THEOREM 5. *$E_{\mathfrak{p}}(\omega, S)$ holds if and only if $|\omega|_{\mathfrak{q}} \geqslant 1$ for all $\mathfrak{q} \neq \mathfrak{p}$.*

Proof. As Theorems 1 and 3.
We define

$$\varphi(\mathfrak{q}) = \begin{cases} 1 & \text{if } \mathfrak{q} \neq \mathfrak{p}, \\ N_{\mathfrak{p}} & \text{if } \mathfrak{q} = \mathfrak{p}. \end{cases}$$

When $E_{\mathfrak{p}}(\omega, S)$ holds, by Theorem 5, ω^{-1} belongs to $V(\varphi) \cap k$ which is a vector space with finite dimension over F. Let $\dim \mathfrak{p}$ be the dimension of $V(\varphi) \cap k$. As

$$F = \{(x_{\mathfrak{a}}) \in R(k) \mid |x_{\mathfrak{a}}|_{\mathfrak{a}} = 1 \text{ for all } \mathfrak{a}\} \cap k,$$

we have

COROLLARY 1 TO THEOREM 5. *There exists a prime element ω satisfying $|\omega|_{\mathfrak{q}} \geqslant 1$ for all $\mathfrak{q} \neq \mathfrak{p}$ if and only if $\dim \mathfrak{p} \geqslant 2$.*

Furthermore, we can see easily a following corollary.

COROLLARY 2 TO THEOREM 5. *Let $E_{\mathfrak{p}}(\omega, S)$ holds. Then the period of each $\alpha \in \mathfrak{O}$ is bounded.*

References

[1] E. Artin and G. Whaples, *Axiomatic characterization of fields by the product formula for valuations*, Bull. Amer. Math. Soc. 164 (1931), 1–11.
[2] H. Hasse, *Zahlentheorie*, Berlin 1963.
[3] S. Iyanaga (ed.), *Theory of numbers*, North-Holland, 1975.
[4] S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, MA, 1970.

22-4 Mikagahara, Asahi-ku
Yokohama, 241 Japan

Received on 17. 6. 1986 (1651)

ACTA ARITHMETICA
LI (1988)

Über ganzzahlige Vertauschbarkeitsketten ungeraden Grades*

von

WINFRIED B. MÜLLER und RUPERT NÖBAUER (Klagenfurt)

1. Einleitung. Motiviert durch Anwendungen in der Kryptologie haben sich in den letzten Jahren mehrere Arbeiten mit der Kette der Potenzen $x, x^2, x^3, \ldots$ sowie mit den beiden Ketten der Dicksonpolynome $g_1(d, x)$, $g_2(d, x)$, $g_3(d, x), \ldots, d = \pm 1$, über den ganzen Zahlen $\boldsymbol{Z}$ (vgl. [2]) und mit den davon induzierten Permutationen auf Restklassenringen $\boldsymbol{Z}/(m)$ beschäftigt. Insbesondere wird in [5], [6] und [7] die Fixpunktanzahl der von den Polynomen dieser Ketten dargestellten Permutationen von $\boldsymbol{Z}/(m)$ berechnet, und in [8], [1] und [4] die Gruppenstruktur der von diesen Ketten induzierten Permutationsgruppen von $\boldsymbol{Z}/(m)$ ermittelt.

In [2] (vgl. Chapter 3, Prop. 3.51) wurde bewiesen, daß für ein lineares Polynom $l = ax + b$ mit reellen Koeffizienten a und b die konjugierte Kette $\{l^{-1} \circ x^k \circ l \mid k \in \boldsymbol{N}\}$ bzw. $\{l^{-1} \circ g_k(d, x) \circ l \mid k \in \boldsymbol{N}\}$, $d = +1$, nur dann ganzzahlig ist, wenn $l = ax + b$ ganzzahlig ist. Daher lassen sich Eigenschaften der von den ganzzahligen konjugierten Ketten induzierten Permutationen von $\boldsymbol{Z}/(m)$ (z.B. Fixpunktanzahl, Zyklenlänge und Struktur der gebildeten Gruppen) unmittelbar aus den entsprechenden Eigenschaften der von den ursprünglichen Ketten induzierten Permutationen von $\boldsymbol{Z}/(m)$ herleiten.

Lidl und Müller haben in [3] die ungerade Kette der Potenzen $x, x^3, x^5, \ldots$ und die ungerade Kette der Dicksonpolynome $g_1(d, x)$, $g_3(d, x)$, $g_5(d, x), \ldots, d = \pm 1$, betrachtet. In der vorliegenden Arbeit wird gezeigt, daß konjugierte Ketten dieser Ketten auch dann ganzzahlig sein können, wenn das transformierende Polynom $l = ax + b$ nicht ganzzahlig ist.

Es werden alle konjugierten Ketten der ungeraden Kette der Potenzen sowie der Dicksonpolynome mit $d = +1$ bestimmt, welche ganzzahlig sind. Weiters werden Kriterien dafür angegeben, wann die Elemente der ganzzahligen konjugierten Ketten Permutationen von $\boldsymbol{Z}/(m)$ induzieren, und im Fall der Potenzen auch die Anzahl der Fixpunkte dieser Permutationen sowie

* Die vorliegende Arbeit wurde vom Österreichischen Fonds zur Förderung der wissenschaftlichen Forschung unter dem FWF-Projekt Nr. 5452 wesentlich unterstützt.

die Struktur der von diesen Permutationen gebildeten Permutationsgruppe bestimmt. Es zeigt sich, daß es unter diesen Permutationen solche gibt, die lediglich einen Fixpunkt aufweisen. Dieses Ergebnis ist insofern von entscheidender Relevanz für kryptographische Anwendungen, als nunmehr Verschlüsselungssysteme auf der Basis der Potenzen mit nur einem Fixpunkt konstruiert werden können. Für den Fall der Dicksonpolynome dürfte die Bestimmung von Ordnung und Fixpunktanzahl schwieriger sein als bei den Potenzen.

2. Die ungerade Kette der Potenzen $x, x^3, x^5, \ldots$ Damit für ein lineares Polynom $ax+b \in R[x]$ die Polynome

$$(ax+b)^{-1} \circ x^3 \circ (ax+b) = a^2 x^3 + 3abx^2 + 3b^2 x + \frac{1}{a}(b^3-b)$$

und

$$(ax+b)^{-1} \circ x^5 \circ (ax+b)$$

$$= a^4 x^5 + 5a^3 bx^4 + 10a^2 b^2 x^3 + 10ab^3 x^2 + 5b^4 x + \frac{1}{a}(b^5-b)$$

ganzzahlig sind, müssen a^2 und $3ab$ ganz, und damit ab rational sein. Da auch $(ab)^2$ ganz sein muß, und $\boldsymbol{Z}$ ganz abgeschlossen in seinem Quotientenkörper $\boldsymbol{Q}$ ist, muß ab sogar ganz sein. Ebenso sieht man, daß b^2 ganz sein muß und $b^3-b = ya$ mit $y \in \boldsymbol{Z}$ gelten muß.

Die Bedingungen a^2, ab, $b^2 \in \boldsymbol{Z}$ und $b^3-b = ya$ mit $y \in \boldsymbol{Z}$ sind auch hinreichend dafür, daß

$$\{(ax+b)^{-1} \circ x^k \circ (ax+b) \mid k = 2t-1,\ t \in \boldsymbol{N}\}$$

$$= \left\{\frac{1}{a}((ax+b)^k - b) \mid k = 2t-1,\ t \in \boldsymbol{N}\right\}$$

eine ganzzahlige Kette ist. Es gilt

$$\frac{1}{a}[(ax+b)^k - b] = \sum_{j=0}^{k-1} \binom{k}{j} a^{k-j-1} b^j x^{k-j} + \frac{1}{a}(b^k - b).$$

Für ungerades k ist $a^{k-j-1}b^j$ das Produkt einer geraden Anzahl von Faktoren a und b. Ist die Anzahl der Faktoren a und der Faktoren b gerade, dann ist das Produkt ganzzahlig. Ist die Anzahl der Faktoren a und der Faktoren b ungerade, dann ist das Produkt gleich ab mal einer geraden Potenz von a mal einer geraden Potenz von b, also wieder ganzzahlig. Aus $b^3-b = ya$, $y \in \boldsymbol{Z}$ folgt $b^5-b^3 = x_1 a$, $x_1 \in \boldsymbol{Z}$, und daher $b^5-b = (x_1+y)a = y_1 a$, $y_1 \in \boldsymbol{Z}$. So weiterschließend ergibt sich, daß $b^k-b = y_{(k-3)/2}\, a$ mit ganzem $y_{(k-3)/2}$, und wir erhalten

LEMMA 1. *Die Kette* $\{l^{-1} \circ x^k \circ l \mid k = 2t-1,\ t \in \boldsymbol{N}\}$ *ist genau dann ganzzahlig, wenn für die Koeffizienten des transformierenden Polynoms* $l = ax+b$ *gilt:* a^2, ab, b^2 *ganz und* $b^3-b = ya$ *mit ganzem* y.

Die Bedingungen für a und b in Lemma 1 kann man auch in der Form $a = r\sqrt{u}$, $b = s\sqrt{u}$ mit $r, s, u \in \boldsymbol{Z}$, u quadratfrei, und $s(us^2-1) \equiv 0 \bmod r$ schreiben. Wir erhalten somit

SATZ 1. *Die Kette* $\{l^{-1} \circ x^k \circ l \mid k = 2t-1,\ t \in \boldsymbol{N}\}$ *ist genau dann ganzzahlig, wenn für die Transformation* l *gilt* $l = \sqrt{u}(rx+s)$, *wo* u *quadratfrei ganz,* r, s *ganz, und* $s(us^2-1) \equiv 0 \bmod r$.

Nun untersuchen wir, unter welchen Bedingungen die ganzzahligen Konjugierten der Potenzen x^k, $k > 1$ ungerade, Permutationspolynome (PP) mod m sind.

$\frac{1}{a}[(ax+b)^k - b]$ ist genau dann PP mod p^e, wenn auch

$$\sum_{j=0}^{k-1} \binom{k}{j} a^{k-j-1} b^j x^{k-j}$$

ein PP ist. Setzt man hier $a = r\sqrt{u}$, $b = s\sqrt{u}$, dann wird dies zu

$$u^{(k-1)/2} \sum_{j=0}^{k-1} \binom{k}{j} r^{k-j-1} s^j x^{k-j},$$

und dies ist nur dann PP mod p^e, wenn $(u, p) = 1$. Im Fall $(u, p) = 1$ ist dies genau dann PP mod p^e, wenn auch $\sum_{j=0}^{k-1} \binom{k}{j} r^{k-j-1} s^j x^{k-j}$ ein PP mod p^e ist. Ist $(r, p) = p$, so ist dies nur dann ein PP mod p^e, wenn es ein PP mod p ist, und dies ist der Fall genau für $(ks, p) = 1$. Da in diesem Fall die Ableitung des Polynoms stets $\not\equiv 0 \bmod p$, ist es in diesem Fall auch PP mod p^e. Ist aber $(r, p) = 1$, so ist

$$\sum_{j=0}^{k-1} \binom{k}{j} r^{k-j-1} s^j x^{k-j} \equiv r^{-1}\left((rx+s)^k - s^k\right) \bmod p^e,$$

und dies ist ein PP mod p^e genau dann, wenn $(rx+s)^k$ ein PP mod p^e ist, also wenn $e = 1$ und $(k, p-1) = 1$. Somit ist $\frac{1}{a}[(ax+b)^k - b]$ ein PP mod p^e genau dann, wenn $(u, p) = 1$ und entweder $(r, p) = p$, $(ks, p) = 1$ oder $(r, p) = 1$, $e = 1$ und $(k, p-1) = 1$.

Das mit $\sqrt{u}(rx+s)$ Transformierte von x^k ist genau dann PP mod m, wenn $(u, m) = 1$, und wenn für jeden Primzahlpotenzfaktor $p_i^{e_i}$ von m entweder gilt $(r, p_i) = p_i$, $(ks, p_i) = 1$ oder $(r, p_i) = 1$, $e_i = 1$, $(k, p_i-1) = 1$. Zusammenfassend erhält man

SATZ 2. *Das mit* $\sqrt{u}(rx+s)$ *Transformierte von* x^k *mit* $k > 1$ *ist genau dann Permutationspolynom* mod m, *wenn* $(u, m) = 1$, $(r, ks, m) = 1$, *und wenn*

für jede Primzahlpotenz $p_i^{e_i}$ *der Faktorzerlegung von* m *mit* $(r, p_i) = 1$ *gilt* $e_i = 1$, $(k, p_i - 1) = 1$.

Wir untersuchen nun die Fixpunktanzahl der Permutationen $x \to l^{-1} \circ x^k \circ l \bmod m$ sowie die Struktur der von diesen Permutationen bei festem l gebildeten Permutationsgruppe modulo m.

Aufgrund des Chinesischen Restsatzes beschränken wir uns bei der Berechnung der Fixpunktanzahl der durch $l^{-1} \circ x^k \circ l$, $l = \sqrt{u}(rx+s)$, induzierten Permutation von $Z/(m)$ auf den Fall $m = p^e$. Wir unterscheiden dabei drei Fälle:

(a) $(r, p) = 1$, u ist Quadrat mod p.

(b) $(r, p) = 1$, u ist Nichtquadrat mod p.

(c) $(r, p) > 1$.

Im Fall (a) folgt aus Satz 2, daß $e = 1$. Es gibt dann eine ganze Zahl v mit $(v, p) = 1$ und $v^2 \equiv u \bmod p$. Daher ist die Fixpunktanzahl von $l^{-1} \circ x^k \circ l \bmod p$ gleich jener von $x^k \bmod p$, und diese ist gemäß [5] gegeben durch $(k-1, p-1)+1$.

Auch im Fall (b) folgt aus Satz 2 $e = 1$. Die Fixpunktzahl von $l^{-1} \circ x^k \circ l$ ist gleich der Fixpunktzahl von $\frac{1}{\sqrt{u}} x \circ x^k \circ \sqrt{u} x$, also gleich der Lösungsanzahl von $u^{(k-1)/2} x^k \equiv x \bmod p$.

Es ist $u^{(k-1)/2} x^k \equiv x \bmod p$ für $x \not\equiv 0 \bmod p$ gleichbedeutend mit $(ux^2)^{(k-1)/2} \equiv 1 \bmod p$. Wir haben also alle quadratischen Nichtreste h mit $h^{(k-1)/2} \equiv 1 \bmod p$ zu bestimmen und jeder davon liefert mittels der Kongruenz $ux^2 \equiv h \bmod p$ genau zwei Fixpunkte.

Schreibt man $v_q(t)$ für die Vielfachheit, mit der die Primzahl q in der Primfaktorzerlegung von t vorkommt, so ist die Anzahl der Fixpunkte $x \not\equiv 0 \bmod p$ von $l^{-1} \circ x^k \circ l$ für $v_2(k-1) > v_2(p-1)$ gleich $(k-1, p-1)$ und für $v_2(k-1) \leqslant v_2(p-1)$ gleich 0.

Wir fassen die bisherigen Ergebnisse zusammen in

Satz 3. *Sei* $l = \sqrt{u}(rx+s)$, *sei* $t_k(x) = l^{-1} \circ x^k \circ l$ *Permutationspolynom modulo der Primzahl* p, *und gelte* $(r, p) = 1$. *Dann ist im Fall, daß* u *quadratischer Rest* mod p *ist, die Fixpunktanzahl von* $t_k(x)$ mod p *gegeben durch* $(k-1, p-1)+1$, *und im Fall, daß* u *quadratischer Nichtrest* mod p *ist, für* $v_2(k-1) > v_2(p-1)$ *ebenfalls durch* $(k-1, p-1)+1$, *und für* $v_2(k-1) \leqslant v_2(p-1)$ *durch* 1.

Folgerung. Sei $l = \sqrt{u}(rs+s)$, sei $t_k(x) = l^{-1} \circ x^k \circ l$ Permutationspolynom modulo der quadratfreien Zahl $m = p_1 p_2 \dots p_r q_1 q_2 \dots q_s$, sei $(r, m) = 1$, und seien $q_1, q_2, \dots, q_s$ jene Primfaktoren p von m, für welche u quadratischer Nichtrest ist und $v_2(k-1) \leqslant v_2(p-1)$ gilt. Dann ist die Fixpunktzahl von $t_k(x)$ gegeben durch

$$\prod_{i=1}^{r} ((d, p_i - 1) + 1)$$

wenn $v = [p_1 - 1, p_2 - 1, \dots, p_r - 1]$ das kleinste gemeinsame Vielfache der $p_i - 1$ bezeichnet und $d = (k-1, v)$ der größte gemeinsame Teiler von $k-1$ mit v ist.

Nun betrachten wir den Fall (c). Es sei $r = p^n g$ mit $n \geqslant 1$ und $(g, p) = 1$. Aufgrund von Satz 2 gilt in diesem Fall $(ks, p) = (s, p) = 1$. Ist x Fixpunkt der Transformierten mit $ax+b$, dann gilt

$$\frac{1}{a}((ax+b)^k - b) \equiv x \bmod p^e,$$

was wegen $a = r\sqrt{u}$, $b = s\sqrt{u}$ gleichbedeutend ist mit

$$u^{(k-1)/2}(rx+s)^k \equiv rx+s \bmod p^{e+n}. \tag{1}$$

Wegen der Invertierbarkeit von $rx+s \bmod p^{e+n}$ ist (1) äquivalent mit

$$((1+s^{-1}rx)^2 s^2 u)^{(k-1)/2} \equiv 1 \bmod p^{e+n}.$$

Aufgrund von Satz 1 gilt $s(us^2-1) \equiv 0 \bmod r$, und daraus folgt wegen $(s, p) = 1$, daß $us^2 \equiv 1 \bmod p^n$. Ebenso folgt aus $r \equiv 0 \bmod p^n$, daß $1+s^{-1}rx \equiv 1 \bmod p^n$. Bezeichnet G die Untergruppe der primen Restklassengruppe mod p^{e+n} aus den Restklassen, welche $\equiv 1 \bmod p^n$ sind, so ist also $(1+s^{-1}rx)^2 s^2 u$ ein Element w dieser Untergruppe, für welches gilt $w^{(k-1)/2} \equiv 1 \bmod p^{e+n}$. Sei nun zunächst $p > 2$. Aus

$$(1+s^{-1}rx)^2 s^2 u \equiv (1+s^{-1}ry)^2 s^2 u \bmod p^{e+n}$$

folgt, da für $p > 2$ die Ordnung von G ungerade ist, daß $1+s^{-1}rx \equiv 1+s^{-1}ry \bmod p^{e+n}$, und es ergibt sich $x \equiv y \bmod p^e$. Schließlich wird für $p > 2$ jedes Element $w \in G$ tatsächlich aus einem Fixpunkt x erhalten, denn die Kongruenz $(1+s^{-1}rx)^2 s^2 u \equiv w \bmod p^{e+n}$ ist für $w \equiv 1 \bmod p^n$ wegen $s^2 u \equiv 1 \bmod p^n$ tatsächlich lösbar. Also ist im Fall $p > 2$ die gesuchte Fixpunktanzahl gleich der Anzahl der $w \in G$ mit $w^{(k-1)/2} = 1$, und diese ist gleich $((k-1)/2, p^e)$.

Sei nun $p = 2$. Dieser Fall ist schwieriger, da in diesem Fall die Lösung von $(1+s^{-1}rx)^2 s^2 u \equiv w \bmod p^{e+n}$ nicht mehr eindeutig bestimmt ist.

Wir setzen zunächst voraus, daß nicht gilt $n = e = 1$. Es ist dann $e+n \geqslant 3$. Bezeichnet allgemein Z_b die Gruppe der primen Restklassen modulo b, dann gilt $Z_{2^{n+e}} = \{\overline{(-1)}^{\alpha} \overline{5}^{\beta} \mid 0 \leqslant \alpha < 2,\ 0 \leqslant \beta < 2^{n+e-2}\}$, wenn allgemein $\bar{u}$ die Restklasse von u modulo 2^{n+e} bezeichnet. Für $n > 1$ gilt $a \equiv 1 \bmod 4$ für alle $a \in G$, wegen $|G| = 2^e$ also $G = \{\overline{5}^{2^{n-2}\gamma} \mid 0 \leqslant \gamma < 2^e\}$. Für $n = 1$ aber gilt $G = Z_{2^{n+e}}$. Es sei H die Untergruppe von G, welche aus den Quadraten der Elemente von G gebildet wird, dann gilt $H = \{\overline{5}^{2^{n-1}\gamma} \mid 0 \leqslant \gamma < 2^{e-1}\}$ für $n = 1$ und $H = \{\overline{5}^{2\beta} \mid 0 \leqslant \beta < 2^{e-2}\}$ für $n = 1$. Ist $I = \{v \in G \mid v \equiv 1 \bmod 2^{n+1}\}$ für $n > 1$ und $I = \{v \in G \mid v \equiv 1 \bmod 2^{n+2}\}$ für $n = 1$, dann ist I im Fall $n > 1$ eine Untergruppe von G der Ordnung 2^{e-1}, und im Fall $n = 1$ eine Untergruppe der Ordnung 2^{e-2}, deren Elemente $\equiv 1 \bmod 4$ sind, also gilt $I = H$.

Wir betrachten nun die Kongruenz $(1+s^{-1}rx)^2 s^2 u \equiv w \bmod 2^{e+n}$, die gleichbedeutend ist mit der Kongruenz

$$(2) \qquad (1+s^{-1}rx)^2 \equiv w(s^2u)^{-1} \bmod 2^{e+n}.$$

(2) ist wegen $r \equiv 0 \bmod p^n$ genau dann lösbar, wenn die rechte Seite das Quadrat eines Elements von G ist, denn jedes Element von G läßt sich schreiben in der Form $1+s^{-1}rx$, und hat in diesem Fall für $n > 1$, wo G zyklisch ist, 2 Lösungen, und für $n = 1$, wo G das direkte Produkt einer zyklischen Gruppe der Ordnung 2 mit einer weiteren zyklischen Gruppe ist, 4 Lösungen.

Ist nun $(s^2u)^{-1}$ das Quadrat eines Elements von G, was wegen $H = I$ gleichbedeutend ist mit $s^2u \equiv 1 \bmod 2^{n+1}$ für $n > 1$ und mit $s^2u \equiv 1 \bmod 2^{n+2}$ für $n = 1$, dann ist die rechte Seite von (2) genau dann Quadrat eines Elements von G, wenn w eines ist.

Da nach dem früher Festgestellten jeder Fixpunkt x aus einer Kongruenz (2) mit einem w, welches $w^{(k-1)/2} \equiv 1 \bmod 2^{e+n}$ erfüllt, erhalten wird und jedes derartige x tatsächlich ein Fixpunkt ist, müssen wir also die $w \in H$ mit $w^{(k-1)/2} = 1$ abzählen. Aufgrund der oben festgestellten Struktur von H ergibt sich dabei der Wert $(2^{e-1}, (k-1)/2)$ für $n > 1$ und der Wert $(2^{e-2}, (k-1)/2)$ für $n = 1$. Damit ergibt sich für die Fixpunktzahl der Wert

$$2(2^{e-1}, (k-1)/2) = (2^e, k-1) \qquad \text{für } n > 1,$$

$$4(2^{e-2}, (k-1)/2) = (2^e, 2(k-1)) \qquad \text{für } n = 1.$$

Nun sei $(s^2u)^{-1}$ nicht Quadrat eines Elementes von G. Dies ist wegen $H = I$ gleichbedeutend mit $s^2u \not\equiv 1 \bmod 2^{n+1}$, falls $n > 1$, und mit $s^2u \not\equiv 1 \bmod 2^{n+2}$, falls $n = 1$. Die Kongruenz (2) ist nun lösbar genau für die w von der Gestalt $(s^2u)v$, wo v Quadrat eines Elementes von G ist, also genau für $w = (s^2u)v$ mit $v \in H$. So wie im vorhergehenden Fall müssen wir die Anzahl dieser w ermitteln, für die $w^{(k-1)/2} = 1$ gilt.

Im Falle $n > 1$ ist G eine zyklische Gruppe der Ordnung 2^e. Ist g erzeugendes Element dieser Gruppe, dann besteht H genau aus den geraden Potenzen von g. Wegen $s^2u \notin H$ gilt daher $\{(s^2u)v \mid v \in H\} = \{g^{2l+1} \mid 0 \leqslant l < 2^{e-1}\}$. Es ist aber $(g^{2l+1})^{(k-1)/2} = 1$ wegen $g^{2^e} = 1$ gleichbedeutend mit $g^{(k-1)/2} = 1$, und dies ist gleichbedeutend mit $\frac{1}{2}(k-1) \equiv 0 \bmod 2^e$. Die Anzahl der w mit $w^{(k-1)/2} = 1$ beträgt somit 0 für $k \not\equiv 1 \bmod 2^{e+1}$ und 2^{e-1} für $k \equiv 1 \bmod 2^{e+1}$, und die Fixpunktzahl ist 0 im ersten Fall, 2^e im zweiten Fall.

Nun sei $n = 1$. In diesem Fall ist G das direkte Produkt zweier zyklischer Gruppen C_2 und $C_{2^{e-1}}$ der Ordnung 2 und 2^{e-1} mit den erzeugenden Elementen $\overline{-1}$ und $\overline{5}$. H besteht genau aus den geraden Potenzen von $\overline{5}$, wegen $s^2u \notin H$ gilt also $s^2u = \pm\overline{5}^{2h+1}$ oder $s^2u = -\overline{5}^{2h}$. Im ersten Fall – dieser ist gleichbedeutend mit $s^2u \equiv \mp 3 \bmod 8$ – gilt $\{(s^2u)v \mid v \in H\}$ $= \{\pm\overline{5}^{2l+1} \mid 0 \leqslant l < 2^{e-2}\}$, es ist aber $(\pm\overline{5}^{2l+1})^{(k-1)/2} = 1$ wegen $\pm\overline{5}^{2l+1}$ $= (\pm\overline{5})^{2l+1}$ und $(\pm\overline{5})^{2^{e-1}} = 1$ gleichbedeutend mit $(\pm\overline{5})^{(k-1)/2} = 1$ und das ist äquivalent mit $\frac{1}{2}(k-1) \equiv 0 \bmod 2^{e-1}$, was wiederum gleichbedeutend mit $k-1 \equiv 0 \bmod 2^e$ ist. Die Anzahl der w mit $w^{(k-1)/2} = 1$ beträgt somit 0 für $k \not\equiv 1 \bmod 2^e$ und 2^{e-2} für $k \equiv 1 \bmod 2^e$ und die Fixpunktzahl ist 0 im ersten Fall, $2^e = (2(k-1), 2^e)$ im zweiten Fall. Im Fall $s^2u = -\overline{5}^{2h}$ – dieser ist gleichbedeutend mit $s^2u \equiv -1 \bmod 8$ – gilt $\{(s^2u)v \mid v \in H\} =$ $\{-\overline{5}^{2l} \mid 0 \leqslant l < 2^{e-2}\}$, es ist aber $(-\overline{5}^{2l})^{(k-1)/2} = 1$ wegen $(-\overline{5}^{2l})^{(k-1)/2} =$ $(-1)^{(k-1)/2}(\overline{5}^{2l})^{(k-1)/2}$ nur lösbar für $\frac{1}{2}(k-1) \equiv 0 \bmod 2$. Ist dies erfüllt, dann hat die Gleichung, da H eine zyklische Gruppe der Ordnung 2^{e-2} ist, insgesamt $((k-1)/2, 2^{e-2})$ Lösungen. Die Fixpunktzahl ist also 0 für $k \not\equiv 1 \bmod 4$ und $(2^e, 2(k-1))$ für $k \equiv 1 \bmod 4$.

Schließlich haben wir noch den Fall $n = 1$, $e = 1$ zu betrachten. In diesem Fall gilt $Z_{2^{n+e}} = G = \{(\overline{-1})^\alpha \mid 0 \leqslant \alpha \leqslant 1\}$ und $H = \{\overline{1}\}$. Die Kongruenz (2) ist für $s^2u \equiv 1 \bmod 4$ genau im Falle $w = 1$ lösbar, dieses erfüllt $w^{(k-1)/2} = 1$, die Fixpunktzahl ist daher $2 = (2(k-1), 2)$. Für $s^2u \equiv -1 \bmod 4$ ist (2) genau im Falle $w = -1$ lösbar, dieses erfüllt $w^{(k-1)/2} = 1$ genau dann, wenn $\frac{1}{2}(k-1) \equiv 0 \bmod 2$. Die Fixpunktzahl beträgt daher 0 für $k \not\equiv 1 \bmod 4$ und $2 = (2(k-1), 2)$ für $k \equiv 1 \bmod 4$.

Wir fassen unsere Ergebnisse zusammen in folgendem

Satz 4. *Es sei $l = \sqrt{u}(rx+s)$, es sei $t_k(x) = l^{-1} \circ x^k \circ l$ ein Permutationspolynom modulo p^e, und es gelte $r = p^n g$ mit $n \geqslant 1$ und $(g, p) = 1$. Dann ist die Fixpunktzahl von $t_k(x)$ im Falle eines ungeraden p gegeben durch $((k-1)/2, p^e)$. Ist aber $p = 2$, dann ist die Fixpunktzahl gegeben im Fall $n > 1$ durch*

$$\begin{array}{ll} (k-1, 2^e) & \text{falls } s^2u \equiv 1 \bmod 2^{n+1}, \\ \left.\begin{array}{ll} (k-1, 2^e) & \text{für } k \equiv 1 \bmod 2^{e+1} \\ 0 & \text{für } k \not\equiv 1 \bmod 2^{e+1} \end{array}\right\} & \text{falls } s^2u \not\equiv 1 \bmod 2^{n+1}, \end{array}$$

und im Fall $n = 1$ wegen $s^2 \equiv 1 \bmod 8$ gegeben durch

$$\begin{array}{ll} (2(k-1), 2^e) & \text{falls } u \equiv 1 \bmod 8 \text{ für } e > 1 \text{ und} \\ & u \equiv 1 \bmod 4 \text{ für } e = 1, \\ \left.\begin{array}{ll} (2(k-1), 2^e) & \text{für } k \equiv 1 \bmod 4 \\ 0 & \text{für } k \not\equiv 1 \bmod 4 \end{array}\right\} & \text{falls } u \equiv -1 \bmod 8 \text{ für } e > 1 \\ & \text{und } u \equiv -1 \bmod 4 \text{ für } e = 1, \\ \left.\begin{array}{ll} (2(k-1), 2^e) & \text{für } k \equiv 1 \bmod 2^e \\ 0 & \text{für } k \not\equiv 1 \bmod 2^e \end{array}\right\} & \text{falls } u \equiv \pm 3 \bmod 8. \end{array}$$

Wir wollen nun die Struktur der von den Permutationen $x \to l^{-1} \circ x^k \circ l \bmod m$ bei festem $l = \sqrt{u}(rx+s)$ gebildeten Permutationsgruppe untersuchen. Es sei zunächst $m = p^e$. Da für $(u, p^e) \neq 1$ die Gruppe nur aus dem Einselement besteht, können wie annehmen, daß $(u, p^e) = 1$ gilt. Zunächst betrachten wir den Fall $(r, p^e) = 1$. Nach Satz 2 kann in diesem Fall $e = 1$ angenommen werden – andernfalls besteht die Gruppe nur aus

dem Einselement. Wegen $l = \sqrt{u}\,x \circ (rx+s)$ ist die zu untersuchende Gruppe isomorph zu der durch die Polynome $\frac{1}{\sqrt{u}} x \circ x^k \circ \sqrt{u}x = u^{(k-1)/2} x^k$ erzeugten Permutationsgruppe modulo p.

Es ist $u^{(k-1)/2} x^k \equiv u^{(l-1)/2} x^l \bmod p$ für alle x genau dann erfüllt, wenn gilt

$$(ux^2)^{(k-1)/2} \equiv 1 \bmod p \quad \text{für alle } x \not\equiv 0 \bmod p.$$

Ist u ein quadratischer Rest modulo p, dann durchläuft ux^2 alle quadratischen Reste modulo p, und darunter gibt es einen mit Ordnung $(p-1)/2$. Also gilt $k \equiv l \bmod p-1$. Ist aber u quadratischer Nichtrest modulo p, dann durchläuft ux^2 alle quadratischen Nichtreste modulo p, darunter gibt es einen mit Ordnung $p-1$, also gilt $k \equiv l \bmod 2(p-1)$. Ersichtlich sind die soeben gefundenen Bedingungen auch hinreichend dafür, daß $u^{(k-1)/2} x^k \equiv u^{(l-1)/2} x^l \bmod p$ für alle ganzen x gilt.

Da wegen Satz 2 das Polynom $\frac{1}{\sqrt{u}} x \circ x^k \circ \sqrt{u}x$ genau dann ein Permutationspolynom modulo p ist, wenn $(k, p-1) = 1$, erhalten wir somit

Satz 5. *Ist $l = \sqrt{u}(rx+s)$, ist $(u, p) = (r, p) = 1$ und p eine Primzahl, dann ist die durch die Permutationen $x \to l^{-1} \circ x^k \circ l \bmod p$ gebildete Permutationsgruppe isomorph zur Gruppe der primen Restklassen modulo $\eta \cdot (p-1)$, wobei $\eta = 1$, wenn u quadratischer Rest mod p ist, und $\eta = 2$, wenn u quadratischer Nichtrest mod p ist.*

Nun wenden wir uns dem Fall $(r, p^e) > 1$ zu. Wir können annehmen, daß in $l = \sqrt{u}(rx+s)$ gilt $(s, p) = 1$, andernfalls hat die Gruppe ja nur ein Element. Wir setzen $t_k(x) = l^{-1} \circ x^k \circ l$ und beweisen zunächst folgendes

Lemma 2. *Es sei $w(m)$ eine natürliche Zahl mit der Eigenschaft, daß die Abbildung $x \to t_k(x) \bmod m$ genau dann eine Permutation ist, wenn $(k, w(m)) = 1$, und genau dann die identische Permutation ist, wenn $k \equiv 1 \bmod w(m)$. Dann ist die Gruppe der Permutationen $x \to t_k(x) \bmod m$ isomorph zur Gruppe der primen Restklassen modulo $w(m)$.*

Beweis. Sei $(k, w(m)) = (l, w(m)) = 1$ und $k \equiv l \bmod w(m)$. Man wähle h so, daß $hk \equiv hl \equiv 1 \bmod w(m)$, dann induzieren $t_{hk}(x) = t_h(t_k(x))$ und $t_{hl}(x) = t_h(t_l(x))$ beide die identische Permutation, daher induzieren auch $t_k(t_h(t_k(x)))$ und $t_k(t_h(t_l(x)))$ dieselbe Permutation, da aber $t_k(t_h(x))$ die identische Permutation induziert, induzieren auch $t_k(x)$ und $t_l(x)$ dieselbe Permutation. Ist dies umgekehrt der Fall und induziert $t_h(x)$ die Inverse der von $t_k(x)$ induzierten Permutation, so induzieren $t_{hk}(x)$ und $t_{hl}(x)$ beide die identische Permutation, also gilt $1 \equiv hk \equiv hl \bmod w(m)$, also $k \equiv l \bmod w(m)$.

Da die Abbildung $x \to t_k(x) \bmod m$ genau dann die identische Permutation ist, wenn sie m Fixpunkte besitzt, ergibt sich aus Satz 2 und Satz 4 somit folgender

Satz 6. *Es sei $l = \sqrt{u}(rx+s)$ und es gelte $r = p^n g$ mit $n \geqslant 1$ und $(g, p) = 1$ sowie $(s, p) = 1$. Dann ist die durch die Permutationen $x \to l^{-1} \circ x^k \circ l \bmod p^e$ gebildete Permutationsgruppe isomorph zur Gruppe der primen Restklassen modulo $w(p^e)$, wobei gilt*

$$w(p^e) = 2p^e \quad \text{für ungerades } p,$$

und

$$w(2^e) = \begin{cases} 2^e & \text{falls } n > 1 \text{ und } s^2 u \equiv 1 \bmod 2^{n+1}, \\ 2^{e+1} & \text{falls } n > 1 \text{ und } s^2 u \not\equiv 1 \bmod 2^{n+1}, \\ 2^{e-1} & \text{falls } n = 1 \text{ und } u \equiv 1 \bmod 8 \text{ für } e > 1, \\ & \qquad u \equiv 1 \bmod 4 \text{ für } e = 1, \\ 2^{\max(e-1,2)} & \text{falls } n = 1 \text{ und } u \equiv -1 \bmod 8 \text{ für } e > 1, \\ & \qquad u \equiv -1 \bmod 4 \text{ für } e = 1, \\ 2^e & \text{falls } n = 1 \text{ und } u \equiv \pm 3 \bmod 8. \end{cases}$$

Nun können wir auch die Struktur der Gruppe der Permutationen $x \to l^{-1} \circ x^k \circ l \bmod m$ im Falle eines beliebigen $l = \sqrt{u}(rx+s)$ und $m = p_1^{e_1} p_2^{e_2} \ldots p_\nu^{e_\nu}$ leicht feststellen. Ein Polynom $t_k(x)$ induziert nämlich genau dann eine Permutation modulo m, wenn es eine Permutation modulo $p_i^{e_i}$, $i = 1, 2, \ldots, \nu$, induziert, und die Polynome $t_k(x)$, $t_l(x)$ induzieren genau dann dieselbe Abbildung modulo m, wenn sie dieselbe Abbildung modulo $p_i^{e_i}$, $i = 1, 2, \ldots, \nu$, induzieren. Wie wir aber aus Satz 2, Satz 5 und Satz 6 leicht sehen können, gibt es nichtnegative ganze Zahlen $w(p_i^{e_i})$, $i = 1, 2, \ldots, \nu$, so daß $t_k(x)$ eine Permutation modulo $p_i^{e_i}$ genau dann induziert, wenn $(k, w(p_i^{e_i})) = 1$ und daß $t_k(x)$ und $t_l(x)$ mit zu $w(p_i^{e_i})$ teilerfremden k, l genau dann dieselbe Permutation modulo $p_i^{e_i}$ induzieren, wenn $k \equiv l \bmod w(p_i^{e_i})$. Daher ist die zu untersuchende Gruppe isomorph zur Gruppe der primen Restklassen modulo dem kleinsten gemeinsamen Vielfachen der $w(p_i)$.

3. Die Ungerade Kette der Dickson-Polynome $g_k(1, x)$.

$$g_k(1, x) = \sum_{t=0}^{\lfloor k/2 \rfloor} \frac{k}{k-t} \binom{k-t}{t} (-1)^t x^{k-2t}, \quad k = 2t-1, \quad t \in N.$$

Es gilt

$$(ax+b)^{-1} \circ g_3(1, x) \circ (ax+b) = a^2 x^3 + 3abx^2 + (3b^2-3)x + \frac{1}{a}(g_3(1, b) - b)$$

und

$$(ax+b)^{-1} \circ g_5(1, x) \circ (ax+b) = a^4 x^5 + 5a^3 bx^4 + (10a^2 b^2 - 5a^2) x^3 + (10ab^3 - 15ab) x^2 + (5b^4 - 15b^2 + 5) x + \frac{1}{a}(g_5(1, b) - b).$$

In einer ganzzahligen Kette müssen also a^2, $3ab$, $10a^2b^2-5a^2\in\mathbf{Z}$, daher $a^2b^2\in\mathbf{Z}$, und somit $ab\in\mathbf{Z}$ sein. Ferner müssen $3b^2$, $5b^4-15b^2\in\mathbf{Z}$, daher $5b^4\in\mathbf{Z}$ und somit $10b^4-9b^4=b^4\in\mathbf{Z}$, also $b^2\in\mathbf{Z}$ sein. Schließlich gilt auch $g_3(1,b)-b=ya$ mit ganzem y.

Umgekehrt sind die Bedingungen a^2, ab, $b^2\in\mathbf{Z}$, $g_3(1,b)-b=ya$ mit $y\in\mathbf{Z}$ auch hinreichend dafür, daß

$$(3)\quad (ax+b)^{-1}\circ g_k(1,x)\circ(ax+b)=\sum_{t=0}^{[k/2]}\frac{k}{k-t}\binom{k-t}{t}(-1)^t\frac{1}{a}(ax+b)^{k-2t}-\frac{b}{a}$$

eine ganzzahlige Kette ergibt. Wie wir beim Beweis von Lemma 1 gesehen haben, folgt aus der Ganzzahligkeit von a^2, ab, b^2, daß die Koeffizienten der positiven Potenzen von x in $(1/a)(ax+b)^{k-2t}$ ganz sind. Aus der Ganzzahligkeit der Koeffizienten von $g_k(1,x)$ folgt somit, daß auch die Koeffizienten der positiven Potenzen von x in (3) ganze Zahlen sind. Der Koeffizient des Absolutgliedes ist gegeben durch $(1/a)(g_k(1,b)-b)$. Wir zeigen, daß auch er ganz ist. Dazu verwenden wir die für alle $n\geqslant 1$ gültige Rekursionsformel (vgl. etwa [2]) $g_{n+1}(1,x)=g_n(1,x)x-g_{n-1}(1,x)$ und bemerken zunächst, daß alle im Folgenden vorkommenden y_i ganze Zahlen sind. Nach Voraussetzung gilt $g_3(1,b)=b+y_3a$. Die vorher angegebene Rekursionsformel ergibt $g_2(1,x)x=g_3(1,x)+x$, daraus folgt $bg_2(1,b)=2b+y_2a$. Es sei schon gezeigt, daß für ein ungerades $n\geqslant 3$ gilt

$$g_n(1,b)=b+y_na,\qquad bg_{n-1}(1,b)=2b+y_{n-1}a.$$

Dann haben wir

$$\begin{aligned}g_{n+2}(1,b)&=g_{n+1}(1,b)b-g_n(1,b)=g_n(1,b)b^2-g_n(1,b)-bg_{n-1}(1,b)\\&=b^3+y_nb^2a-b-y_na-2b-y_{n-1}a=g_3(1,b)+za\end{aligned}$$

mit ganzem z, daher gilt

$$g_{n+2}(1,b)-b=y_3a+za=y_{n+2}a,$$

und daraus folgt, daß

$$g_{n+1}(1,b)b=g_{n+2}(1,b)+g_n(1,b)=b+y_{n+2}a+b+y_na=2b+y_{n+1}a.$$

Vollständige Induktion ergibt nun sofort die Behauptung.

Somit haben wir

LEMMA 3. *Die Kette* $\{l^{-1}\circ g_k(1,x)\circ l\mid k=2t-1,\ t\in\mathbf{N}\}$ *ist genau dann ganzzahlig, wenn für die Koeffizienten des transformierenden Polynoms* $l=ax+b$ *gilt:* a^2, ab, b^2 *ganz und* $b^3-4b=ya$ *mit ganzem* y.

So wie in Satz 1 ergibt sich, daß $a=r\sqrt{u}$, $b=s\sqrt{u}$, wo r, s ganze Zahlen sind und u eine quadratfreie ganze Zahl ist, die die Bedingung $us^3-4s\equiv 0 \bmod r$ erfüllt. Wir erhalten somit

SATZ 7. *Die Kette* $\{l^{-1}\circ g_k(1,x)\circ l\mid k=2t-1,\ t\in\mathbf{N}\}$ *ist genau dann ganzzahlig, wenn für die Transformation* l *gilt* $l=\sqrt{u}(rx+s)$, *wo* u *quadratfrei ganz,* r, s *ganz und* $s(us^2-4)\equiv 0 \bmod r$.

Wir untersuchen nun, unter welchen Bedingungen ein ganzzahliges Polynom $t_k(x)$ der Kette von Satz 7 ein Permutationspolynom (PP) mod m ist. Aufgrund des Chinesischen Restsatzes können wir uns dabei auf den Fall $m=p^e$ (p Primzahl) beschränken. Klarerweise ist $t_k(x)$ genau dann ein PP mod p^e, wenn $h_k(x)=t_k(x)-t_k(0)$ eines ist. Wir betrachten zunächst den Fall $u\equiv 0 \bmod p$. In (3) enthalten alle Summanden mit $k-2t\geqslant 3$ wegen $a=r\sqrt{u}$, $b=s\sqrt{u}$ einen Faktor u, da aber für $t=(k-1)/2$ gilt

$$\frac{k}{k-t}\binom{k-t}{t}=k,$$

erhalten wir $h_k(x)\equiv\pm kx \bmod p$ und daher $h_k'(x)\equiv\pm k \bmod p$. Nach bekannten Sätzen (siehe etwa [2]) ist also $h_k(x)$ genau dann ein PP mod p^e, wenn $k\not\equiv 0 \bmod p$.

Sei nun also $u\not\equiv 0 \bmod p$. Ist $r\equiv 0 \bmod p$, dann ist wegen $s(us^2-4)\equiv 0 \bmod r$ entweder $s\equiv 0 \bmod p$ oder $s\not\equiv 0 \bmod p$ und $us^2\equiv 4 \bmod p$. Aus (3) erhalten wir bei Berücksichtigung von $r\equiv 0 \bmod p$ nun

$$h_k(x)\equiv\left[\sum_{t=0}^{[k/2]}\frac{k}{k-t}\binom{k-t}{t}(-1)^t(k-2t)\,b^{k-2t-1}\right]x \bmod p.$$

Ist $s\equiv 0 \bmod p$, dann fallen hier alle Glieder, welche b enthalten, weg und wir erhalten $h_k(x)\equiv\pm kx \bmod p$. Ist $s\not\equiv 0 \bmod p$ und $us^2\equiv 4 \bmod p$, dann gilt

$$b^{k-2t-1}\equiv(b^2)^{(k-2t-1)/2}\equiv(us^2)^{(k-2t-1)/2}\equiv 4^{(k-2t-1)/2}\equiv 2^{k-2t-1} \bmod p,$$

und daher

$$\sum_{t=0}^{[k/2]}\frac{k}{k-t}\binom{k-t}{t}(-1)^t(k-2t)\,b^{k-2t-1}\equiv g_k'(1,2) \bmod p.$$

Da aber bekanntlich $g_k'(1,2)=k^2$ (siehe etwa [7]), gilt $h_k(x)\equiv k^2x \bmod p$. Auch in diesen beiden Fällen erhalten wir also, daß $h_k(x)$ genau dann ein PP mod p^e ist, wenn $k\not\equiv 0 \bmod p$.

Sei schließlich $u\not\equiv 0 \bmod p$ und $r\not\equiv 0 \bmod p$. Wegen $l=\sqrt{u}x\circ(rx+s)$ ist nun $l^{-1}\circ g_k(1,x)\circ l$ genau dann ein PP mod p^e, wenn $\frac{1}{\sqrt{u}}x\circ g_k(1,x)\circ\sqrt{u}x$ eines ist.

Nun gilt

$$\frac{1}{\sqrt{u}} x \circ g_k(1, x) \circ \sqrt{u}x = \sum_{t=0}^{[k/2]} \frac{k}{k-t} \binom{k-t}{t} (-1)^t u^{(k-1)/2-t} x^{k-2t}$$

$$\equiv u^{(k-1)/2} \sum_{t=0}^{[k/2]} \frac{k}{k-t} \binom{k-t}{t} (-v)^t x^{k-2t} \bmod p^e,$$

wenn v so gewählt wird, daß $uv \equiv 1 \bmod p^e$. Da aber das zuletzt erhaltene Polynom genau dann ein PP mod p ist, wenn $(k, p^2-1) = 1$, und genau dann ein PP mod p^e mit $e > 1$ ist, wenn $(k, p(p^2-1)) = 1$ (vgl. etwa [2]), gilt

SATZ 8. *Das mit* $\sqrt{u}(rx+s)$ *Transformierte von* $g_k(1, x)$ *mit* $k > 1$ *ist genau dann Permutationspolynom* mod p^e, *wenn* $(ur, p) = p$ *sowie* $(k, p) = 1$, *und wenn* $(ur, p) = 1$ *sowie* $(k, p^2-1) = 1$ *für* $e = 1$ *bzw.* $(k, p(p^2-1)) = 1$ *für* $e > 1$.

Die Berechnung der Fixpunktanzahl der Permutationen $x \to l^{-1} \circ g_k(1, x) \circ l \bmod p^e$ und die Ermittlung der Struktur der von diesen Permutationen bei festem l gebildeten Permutationsgruppe modulo p^e scheinen mühsam und nicht leicht zu sein.

Auf ähnliche Weise wie im Falle der Dickson-Polynome $g_k(1, x)$ lassen sich auch die ganzzahligen konjugierten Ketten der Kette der Dickson-Polynome $g_k(-1, x)$ bestimmen, was aber hier nicht mehr durchgeführt werden soll.

Literatur

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

[2] H. Lausch and W. Nöbauer, *Algebra of Polynomials*, Amsterdam 1973.

[3] R. Lidl and W. Müller, *On Commutative Semigroups of Polynomials with Respect to Composition*, Mh. Math. 102 (1986), 139–153.

[4] W. Müller, *Über eine Klasse von durch Dickson-Polynome dargestellten Gruppen*, Coll. Math. Soc. Janós Bolyai 6, Keszthely 1971.

[5] W. Müller und W. Nöbauer, *Über die Fixpunkte der Potenzpermutationen*, Österr. Akad. Wiss., Sitzungsber. Math. Nat. Kl. 192 (1983), 93–97.

[6] R. Nöbauer, *Über die Fixpunkte einer Klasse von Dickson-Permutationen*, ibid. 193 (1984), 521–547.

[7] — *Über die Fixpunkte der Dickson-Permutationen*, ibid. 193 (1984), 115–133.

[8] — *Über eine Gruppe der Zahlentheorie*, Monatsh. Math. 58 (1954), 181–192.

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT KLAGENFURT
A-9022 Klagenfurt
Austria

Eingegangen am 17. 9. 1986
und in revidierter Form am 8. 12. 1986 (1672)

ACTA ARITHMETICA
LI (1988)

Inhomogeneous norm form equations over function fields

by

I. GAÁL (Debrecen)

1. Introduction. In this paper, we give effective bounds for the solutions of inhomogeneous norm form equations in several dominating variables over function fields in all cases where the solutions can be bounded by usual parameters of the function field.

The first general effective finiteness result on norm form equations in two variables over $\mathbf{Z}$, i.e. on Thue equations was obtained by Baker [1]. This famous theorem was later generalized and extended by several authors. For further references on norm form equations in several variables over number fields see e.g. Győry [7], [9].

In 1974 Sprindžuk [21] gave an inhomogeneous generalization of Baker's result. He obtained effective bounds for all solutions of the equation

$$N_{K/\mathbf{Q}}(x+\alpha y+\lambda) = m \tag{1}$$

where $K = \mathbf{Q}(\alpha)$ is an algebraic number field of degree $\geqslant 3$, $0 \neq m \in \mathbf{Z}$ and the variables are $x, y \in \mathbf{Z}$ and [1] $\lambda \in \mathbf{Z}_K$. Here λ is a non-dominating variable such that [2] $\overline{|\lambda|} < (\max(|x|, |y|))^{1-\zeta}$ ($0 < \zeta < 1$ is a given constant). In the special case $\lambda = 0$ this theorem gives the above mentioned result of Baker.

Combining the method of Sprindžuk [21] with that of Győry and Papp [10], in [5], [6], we extended Sprindžuk's theorem to the case of certain inhomogeneous norm form equations in several dominating variables over number fields.

Now let us turn to norm form equations considered over function fields. In the special case of two variables, Osgood [16], [17], Schmidt [18]–[20] Stepanov [22], Mason [11], Győry [8] and Brindza [2] gave effective bounds for the solutions of Thue equations. Győry [8] derived effective results also for the solutions of certain norm form equations in several variables.

A general effective theorem on norm form equations over function fields

---

[1] Z_K denotes the ring of integers of an algebraic number field K.

[2] $\overline{|\lambda|}$ is the size of an algebraic number λ, that is the maximum absolute value of its conjugates.