende setzen wir $u_i = w^{((q^2-1)/4)(1+2i)}$, $i = 0, 1$. Für $u \in \mathscr{M}_1(-1) \cap \mathscr{M}_2(-1)$ gilt $u^{q+1} = -1$ und $u^{q-1} = 1$, also $u^2 = -1$ und somit $u \in \{u_0, u_1\}$. Für die Betrachtung der umgekehrten Inklusion haben wir die beiden Fälle $q \equiv 1 \bmod 4$ und $q \equiv 3 \bmod 4$ zu unterscheiden. Im Fall $q = 4t+1$, t natürliche Zahl, gelten für $i = 0, 1$ die Beziehungen

$$u_i^{q+1} = w^{\frac{q^2-1}{4}(1+2i)(4t+2)} = w^{\frac{q^2-1}{2}} = -1$$

und

$$u_i^{q-1} = w^{\frac{q^2-1}{4}(1+2i)4t} = 1,$$

sodaß folgt $u_i \in \mathscr{M}_1(-1) \cap \mathscr{M}_2(-1)$, $i = 0, 1$. Im Fall $q = 4t+3$, t nichtnegative ganze Zahl, gelten für $i = 0, 1$ die Beziehungen

$$u_i^{q+1} = w^{\frac{q^2-1}{4}(1+2i)(4t+4)} = 1$$

und

$$u_i^{q-1} = w^{\frac{q^2-1}{4}(1+2i)(4t+2)} = -1,$$

sodaß folgt $u_i \notin \mathscr{M}_j(-1)$, $i = 0, 1$; $j = 1, 2$; also erst recht $u_i \notin \mathscr{M}_1(-1) \cap \mathscr{M}_2(-1)$. Setzt man $\mathscr{N}_3(-1) = \{u_0, u_1\}$ im Fall $q \equiv 1 \bmod 4$, $\mathscr{N}_3(-1) = \{\,\}$ im Fall $q \equiv 3 \bmod 4$, und setzt man weiters $\mathscr{N}_j(-1) = \mathscr{M}_j(-1) \setminus \mathscr{N}_3(-1)$, $j = 1, 2$ so erhält man folgende Darstellung von $\mathscr{M}(-1)$ als Vereinigung disjunkter Mengen:

$$\mathscr{M}(-1) = \mathscr{N}_1(-1) \cup \mathscr{N}_2(-1) \cup \mathscr{N}_3(-1).$$

Für jede Gleichung $z - 1/z = \varrho$, $\varrho \in Q$, ist mit u auch $-1/u$ Lösung, und die Werte u und $-1/u$ fallen genau für $u^2 = -1$, also für $u \in \mathscr{N}_3(-1)$ zusammen.

Es ist $\varrho \in Q$ genau dann Fixpunkt von $g_k(-1, x)$, wenn gilt $g_k(-1, \varrho) = \varrho$, also mit $\varrho = u - 1/u$ genau dann, wenn gilt $u^k - 1/u^k = u - 1/u$. Dies ist äquivalent zu $u^{2k} - u^{k+1} + u^{k-1} - 1 = 0$, d.h. zu

$$(u^{k+1}+1)(u^{k-1}-1) = 0. \tag{7}$$

Wir haben alle Lösungen von (7) über $\mathscr{M}(-1)$ zu bestimmen, also alle Lösungen jeder der beiden Gleichungen $u^{k+1} = -1$ und $u^{k-1} = 1$ über jeder der drei Mengen $\mathscr{N}_1(-1)$, $\mathscr{N}_2(-1)$ und $\mathscr{N}_3(-1)$. Da eine Lösung v von (7) genau dann Lösung beider Gleichungen $u^{k+1} = -1$ und $u^{k-1} = 1$ ist, wenn gilt $v^2 = -1$, also wenn $v \in \mathscr{N}_3(-1)$, ist die Anzahl der Lösungen der Gleichung (7) über $\mathscr{M}(-1)$ gleich der Summe der Anzahlen der Lösungen jeder der beiden Gleichungen $u^{k+1} = -1$ und $u^{k-1} = 1$ über jeder der beiden Mengen $\mathscr{N}_1(-1)$ und $\mathscr{N}_2(-1)$ plus der Anzahl der Lösungen von (7) über $\mathscr{N}_3(-1)$.

Es ist $v \in \mathscr{M}_1(-1)$ genau dann Lösung von $u^{k+1} = -1$, wenn gilt $w^{\frac{q-1}{2}r(k+1)} = -1$, also wenn

$$\frac{q-1}{2} r(k+1) \equiv \frac{(q-1)}{2}(q+1) \bmod (q-1)(q+1),$$

d.h. wenn

$$r(k+1) \equiv q+1 \bmod 2(q+1). \tag{8}$$

Diese Kongruenz ist genau dann lösbar, wenn gilt $(k+1, 2(q+1)) \mid (q+1)$, also wenn $v_2(k+1) \leqslant v_2(q+1)$. Es sei im folgenden $v_2(k+1) \leqslant v_2(q+1)$, wir haben die Anzahl der ungeraden Lösungen r von (8) zu bestimmen. Setzt man $d = (k+1, 2(q+1))$, so gilt $v_2(d) = \min\{v_2(k+1), v_2(q+1)+1\} = v_2(k+1)$. Sind α, β ganze Zahlen mit

$$\alpha \cdot (k+1) + \beta \cdot 2(q+1) = d, \tag{9}$$

so sind sämtliche Lösungen von (8) gegeben durch

$$\alpha \cdot \frac{q+1}{d} + \frac{2(q+1)}{d} i, \quad i = 0, \ldots, d-1.$$

Die Zahl α ist ungerade, denn wäre α gerade, so würde aus (9) durch Herausheben der größtmöglichen Zweierpotenz auf beiden Seiten die Be-

ziehung

$$v_2(d) \geqslant \min\{v_2(k+1)+1,\ v_2(q+1)+1\} > v_2(k+1)$$

folgen, und dies ergäbe einen Widerspruch. Wegen

$$v_2((q+1)/d) = v_2(q+1) - v_2(d) = v_2(q+1) - v_2(k+1)$$

ist $(q+1)/d$ genau dann ungerade, wenn gilt $v_2(q+1) = v_2(k+1)$. Die Zahl $2(q+1)/d$ ist wegen $d|(q+1)$ stets gerade. Insgesamt erhalten wir somit: Die Kongruenz (8) ist genau dann mit ungeradem r lösbar, wenn gilt $v_2(k+1) = v_2(q+1)$, und wenn dies erfüllt ist, dann hat sie genau $(k+1, 2(q+1))$ Lösungen, die alle ungerade sind.

Es ist $v \in \mathcal{M}_2(-1)$ genau dann Lösung von $u^{k+1} = -1$, wenn gilt $w^{(q+1)s(k+1)} = -1$, also wenn

$$(q+1)s(k+1) \equiv \frac{(q+1)(q-1)}{2} \bmod (q+1)(q-1),$$

d.h. wenn

$$s(k+1) \equiv \frac{q-1}{2} \bmod (q-1).$$

Diese Kongruenz ist genau dann lösbar, wenn gilt $2(k+1, q-1)|(q-1)$, d.h. wenn $v_2(k+1) < v_2(q-1)$, und im Fall der Lösbarkeit hat sie genau $(k+1, q-1)$ Lösungen.

Es ist $v \in \mathcal{M}_1(-1)$ genau dann Lösung von $u^{k-1} = 1$, wenn gilt $w^{\frac{q-1}{2}r(k-1)} = 1$, also wenn $\frac{q-1}{2}r(k-1) \equiv 0 \bmod (q-1)(q+1)$, d.h. wenn

$$r(k-1) \equiv 0 \bmod 2(q+1). \tag{10}$$

Die Kongruenz (10) ist in ungeraden r zu lösen. Setzt man $d = (k-1, 2(q+1))$, so sind sämtliche Lösungen von (10) gegeben durch $\frac{2(q+1)}{d}i$, $i = 0, 1, \ldots, d-1$. $2(q+1)/d$ ist genau dann ungerade, wenn $1 + v_2(q+1) - v_2(d) = 0$, also wenn $v_2(q+1)+1 = v_2(d)$, d.h. wenn $v_2(q+1)+1 = \min\{v_2(k-1), v_2(q+1)+1\}$. Letzteres ist äquivalent zu $v_2(k-1) \geqslant v_2(q+1)+1$, also zu $v_2(k-1) > v_2(q+1)$. Insgesamt erhält man somit: Die Kongruenz (10) ist genau im Fall $v_2(k-1) > v_2(q+1)$ lösbar, und wenn sie lösbar ist, hat sie genau $((k-1)/2, q+1)$ ungerade Lösungen.

Weiters zeigt man genauso wie im Beweis von Satz 1, daß $u^{k-1} = 1$ über $\mathcal{M}_2(-1)$ stets genau $(k-1, q-1)$ Lösungen hat. Schließlich ist die Menge aller Lösungen von (7) über $\mathcal{N}_3(-1)$ zu bestimmen, die gleich ist der Menge aller Lösungen von $u^{k-1} = 1$ über $\mathcal{N}_3(-1)$. Im Fall $q \equiv 3 \bmod 4$ ist diese Menge klarerweise leer, und im Fall $q \equiv 1 \bmod 4$ ist sie bei $k \equiv 3 \bmod 4$ leer

und bei $k \equiv 1 \bmod 4$ gleich $\{u_0, u_1\}$. Somit beträgt die Anzahl der Lösungen von (10) über $\mathcal{N}_3(-1)$ in jedem Fall ε_{-1}.

Beachtet man, daß mit u jeweils auch $-1/u$ Lösung der Gleichung $u^{k+1} = -1$ bzw. $u^{k-1} = 1$ ist, so erhält man unter Berücksichtigung des über die Lösungen von $u - 1/u = \varrho$ Gesagten

$$f(Q, k, -1) = \frac{1}{2}[a_1 \cdot (k+1, 2(q+1)) - \varepsilon_{-1} + a_2 \cdot (k+1, q-1) - \varepsilon_{-1} + a_3 \cdot ((k-1)/2, q+1) - \varepsilon_{-1} + 1 \cdot (k-1, q-1) - \varepsilon_{-1}] + \varepsilon_{-1},$$

und dies ergibt die Behauptung.

Bemerkung. In Ergänzung zu den Sätzen 1 und 2 sei folgende, unter Beachtung von $g_k(0, x) = x^k$ direkt zu verifizierende Aussage vermerkt: Ist Q ein Galoisfeld der Ordnung q, und ist k eine beliebige, natürliche Zahl, dann gilt: $f(Q, k, 0) = (k-1, q-1)+1$.

Die Menge $\mathcal{P}(a)$ aller Permutationspolynome $g_k(a, x)$ eines gegebenen Galoisfelds Q ist genau dann abgeschlossen bezüglich Komposition, wenn gilt $a = 1$, $a = -1$ oder $a = 0$ (vgl. [8]), in diesen Fällen bildet die Menge $\mathcal{G}(a)$ der durch die Polynome von $\mathcal{P}(a)$ dargestellten Permutationen jeweils eine Gruppe. Aufgrund der in diesem Abschnitt dargestellten Ergebnisse ist nun die Anzahl der Fixpunkte sämtlicher Elemente jeder dieser drei Gruppen $\mathcal{G}(-1)$, $\mathcal{G}(0)$ und $\mathcal{G}(1)$ bekannt.

3. Es sollen nun durch $g_k(a, x)$ dargestellte Abbildungen von Z_{p^e}, p Primzahl, $e > 1$, betrachtet werden, wobei wir uns auf bestimmte k beschränken wollen. Wir beweisen

Satz 3. *Sei p eine Primzahl, sei $a = \pm 1$ und sei k ungerade mit $k^2 \not\equiv 1 \bmod p$. Sei überdies im Fall $a = -1$ und $k \equiv 3 \bmod 4$ $k^2 \not\equiv -1 \bmod p$. Dann gilt für jede natürliche Zahl e*

$$f(Z_{p^e}, k, a) = f(Z_p, k, a).$$

Beweis. Nehmen wir an, die Aussage sei für alle $e' < e$, also insbesondere für $e-1$, schon gezeigt. Sei a eine beliebige ganze Zahl, und sei $\varrho \in Z_{p^e}$ Lösung von $g_k(a, x) \equiv x \bmod p^e$, dann ist ϱ klarerweise auch Lösung von $g_k(a, x) \equiv x \bmod p^{e-1}$. Sind $\sigma_1, \ldots, \sigma_n$ sämtliche Lösungen von $g_k(a, x) \equiv x \bmod p^{e-1}$, dann gibt es ein $\sigma \in \{\sigma_1, \ldots, \sigma_n\}$ mit $\varrho \equiv \sigma \bmod p^{e-1}$, d.h. mit $\varrho = \sigma + r \cdot p^{e-1}$. Man findet also alle Lösungen von $g_k(a, x) \equiv x \bmod p^e$, indem man zu jedem $\sigma \in \{\sigma_1, \ldots, \sigma_n\}$ alle r bestimmt mit

$$g_k(a, \sigma + r \cdot p^{e-1}) \equiv \sigma + r \cdot p^{e-1} \bmod p^e. \tag{11}$$

Aufgrund der Taylorformel ist (11) äquivalent mit

$$g_k(a, \sigma) + r \cdot p^{e-1} \cdot g_k'(a, \sigma) \equiv \sigma + r \cdot p^{e-1} \bmod p^e,$$

also mit

$$\frac{g_k(a,\sigma)-\sigma}{p^{e-1}} \equiv r\cdot(1-g_k'(a,\sigma)) \bmod p. \tag{12}$$

Sei $a \neq 0$. Im rationalen Funktionenkörper über Z_p erhält man durch Differenzieren von (1)

$$g_k'\left(a, z+\frac{a}{z}\right)\cdot\left(1-\frac{a}{z^2}\right) = k\cdot z^{k-1} - k\cdot\frac{a^k}{z^{k+1}},$$

also

$$g_k'\left(a, z+\frac{a}{z}\right) = k\cdot\frac{(z^2)^k-a^k}{z^{k-1}(z^2-a)} = \frac{k}{z^{k-1}}\cdot a^{k-1}\cdot\sum_{j=0}^{k-1}\left(\frac{z^2}{a}\right)^j. \tag{13}$$

Sei nun $a = \pm 1$. Ist σ Fixpunkt von $g_k(1, x)$ mod p, dann gilt für das zugehörige u mit $\sigma = u + a/u$, daß $u^{k+1} = a$ oder $u^{k-1} = 1$. Wir unterscheiden drei Fälle:

(i) $u^{k+1} = a$; $u^2 \neq a$. Wegen (13), 1. Gleichung, gilt (unter Verwendung von $a^k = a$)

$$g_k'(a,\sigma) = g_k'\left(a, u+\frac{a}{u}\right) = \frac{k\cdot(1/u^2-a)}{(a/u^2)\cdot(u^2-a)} = k\cdot\frac{1-u^2a}{au^2-1} = -k.$$

(ii) $u^{k-1} = 1$; $u^2 \neq a$. Ähnlich wie in (i) findet man $g_k'(a,\sigma) = k$.

(iii) $u^2 = a$. Wegen (13), 2. Gleichung, gilt

$$g_k'(a,\sigma) = \frac{k}{a^{(k-1)/2}}\cdot a^{k-1}\cdot k = \begin{cases} k^2 & \text{falls } a = 1 \text{ oder} \\ & a = -1 \text{ und } k \equiv 1 \bmod 4, \\ -k^2 & \text{falls } a = -1 \text{ und } k \equiv 3 \bmod 4. \end{cases}$$

Erfüllt k die im Satz angegebenen Bedingungen, dann gilt also für alle σ mit $g_k(a,\sigma) \equiv \sigma \bmod p^{e-1}$ die Beziehung $g_k'(a,\sigma) \not\equiv 1 \bmod p$, und (12) hat genau eine Lösung r. Damit gilt die Behauptung auch für e, womit der Satz bewiesen ist.

Aufgrund des Chinesischen Restsatzes gilt für jedes ganze a und für teilerfremde natürliche Zahlen m_1, m_2 die Beziehung

$$f(Z_{m_1m_2}, k, a) = f(Z_{m_1}, k, a)f(Z_{m_2}, k, a).$$

Da Z_p für Primzahlen p gleich dem Galoisfeld der Ordnung p ist, ist somit aufgrund der in dieser Arbeit gewonnenen Ergebnisse die Anzahl der Fixpunkte von durch $g_k(a, x)$, $a = \pm 1$, auf Z_m dargestellten Permutationen bei quadratfreiem m für beliebige k bekannt. Bei nicht quadratfreiem m mit der Primfaktorzerlegung $m = p_1^{e_1}\dots p_n^{e_n}$ ist die Fixpunkteanzahl im Fall $a = 1$ für

k mit $k \not\equiv \pm 1 \bmod p_i$, $i = 1, \dots, n$, bekannt, und im Fall $a = -1$ für k mit $k \equiv 1 \bmod 4$ und $k \not\equiv \pm 1 \bmod p_i$, $i = 1, \dots, n$, sowie weiters für k mit $k \equiv 3 \bmod 4$ und $k^2 \not\equiv \pm 1 \bmod p_i$, $i = 1, \dots, n$.

Literaturverzeichnis

[1] W. Diffie und M. Hellman, *New directions in cryptography*, IEEE Trans. Information Theory IT-22 (1976), S. 644–654.

[2] H. Lausch, W. B. Müller und W. Nöbauer, *Über die Struktur einer durch Dicksonpolynome dargestellten Permutationsgruppe des Restklassenringes modulo n*, J. Reine Angew. Math. 261 (1973), S. 88–99.

[3] H. Lausch und W. Nöbauer, *Algebra of polynomials*, Amsterdam 1973.

[4] W. B. Müller, *Über eine Klasse von durch Dickson-Polynome dargestellten Gruppen*, Coll. Math. Soc. János Bolyai 6 (1971), S. 361–376.

[5] W. B. Müller und W. Nöbauer, *Some remarks on public-key cryptosystems*, Studia Sci. Math. Hungar. 16 (1981), S. 71–76.

[6] –, – *Über die Fixpunkte der Potenzpermutationen*, Österr. Akad. Wiss. Math. Naturwiss. Kl. Sitzungsber. II (1983), S. 93–97.

[7] W. Nöbauer, *Über Permutationspolynome und Permutationsfunktionen für Primzahlpotenzen*, Monatsh. Math. 69 (1965), S. 230–238.

[8] – *Über eine Klasse von Permutationspolynomen und die dadurch dargestellten Gruppen*, J. Reine Angew. Math. 231 (1968), S. 215–219.

[9] R. L. Rivest, A. Shamir und L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM 21 (1978), S. 120–126.

UNIVERSITÄT FÜR BILDUNGSWISSENSCHAFTEN
INSTITUT FÜR MATHEMATIK
Universitätsstraße 65–67
A-9010 Klagenfurt

Eingegangen am 28.2.1984 (1406)