Prof. Dr. H. Brenner **Osnabrück SS 2015**

Elemente der Algebra

Vorlesung 16

Der Chinesische Restsatz für $\mathbb{Z}$

Satz 16.1. *Sei n eine positive natürliche Zahl mit kanonischer Primfaktorzerlegung $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$ (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. Dies folgt unmittelbar aus Satz 15.7. □

Beweisvariante

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 $i = 1, 2, \ldots, k$. 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 Lemma 9.9 ein Vielfaches des Produktes sein muss, also ein Vielfaches von n. Damit ist $x = 0$ in $\mathbb{Z}/(n)$ und die Abbildung ist injektiv.

Unter den Basislösungen zu einer simultanen Kongruenz versteht man die kleinsten natürlichen Zahlen, die modulo den vorgegebenen Zahlen ein Restetupel ergeben, das an genau einer Stelle den Wert 1 und sonst überall den Wert 0 besizt. Aus diesen Basislösungen kann man die Lösungen zu sämtlichen simultanen Kongruenzen berechnen.

Beispiel 16.2. 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 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 $269 - 2 \cdot 105 \ = \ 59$.

KOROLLAR 16.3. *Sei n eine positive natürliche Zahl mit kanonischer Primfaktorzerlegung $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$ (die p_i seien also verschieden und $r_i \geq 1$). Dann gibt es einen kanonischen Gruppenisomorphismus*

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

Insbesondere ist eine Zahl a genau dann eine Einheit modulo n, wenn sie eine Einheit modulo $p_i^{r_i}$ ist für $i = 1, \ldots, k$.

Beweis. Dies folgt aus dem chinesischen Restsatz und Lemma 15.6. □

Die Eulersche φ-Funktion

SATZ 16.4. *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. Dies folgt aus Lemma 14.9. □

Beweisvariante

Sind a und n teilerfremd, so gibt es nach Satz 8.5 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.

Leonhard Euler (1707-1783)

DEFINITION 16.5. 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 16.6. Die Eulersche Funktion $\varphi(n)$ gibt also nach Satz 16.4 an, wie viele Zahlen r, $0 < r < n$, zu n teilerfremd sind.

Für eine Primzahl p ist $\varphi(p) = p - 1$. Eine Verallgemeinerung des *kleinen Fermat* ist der folgende Satz von Euler.

SATZ 16.7. *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 11.6 ist aber die Gruppenordnung ein Vielfaches der Ordnung des Elementes. □

Wir geben abschließend Formeln an, wie man die Eulersche φ-Funktion berechnet, wenn die Primfaktorzerlegung bekannt ist.

LEMMA 16.8. *Es sei p eine Primzahl und p^r eine Potenz davon. Dann ist*

$$\varphi(p^r) = p^{r-1}(p-1).$$

Beweis. Eine Zahl a ist genau dann teilerfremd zu einer Primzahlpotenz p^r, wenn sie teilerfremd zu p selbst ist, und dies ist genau dann der Fall, wenn sie kein Vielfaches von p ist. Unter den natürlichen Zahlen $< p^r$ sind genau die Zahlen

$$0, p, 2p, 3p, \ldots, (p^{r-1} - 1)p$$

Vielfache von p. Das sind p^{r-1} Stück, und daher gibt es

$$p^r - p^{r-1} = p^{r-1}(p-1)$$

Einheiten in $\mathbb{Z}/(p^r)$. Also ist $\varphi(p^r) = p^{r-1}(p-1)$. □

KOROLLAR 16.9. *Sei n eine positive natürliche Zahl mit kanonischer Primfaktorzerlegung $n = p_1^{r_1} \cdots p_k^{r_k}$ (die p_i seien also verschieden und $r_i \geq 1$). Dann ist*

$$\varphi(n) = \varphi(p_1^{r_1}) \cdots \varphi(p_k^{r_k}) = (p_1 - 1)p^{r_1 - 1} \cdots (p_k - 1)p^{r_k - 1}.$$

Beweis. Die erste Gleichung folgt aus Korollar 16.3 und die zweite aus Lemma 16.8. □

Abbildungsverzeichnis