Über die Faktorisation im Restklassenring mod m.

Von B. GYIRES in Debrecen.

§ 1. Einleitung.

In einem beliebigen kommutativen Ring R nenne man jede Gleichung

$$\alpha = \xi_1 \dots \xi_{r+1} \qquad (r \geqq 0;\ \alpha, \xi_i \in R;\ i = 1, \dots, r+1) \tag{1}$$

ein Faktorisation von α. Unter den diesbezüglichen vielartigen Fragen wird uns in dieser Arbeit nur die Anzahl der Faktorisationen von α interessieren. Die Bestimmung dieser Anzahl nennen wir kurz das Faktorisationsproblem in R. Den Fall eines Körpers R lassen wir außer Acht, da dann die Faktorisation kein eigentliches Problem bietet. Wenn R den Ring der ganzen Zahlen bedeutet, so hat man es mit dem klassisch wichtigen Problem der „Factorisatio numerorum" zu tun. Hierfür genügt es offenbar nur den Fall $\alpha = p^t$ (p Primzahl) zu betrachten und dann ist die Anzahl der Faktorisationen durch die bekannte Formel

$$\binom{t+r}{t} \qquad (t, r \geqq 0) \tag{2}$$

angegeben. Diese Formel wird bei uns später zur Anwendung kommen.

Ein ebenfalls interessanter Fall entsteht, den wir im folgenden ausschließlich betrachten wollen, wenn $R = R(m)$ den Restklassenring (der ganzen Zahlen) mod m bedeutet, selbst m bezeichnet eine natürliche Zahl. Wir wollen bei festem m, α, r die Anzahl $N_r(\alpha, m)$ aller Faktorisationen (1) bestimmen.

Selbstverständlich läßt sich diese Anzahl auch elementar-zahlentheoretisch deuten, und zwar es handelt sich für eine ganze Zahl a um die Anzahl der (mod m inkongruenten) Lösungen $x_1 \dots x_{r+1}$ der Kongruenz

$$a \equiv x_1 \dots x_{r+1} \pmod{m} \quad (x_i = 1, \dots, m;\ i = 1, \dots, r+1),$$

die wir mit dem ähnlichen Symbol $N_r(a, m)$ bezeichnen. Es ist klar, daß

$$N_r(a, m) = N_r(\bar{a}, m) \tag{3}$$

gilt, wobei $\bar{a}$ die durch a representierte Restklasse mod m bezeichnet. Durch diese Formel läßt sich die Berechnung von $N_r(\alpha, m)$ und $N_r(a, m)$ aufeinander zurückführen.

Wir bemerken noch die folgende Bedeutung von $N_r(a, m)$. Man multipliziere $(1+2+\ldots+m)^{r+1}$ aus, wodurch m^{r+1} Glieder von der Form $x_1 \ldots x_{r+1}$ entstehen, die wir die Variationsprodukte $(r+1)$-ter Klasse mit Wiederholung aus den Elementen $1, 2, \ldots, m$) nennen. Unter diesen gibt es genau $N_r(a, m)$ solche, die kongruent mit $a \pmod m$ sind[1]).

Wir gewinnen die folgenden Formeln, die die Lösung unseres Problems liefern. Vor allem gilt die *„Invarianzeigenschaft"*

$$N_r(a, m) = N_r((a, m), m). \tag{4}$$

Wegen $(a, m)|m$ genügt es also nur noch den Fall $N_r(d, m)$ $(d|m)$ zu betrachten. Es gilt die *multiplikative* Eigenschaft

$$N_r(d'd'', m'm'') = N_r(d', m')\, N_r(d'', m'') \quad (d'|m';\ d''|m'';\ (m', m'') = 1), \tag{5}$$

woraus sich

$$N_r(d, m) = N_r(p_1^{t_1}, p_1^{e_1}) \ldots N_r(p_u^{t_u}, p_u^{e_u}) \tag{6}$$

ergibt. (Hier ist $m = p_1^{e_1} \ldots p_u^{e_u}$, $d = p_1^{t_1} \ldots p_u^{t_u}$ die Primpotenzzerlegung von m bzw. d.) Deshalb braucht nur noch der Fall $m = p^e$ betrachtet zu werden. Hierfür gelten

$$N_r(p^t, p^e) = \binom{t+r}{t} \varphi^r(p^e) \qquad (0 \leqq t < e), \tag{7}$$

$$N_r(p^e, p^e) = \sum_{k=0}^{r} \binom{k+e-1}{k} p^{e(r-k)} \varphi^k(p^e), \tag{8}$$

wobei φ die EULERsche Funktion bezeichnet[2]). Durch die Formel (4), (6), (7) und (8) bestimmt sich $N_r(a, m)$ in jedem Falle. Auf Grund von (4) werden wir auch folgenden Zusammenhang erhalten:

$$\sum_{a=1}^{m} N_r(a, m) = \sum_{d|m} \varphi\left(\frac{m}{d}\right) N_r(d, m) = m^{r+1}. \tag{9}$$

Dies ist (wegen $N_0(a, m) = 1$) eine Verallgemeinerung der bekannten Relation

$$\sum_{d|m} \varphi\left(\frac{m}{d}\right) = m.$$

Die Beweise von (4), (5), (7), (8) und (9) bringen wir im § 2. In § 3 untersuchen wir bei (festem m und) großen Werten von r das Verhalten der „Verteilungsfunktion" $N_r(\alpha, m)$ für α $(\in R(m))$.

§ 2. Beweise.

Dem Beweis der Formeln (4), (5), (7) und (8) schicken wir folgendes voran. Bezeichne ε das Einselement von $R(m)$. Dann sind die $a\varepsilon$ $(a = 1, \ldots, m)$ alle verschiedenen Elemente von $R(m)$. Hiervon bilden die $a\varepsilon$ mit $(a, m) = 1$

---

[1]) Ursprünglich habe ich das Problem in den obigen beiden elementaren Fassungen aufgeworfen und gelöst. Die endgültige Form der Arbeit habe ich den Herren L. RÉDEI und T. SZELE zu danken.

[2]) Insbesondere gibt also (8) die Anzahl der Faktorisationen von 0 in $R(p^e)$ an.

die Nullteiler von $R(m)$; die übrigen $\varphi(m)$ Elemente sind die Einheiten von $R(m)$, welche eine multiplikative Gruppe $R^{\times}(m)$ bilden. Ähnlich bezeichne $R^{+}(m)$ die (zyklische) additive Gruppe aller m Elemente von $R(m)$. Mit $O^{+}(\alpha)$ bezeichnen wir die additive Ordnung von α, d. h. die Ordnung von α in $R^{+}(m)$. Zwei Elemente von $R(m)$ nennen wir, wie üblich, assoziiert, wenn sie durch Multiplikation mit einer Einheit auseinander hervorgehen. Die assoziierten Elemente lassen sich offenbar auch so charakterisieren, daß sie die gleiche additive Ordnung haben. Mit anderen Worten bilden die sämtlichen Lösungen ξ von $O^{+}(\xi)=d$ $(d|m)$ bei festem d eine volle Klasse assoziierter Elemente; die Anzahl dieser Assoziierten ist gleich $\varphi(d)$.

Als abstrakter Ring läßt sich $R(m)$ so charakterisieren: $R(m)$ ist der Ring von m Elementen mit Einselement und zyklischer additiver Gruppe[3]). Nach dieser Bemerkung beweisen wir zuerst (5), wie folgt. Es gilt die Zerlegung in eine direkte Summe

$$R(m)=R(m')+R(m'').$$

Wird also allgemein

$$\xi=\xi'+\xi'' \qquad (\xi\in R(m),\ \xi'\in R(m'),\ \xi''\in R(m''))$$

gesetzt, so ist (1) offenbar äquivalent mit dem Gleichungspaar

$$\alpha^{(i)}=\xi_1^{(i)}\dots\xi_{r+1}^{(i)} \qquad (i=1,2).$$

Hieraus folgt sofort $N_r(\alpha,m)=N_r(\alpha',m')\,N_r(\alpha'',m'')$. Wendet man dies mit $\alpha=d'd''\varepsilon$, $\alpha'=d'\varepsilon'$, $\alpha''=d''\varepsilon''$ an, so entsteht wegen (3) eben (5).

Dann wollen wir (4) und (7) beweisen. Bei festem m, r (und beliebigen $\alpha, \xi_1, \dots, \xi_{r+1}$) teilen wir die sämtlichen Gleichungen (1) in Klassen ein. Zwei solche Gleichungen rechnen wir zur selben Klasse, wenn ihnen dieselbe Folge $O^{+}(\xi_1),\dots,O^{+}(\xi_{r+1})$ zugehört. Man erhält also die durch (1) repräsentierte Klasse so, daß man die ξ_i voneinander unabhängig durch alle Assoziierten ersetzt. Es ist klar, daß dabei auf der linken Seite von (1) alle Assoziierten von α gleich oft auftreten, also jede Assoziierte von α genau

$$\varphi^{-1}(O^{+}(\alpha))\prod_{i=1}^{r+1}\varphi(O^{+}(\xi_i)) \tag{10}$$

-mal. Dies hat sofort zur Folge, daß $N_r(\alpha, m)$ nur von m, r und $O^{+}(\alpha)$ abhängt[4]), und so folgt aus (3) die Richtigkeit von (4). Um auch (7) zu beweisen, wenden wir (10) für $m=p^e$, $\alpha=p^t\varepsilon$ an. Wegen $0\leqq t<e$ ist $\alpha\neq 0$, und so muß jetzt nach (1) offenbar

$$\frac{p^e}{O^{+}(\alpha)}=\prod_{i=1}^{r+1}\frac{p^e}{O^{+}(\xi_i)} \tag{11}$$

[3]) Vgl. L. Rédei und T. Szele: Algebraisch-zahlentheoretische Betrachtungen über Ringe. I. *Acta Mathematica* **79**, 291—320 (1947), Seite 292.

[4]) Das ist eine „paradoxe Erscheinung", denn es handelt sich darum, daß die Anzahl $N_r(\alpha, m)$ der multiplikativen Zerlegungen (1) von α bloß durch die additive Ordnung $O^{+}(\alpha)$ von α bestimmt ist.

gelten. Wegen $O^+(\alpha)>1$ muß auch $O^+(\xi_i)>1 \quad (i=1,\ldots,r+1)$ sein und so folgt aus (11)

$$\frac{\varphi(p^e)}{\varphi(O^+(\alpha))}=\prod_{i=1}^{r+1}\frac{\varphi(p^e)}{\varphi(O^+(\xi_i))}\,.\ ^{5})$$

Hiernach hat (10) den Wert $\varphi^r(p^e)$; dies ist also die Anzahl derjenigen Faktorisationen von α, die mit (1) zur selben Klasse gehören. Diese Anzahl hängt nicht von der betrachteten Klasse ab, und so braucht nur noch die Anzahl der (bei der Faktorisation von α) wirklich auftretenden Klassen bestimmt zu werden, selbst $N_r(\alpha,p^e)$ — das sich nach (3) auch als $N_r(p^t,p^e)$ schreiben läßt — ist dann gleich dem $\varphi^r(p^e)$-fachen der letztgenannten Anzahl. Um diese zu bestimmen, berücksichtige man, daß zum Auftreten der durch die Folge $O^+(\xi_i)$ charakterisierten Klasse die Bedingung (11) (für α) nicht nur notwendig, sondern offenbar auch hinreichend ist. Da wegen $O^+(\alpha)=O^+(p^t\varepsilon)=p^{e-t}$ die linke Seite von (11) gleich p^t ist, so ist die gesuchte Anzahl der Klassen gleich (2). Mit dem vorhergesagten zusammen haben wir (7) bestätigt.

Den Beweis von (8) können wir nur so erbringen, daß wir zunächst (9) zeigen. In dieser sind die zwei Seiten offenbar gleich, da es insgesamt m^{r+1} Produkte $\xi_1\ldots\xi_{r+1}$ in $R(m)$ gibt. Auch die Mitte von (9) ist wegen (4) der linken Seite von (9) gleich, womit wir (9) bewiesen haben.

Der Fall $m=p^e$ von (9) lautet:

$$\sum_{t=0}^{e}\varphi(p^{e-t})\,N_r(p^t,p^e)=p^{e(r+1)}$$

Zum Beweis von (8) genügt es hier (7) und (8) einzusetzen und von der so entstehenden Gleichung

$$\sum_{t=0}^{e-1}\binom{t+r}{t}\varphi(p^{e-t})\,\varphi^r(p^e)+\sum_{k=0}^{r}\binom{k+e-1}{k}p^{e(r-k)}\,\varphi^k(p^e)=p^{e(r+1)}\qquad(e\geqq 1;\ r\geqq 0)$$

ihre Richtigkeit nachzuweisen. Nach dividieren durch $p^{e(r+1)}$ und Ersetzen von e durch $s+1$ hat man:

$$\left(1-\frac{1}{p}\right)^{r+1}\sum_{t=0}^{s}\binom{t+r}{t}p^{-t}+p^{-(s+1)}\sum_{k=0}^{r}\binom{k+s}{k}\left(1-\frac{1}{p}\right)^k=1\qquad(r,s\geqq 0).$$

Da dies aus der Polynomidentität

$$(1-x)^{r+1}\sum_{t=0}^{s}\binom{t+r}{t}x^t+x^{s+1}\sum_{k=0}^{r}\binom{k+s}{k}(1-x)^k=1\qquad(r,s\geqq 0)$$

mit $x=\dfrac{1}{p}$ entsteht, so haben wir alle unsere Behauptungen bewiesen.

---

5) Es gilt nämlich $\dfrac{p^f}{p^g}=\dfrac{\varphi(p^f)}{\varphi(p^g)}$ für $f,g>0$.

§ 3. Verhalten von $N_r(\alpha, m)$ für große r.

Wir machen noch einige Bemerkungen über die Größenverhältnisse der Anzahl $N_r(\alpha, m)$. Dazu genügt es nach (3) $N_r(a, m)$ zu betrachten. Vor allem ist nach (7) und (8) klar, daß

$$(12) \qquad N_r(1, p^e) < N_r(p, p^e) < N_r(p^2, p^e) < \ldots < N_r(p^e, p^e) \qquad (e > 0)$$

gilt. (Insbesondere folgt die Richtigkeit von $N_r(p^{e-1}, p^e) < N_r(p^e, p^e)$ daraus, daß die rechte Seite von (7) im Falle $t = e-1$ ein Glied der Summe auf der rechten Seite von (8) ist.) Aus (6) und (12) ergibt sich dann unmittelbar, daß

$$N_r(1, m), \quad N_r(m, m)$$

der kleinste, bzw. der größte Wert von $N_r(a, m)$ (bei festem m und r) ist. Für das Minimum $N_r(1, m)$ gilt nach (6) und (7) einfach:

$$N_r(1, m) = \varphi^r(m).$$

Für das Maximum $N_r(m, m)$ erhält man nach (6) und (8)

$$(13) \qquad N_r(m, m) = \prod_{j=0}^{u} \sum_{k=0}^{r} \binom{e_j + k - 1}{k} p_j^{(r-k)e_j} \varphi^k(p_j^{e_j}),$$

woraus wir unten

$$(14) \qquad \lim_{r \to \infty} \frac{N_r(m, m)}{m^{r+1}} = 1$$

ableiten werden. Nach (9) folgt hieraus noch

$$(15) \qquad \lim_{r \to \infty} \frac{N_r(a, m)}{m^{r+1}} = 0 \quad \text{für} \quad m \nmid a.$$

Dabei lassen sich (14) und (15) auch folgendermaßen aussprechen: Bei festem m und für große Werte von r sind „fast alle" Variationsprodukte $x_1 \ldots x_{r+1}$ $(1 \leqq x_k \leqq m)$ durch m teilbar, oder: „fast alle" Produkte $\xi_1 \ldots \xi_{r+1}$ (in $R(m)$) sind gleich 0.

Um (14) zu beweisen, genügt es nach (6), (13) zu zeigen, daß es für eine beliebige Primzahlpotenz p^e

$$\lim_{r \to \infty} \frac{N_r(p^e, p^e)}{p^{(r+1)e}} = \lim_{r \to \infty} \frac{1}{p^{(r+1)e}} \sum_{k=0}^{r} \binom{e+k-1}{k} p^{(r-k)e} \varphi^k(p^e) =$$

$$= \lim_{r \to \infty} \frac{1}{p^e} \sum_{k=0}^{r} \binom{e+k-1}{k} \frac{\varphi^k(p^e)}{p^{ke}} = \frac{1}{p^e} \sum_{k=0}^{\infty} \binom{e+k-1}{k} \left(1 - \frac{1}{p}\right)^k = 1$$

gilt. Dies folgt aber unmittelbar $\left(\text{mit } x = 1 - \frac{1}{p}\right)$ aus folgendem Spezialfall des NEWTONschen Entwicklungssatzes:

$$\left(\frac{1}{1-z}\right)^e = \sum_{k=0}^{\infty} \binom{e+k-1}{k} x^k \qquad (|x| < 1).$$

(Eingegangen am 31. März 1949.)