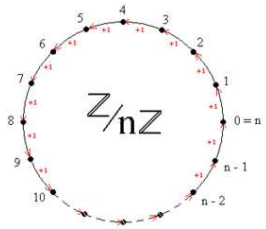
Prof. Dr. H. Brenner **Osnabrück SS 2008**

Zahlentheorie

Vorlesung 4

Die Restklassenringe $\mathbb{Z}/(n)$



SATZ 4.1. *(Einheiten modulo n) Genau dann ist $a \in \mathbb{Z}$ eine Einheit modulo n (d.h. a repräsentiert eine Einheit in $\mathbb{Z}/(n)$) wenn a und n teilerfremd sind.*

Beweis. Sind a und n teilerfremd, so gibt es nach Lemma von Bezout (Lemma 3.3) eine Darstellung der 1, es gibt also natürliche Zahlen r, s mit $ra+sn = 1$. Betrachtet man diese Gleichung modulo n, so ergibt sich $ra = 1$ in $\mathbb{Z}/(n)$. Damit ist a eine Einheit mit Inversem $a^{-1} = r$.

Ist umgekehrt a eine Einheit in $\mathbb{Z}/(n)$, so gibt es ein $r \in \mathbb{Z}/(n)$ mit $ar = 1$ in $\mathbb{Z}/(n)$. Das bedeutet aber, dass $ar - 1$ ein Vielfaches von n ist, so dass also $ar - 1 = sn$ gilt. Dann ist aber wieder $ar - sn = 1$ und a und n sind teilerfremd. □

KOROLLAR 4.2. *Der Restklassenring $\mathbb{Z}/(n)$ ist genau dann ein Körper, wenn n eine Primzahl ist.*

Beweis. Die Zahl n ist genau dann prim, wenn sie teilerfremd zu jeder Zahl a, $0 < a < n$, ist. Dies ist nach Lemma zu modularen Einheiten (Satz 4.1) genau dann der Fall, wenn in $\mathbb{Z}/(n)$ jedes von null verschiedene Element eine Einheit ist. □

Leonhard Euler (1707-1783)

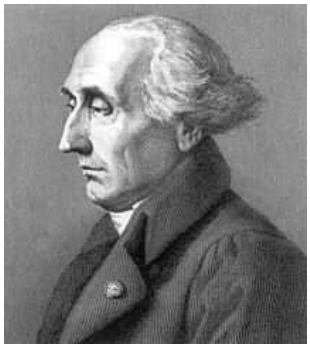
DEFINITION 4.3. Zu einer natürlichen Zahl n bezeichnet $\varphi(n)$ die Anzahl der Elemente von $(\mathbb{Z}/(n))^\times$. Man nennt $\varphi(n)$ die *Eulersche Funktion.*

BEMERKUNG 4.4. Die Eulersche Funktion $\varphi(n)$ gibt also (nach Lemma zu modularen Einheiten (Satz 4.1)) an, wie viele Zahlen r, $0 < r < n$, zu n teilerfremd sind.

SATZ 4.5. *(Euler) Sei n eine natürliche Zahl. Dann gilt für jede zu n teilerfremde Zahl a die Beziehung*

$$a^{\varphi(n)} = 1 \mod n\,.$$

Beweis. Das Element a gehört zur Einheitengruppe $(\mathbb{Z}/(n))^\times$, die $\varphi(n)$ Elemente besitzt. Nach Satz von Lagrange ist aber die Gruppenordnung ein Vielfaches der Ordnung des Elementes. □



Joseph-Louis Lagrange (1736 Turin - 1813 Paris)

Als Spezialfall erhalten wir den sogenannten kleinen Fermatschen Satz:

LEMMA 4.6. *(Kleiner Fermat) Für eine Primzahl p und eine beliebige ganze Zahl a gilt*

$$a^p \equiv a \mod p\,.$$

Anders ausgedrückt: $a^p - a$ ist durch p teilbar.

Beweis. Ist a nicht durch p teilbar, so definiert a ein Element $\bar{a}$ in der Einheitengruppe $(\mathbb{Z}/p)^\times$; diese Gruppe hat die Ordnung $\varphi(p) = p-1$, und nach Satz von Lagrange gilt $\bar{a}^{p-1} = 1$. Durch Multiplikation mit a ergibt sich die Behauptung. Für Vielfache von p gilt die Aussage ebenso, da dann beidseitig null steht. □

Pierre de Fermat (1607/08-1665)

BEISPIEL 4.7. Sei beispielsweise $p = 5$. Dann ist für

$$\begin{aligned} a = 1 &: 1^5 = 1 \mod 5 \\ a = 2 &: 2^5 = 32 = 2 \mod 5 \\ a = 3 &: 3^5 = 243 = 3 \mod 5 \\ a = 4 &: 4^5 = 1024 = 4 \mod 5\,. \end{aligned}$$

DEFINITION 4.8. Ein Körper heißt *endlich*, wenn er nur endlich viele Elemente besitzt.

SATZ 4.9. *Sei K ein endlicher Körper. Dann ist das Produkt aller von 0 verschiedener Elemente aus K gleich -1.*

Beweis. Die Gleichung $x^2 = 1$ hat in einem Körper nur die Lösungen 1 und -1, die allerdings gleich sein können. Das bedeutet, dass für $x \neq 1, -1$ immer $x \neq x^{-1}$ ist. Damit kann man das Produkt aller Einheiten schreiben als

$$1(-1)x_1x_1^{-1}\cdots x_kx_k^{-1}\,.$$

Ist $-1 \neq 1$, so ist das Produkt -1. Ist hingegen $-1 = 1$, so fehlt in dem Produkt der zweite Faktor und das Produkt ist $1 = -1$. □

KOROLLAR 4.10. *(Wilson) Sei p eine Primzahl. Dann ist*

$$(p-1)! = -1 \mod p\,.$$

Beweis. Dies folgt unmittelbar aus Satz 4.9, da ja die Fakultät durch alle Zahlen zwischen 1 und $p-1$ läuft, also durch alle Einheiten im Restklassenkörper $\mathbb{Z}/(p)$. □

Wir wollen im folgenden die Struktur der Restklassenringe $\mathbb{Z}/(n)$ verstehen, insbesondere, wenn die Primfaktorzerlegung von n bekannt ist.

LEMMA 4.11. *Seien n und k positive natürliche Zahlen, und k teile n. Dann gibt es einen kanonischen Ringhomomorphismus*

$$\mathbb{Z}/(n) \longrightarrow \mathbb{Z}/(k),\ (a \mod n) \longmapsto (a \mod k).$$

Beweis. Wir betrachten die Ringhomomorphismen

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi} & \mathbb{Z}/(k) \\ \phi\downarrow & & \\ \mathbb{Z}/(n) & & \end{array}$$

Aufgrund der Teilerbeziehung haben wir die Beziehung

$$\text{kern } \phi = (n) \subseteq (k) = \text{kern } \varphi\,.$$

Aufgrund des Homomorphisatzes hat man daher eine kanonische Abbildung von links unten nach rechts oben. □

Zur Formulierung des Chinesischen Restsatzes erinnern wir an den Begriff des Produktringes.

DEFINITION 4.12. Seien $R_1, \ldots, R_n$ kommutative Ringe. Dann heißt das Produkt

$$R_1 \times \cdots \times R_n\,,$$

versehen mit komponentenweiser Addition und Multiplikation, der *Produktring* der R_i, $i = 1, \ldots, n$.

SATZ 4.13. *(Chinesischer Restsatz) Sei n eine positive natürliche Zahl mit kanonischer Primfaktorzerlegung $n = p_1^{r_1} \cdot p_2^{r_2} \cdot \cdots \cdot p_k^{r_k}$ (die p_i seien also verschieden und $r_i \geq 1$). Dann induzieren die kanonischen Ringhomomorphismen $\mathbb{Z}/(n) \to \mathbb{Z}/(p_i^{r_i})$ einen Isomorphismus*

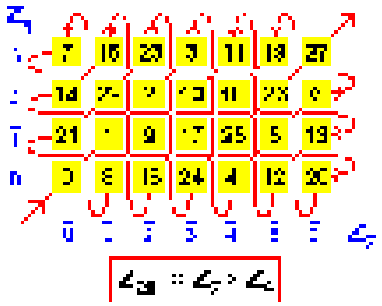
$$\mathbb{Z}/(n) \cong \mathbb{Z}/(p_1^{r_1}) \times \mathbb{Z}/(p_2^{r_2}) \times \cdots \times \mathbb{Z}/(p_k^{r_k})\,.$$

Zu einer gegebenen ganzen Zahl $(a_1, a_2, \ldots, a_k)$ gibt es also genau eine natürliche Zahl $a < n$, die die simultanen Kongruenzen

$$a = a_1 \mod p_1^{r_1},\ a = a_2 \mod p_2^{r_2},\ \ldots,\ a = a_k \mod p_k^{r_k}$$

löst.

Beweis. Da die Ringe links und rechts beide endlich sind und die gleiche Anzahl von Elementen haben, nämlich n, genügt es, die Injektivität zu zeigen. Sei x eine natürliche Zahl, die im Produktring (rechts) zu null wird, also modulo $p_i^{r_i}$ den Rest null hat für alle $i = 1, 2, \ldots, k$. Dann ist x ein Vielfaches von $p_i^{r_i}$ für alle $i = 1, 2, \ldots, k$, d.h., in der Primfaktorzerlegung von x muss p_i zumindest mit Exponent r_i vorkommen. Also muss x nach Satz 3.10 ein Vielfaches des Produktes sein muss, also ein Vielfaches von n. Damit ist $x = 0$ in $\mathbb{Z}/(n)$ und die Abbildung ist injektiv. □



Aufgabe:

(a) Bestimme für die Zahlen 3, 5 und 7 modulare Basislösungen, finde also die kleinsten positiven Zahlen, die in

$$\mathbb{Z}/(3) \times \mathbb{Z}/(5) \times \mathbb{Z}/(7)$$

die Restetupel $(1,0,0)$, $(0,1,0)$ und $(0,0,1)$ repräsentieren.

(b) Finde mit den Basislösungen die kleinste positive Lösung x der simultanen Kongruenzen

$$x = 2 \mod 3, x = 4 \mod 5 \text{ und } x = 3 \mod 7$$

Lösung:

(a) $(1,0,0)$: alle Vielfachen von $5 \cdot 7 = 35$ haben modulo 5 und modulo 7 den Rest 0. Unter diesen Vielfachen muss also die Lösung liegen. 35 hat modulo 3 den Rest 2, somit hat 70 modulo 3 den Rest 1. Also repräsentiert 70 das Restetupel $(1,0,0)$.

$(0,1,0)$: hier schaut man die Vielfachen von 21 an, und 21 hat modulo 5 den Rest 1. Also repräsentiert 21 das Restetupel $(0,1,0)$.

$(0,0,1)$: hier schaut man die Vielfachen von 15 an, und 15 hat modulo 7 den Rest 1. Also repräsentiert 15 das Restetupel $(0,0,1)$.

(b) Man schreibt (in $\mathbb{Z}/(3) \times \mathbb{Z}/(5) \times \mathbb{Z}/(7)$)

$$(2,4,3) = 2(1,0,0) + 4(0,1,0) + 3(0,0,1)\,.$$

Die Lösung ist dann

$$2 \cdot 70 + 4 \cdot 21 + 3 \cdot 15 = 140 + 84 + 45 = 269\,.$$

Die minimale Lösung ist dann $269 - 2 \cdot 105 = 59$.

Die Einheiten im Restklassenring

Wir wollen zeigen, dass die Einheitengruppe $(\mathbb{Z}/(p))^\times$, wenn p eine Primzahl ist, eine zyklische Gruppe ist, also von einem Element erzeugt wird. Der Restklassenring $\mathbb{Z}/(p)$ ist ein Körper, und wir werden hier nach einigen Vorbereitungen allgemeiner zeigen, dass jede endliche Untergruppe der

multiplikativen Gruppe eines Körpers zyklisch ist. Dazu benötigen wir einige Resultate über kommutative Gruppen und zu Polynomringen über Körpern. Wir beginnen mit zwei gruppentheoretischen Lemmata. Wir verwenden multiplikative Schreibweise.

LEMMA 4.14. *Sei G eine kommutative Gruppe und $x, y \in G$ Elemente der endlichen Ordnungen $n = \operatorname{ord}(x)$ und $m = \operatorname{ord}(y)$, wobei n und m teilerfremd seien. Dann hat xy die Ordnung nm.*

Beweis. Sei $(xy)^k = 1$. Wir haben zu zeigen, dass k ein Vielfaches von nm ist. Es ist

$$1 = (x^k y^k)^n = x^{kn} y^{kn} = y^{kn} ,$$

da ja n die Ordnung von x ist. Aus dieser Gleichung erhält man, dass kn ein Vielfaches der Ordnung von y, also von m sein muss. Da n und m teilerfremd sind, folgt aus Lemma von Euklid (Lemma 3.4), dass k ein Vielfaches von m ist. Ebenso ergibt sich, dass k ein Vielfaches von n ist, so dass k, wieder aufgrund der Teilerfremdheit, ein Vielfaches von nm sein muss. □

DEFINITION 4.15. Der *Exponent* $\exp(G)$ einer endlichen Gruppe G ist die kleinste positive Zahl n mit der Eigenschaft, dass $x^n = 1$ ist für alle $x \in G$.

LEMMA 4.16. *Sei G eine endliche kommutative Gruppe und sei $\exp(G) = \operatorname{ord}(G)$, wobei $\exp(G)$ den Exponenten der Gruppe bezeichnet. Dann ist G zyklisch.*

Beweis. Sei $n = \operatorname{ord}(G) = p_1^{r_1} \cdots p_k^{r_k}$ die Primfaktorzerlegung der Gruppenordnung. Der Exponent der Gruppe ist

$$\exp(G) = \operatorname{kgV}(\operatorname{ord}(x) : \, x \in G) .$$

Sei p_i ein Primteiler von n. Wegen $\exp(G) = \operatorname{ord}(G)$ gibt es ein Element $x \in G$, dessen Ordnung ein Vielfaches von $p_i^{r_i}$ ist. Dann gibt es auch (in der von x erzeugten zyklischen Untergruppe) ein Element x_i der Ordnung $p_i^{r_i}$. Dann hat das Produkt $x_1 \cdots x_k \in G$ nach Lemma 4.14 die Ordnung n. □

Abbildungsverzeichnis