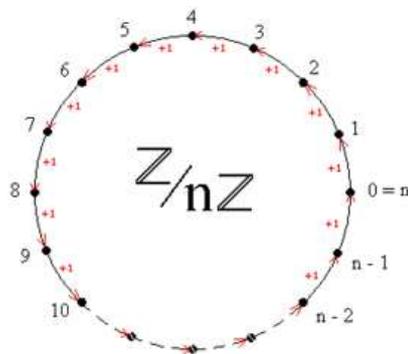


## Zahlentheorie

### Vorlesung 4

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



Für die Restklassenringe  $\mathbb{Z}/(n)$  verwenden wir  $\{0, 1, 2, \dots, n-1\}$  als kanonisches Repräsentantensystem.

**SATZ 4.1.** *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 Satz 3.3 eine Darstellung der 1, es gibt also ganze 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.  $\square$

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

*Beweis.* Dies folgt unmittelbar aus Satz 3.12.  $\square$

Wir geben noch einen zweiten Beweis.

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

## Die eulersche Phi-Funktion



Leonhard Euler (1707-1783)

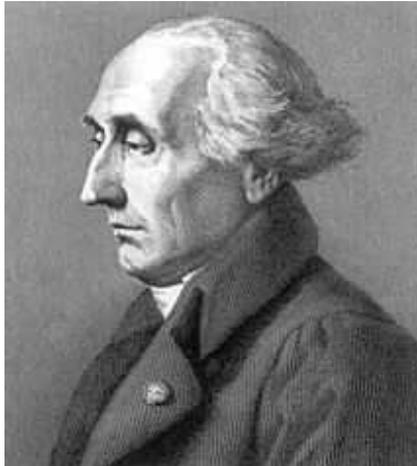
**DEFINITION 4.3.** Zu einer natürlichen Zahl  $n$  bezeichnet  $\varphi(n)$  die Anzahl der Elemente von  $(\mathbb{Z}/(n))^\times$ . Man nennt  $\varphi(n)$  die *Eulersche Funktion*.

**BEMERKUNG 4.4.** Die Eulersche Funktion  $\varphi(n)$  gibt also für  $n \geq 1$  nach Satz 4.1 an, wie viele Zahlen  $r$ ,  $0 \leq r < n$ , zu  $n$  teilerfremd sind.

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

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

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



Joseph-Louis Lagrange (1736 Turin - 1813 Paris)

Als Spezialfall erhalten wir den sogenannten kleinen Fermatschen Satz:

LEMMA 4.6. Für eine Primzahl  $p$  und eine beliebige ganze Zahl  $a$  gilt

$$a^p \equiv a \pmod{p}.$$

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 dem 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 0 steht.  $\square$



Pierre de Fermat (1607/08-1665)

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

$$a = 1 : 1^5 = 1 \pmod{5}$$

$$a = 2 : 2^5 = 32 = 2 \pmod{5}$$

$$a = 3 : 3^5 = 243 = 3 \pmod{5}$$

$$a = 4 : 4^5 = 1024 = 4 \pmod{5}.$$

### Endliche Körper und der Satz von Wilson

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 als

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

schreiben. 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  $1 = -1$ .  $\square$

Die folgende Aussage heißt *Satz von Wilson*.

KOROLLAR 4.10. Sei  $p$  eine Primzahl. Dann ist

$$(p-1)! = -1 \pmod{p}.$$

*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  $\mathbb{Z}/(p)$ .  $\square$

### Der Chinesische Restsatz

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

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

*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 Homomorphiesatzes hat man daher einen kanonischen Ringhomomorphismus von links unten nach rechts oben.  $\square$

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

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

$$R_1 \times \dots \times R_n,$$

versehen mit komponentenweiser Addition und Multiplikation, der *Produkt-ring* der  $R_i$ ,  $i = 1, \dots, n$ .

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

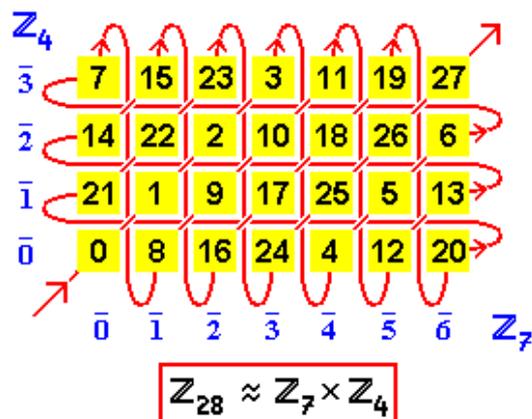
$$\mathbb{Z}/(n) \cong \mathbb{Z}/(p_1^{r_1}) \times \mathbb{Z}/(p_2^{r_2}) \times \dots \times \mathbb{Z}/(p_k^{r_k}).$$

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

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

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 0 wird, also modulo  $p_i^{r_i}$  den Rest 0 hat für alle  $i = 1, 2, \dots, k$ . Dann ist  $x$  ein Vielfaches von  $p_i^{r_i}$  für alle  $i = 1, 2, \dots, k$ , d.h. in der Primfaktorzerlegung von  $x$  muss  $p_i$  zumindest mit den Exponenten  $r_i$  vorkommen. Also muss  $x$  nach Korollar 3.10 ein Vielfaches des Produktes sein, also ein Vielfaches von  $n$ . Damit ist  $x = 0$  in  $\mathbb{Z}/(n)$  und die Abbildung ist injektiv.  $\square$



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

$$x = 2 \pmod{3}, \quad x = 4 \pmod{5} \text{ und } x = 3 \pmod{7}.$$

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

$(0, 0, 1)$ : Hier betrachtet man die Vielfachen von 15, 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 Einheitengruppe 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  $n = \text{ord}(x)$  und  $m = \text{ord}(y)$ , 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 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.  $\square$

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  $\exp(G) = \text{ord}(G)$ , wobei  $\exp(G)$  den Exponenten der Gruppe bezeichnet. Dann ist  $G$  zyklisch.*

*Beweis.* Sei

$$n = \text{ord}(G) = p_1^{r_1} \cdots p_k^{r_k}$$

die Primfaktorzerlegung der Gruppenordnung. Der Exponent der Gruppe ist

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

Sei  $p_i$  ein Primteiler von  $n$ . Wegen

$$\exp(G) = \text{ord}(G)$$

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  $n$ .  $\square$



## Abbildungsverzeichnis

Quelle = Anillo cíclico.png , Autor = Romero Schmidtke (= Benutzer FrancoGG auf es.wikipedia.org), Lizenz = CC-by-sa 3.0	1
Quelle = Leonhard Euler by Handmann .png , Autor = Emanuel Handmann (= Benutzer QWerk auf Commons), Lizenz = PD	2
Quelle = Joseph-Louis Lagrange.jpeg , Autor = Benutzer Katpatuka auf Commons, Lizenz = PD	3
Quelle = Pierre de Fermat.jpg , Autor = Benutzer Magnus Manske auf en.wikipedia.org, Lizenz = PD	3
Quelle = Tablero producto anillos cíclicos 2.png , Autor = Romero Schmidtke (= Benutzer FrancoGG auf es.wikipedia.org), Lizenz = CC-by-sa 3.0	6