Prof. Dr. H. Brenner **Osnabrück SS 2009**

Einführung in die Algebra

Vorlesung 15

Der Hauptsatz der elementaren Zahlentheorie

Wir beweisen nun, dass sich jede natürliche Zahl in eindeutiger Weise als Produkt von Primzahlen darstellen lässt.

Satz 1. *(Lemma von Euklid) Es sei p eine Primzahl und p teile ein Produkt ab von natürlichen Zahlen $a, b \in \mathbb{N}$. Dann teilt p einen der Faktoren.*

Beweis. Die Voraussetzung bedeutet, dass

$$\overline{a}\,\overline{b} = \overline{0} = 0$$

ist in $\mathbb{Z}/(p)$. Da p eine Primzahl ist, ist dieser Restklassenring nach Satz 14.13 ein Körper, so dass ein Faktor null sein muss. Sagen wir $\overline{a} = 0$. Dies bedeutet aber zurückübersetzt nach $\mathbb{Z}$, dass a ein Vielfaches von p ist. □

Satz 2. *(Der Hauptsatz der elementaren Zahlentheorie) Jede natürliche Zahl $n \in \mathbb{N}$, $n \geq 2$, besitzt eine Zerlegung in Primfaktoren.*

D.h. es gibt eine Darstellung

$$n = p_1 \cdots p_r$$

mit Primzahlen p_i. Dabei sind die Primfaktoren bis auf ihre Reihenfolge eindeutig bestimmt.

Beweis. Wir beweisen die Existenz und die Eindeutigkeit jeweils durch Induktion. Für $n = 2$ liegt eine Primzahl vor. Bei $n \geq 3$ ist entweder n eine Primzahl, und diese bildet die Primfaktorzerlegung, oder aber n ist keine Primzahl. In diesem Fall gibt es eine nichttriviale Zerlegung $n = ab$ mit kleineren Zahlen $a, b < n$. Für diese Zahlen gibt es nach der Induktionsvoraussetzung eine Zerlegung in Primfaktoren, und diese setzen sich zu einer Primfaktorzerlegung für n zusammen. Zur Existenz. Bei $n = 2$ ist die Aussage klar. Im Allgemeinen seien zwei Zerlegungen in Primfaktoren gegeben, sagen wir

$$n = p_1 \cdots p_r = q_1 \cdots q_s\,.$$

Insbesondere teilt die Primzahl p_1 dann das Produkt rechts, und damit nach Satz 15.1 einen der Faktoren. Nach Umordnung können wir annehmen, dass q_1 von p_1 geteilt wird. Da q_1 selbst eine Primzahl ist, folgt, dass $p_1 = q_1$ sein muss. Da $\mathbb{Z}$ nullteilerfrei ist, kann man beidseitig durch $p_1 = q_1$ dividieren und erhält die Gleichung

$$n' = p_2 \cdots p_r = q_2 \cdots q_s\,.$$

Da $n' < n$ ist, können wir die Induktionsvoraussetzung der Eindeutigkeit auf n' anwenden. □

Zu einer Primzahl p und einer positiven ganzen Zahl n ist der *Exponent*, also die Vielfachheit, mit der p als Primfaktor in n auftritt, eindeutich festgelegt. Dieser Exponent wird mit $\nu_p(n)$ bezeichnet. Die eindeutige Primfaktorzerlegung kann man auch als

$$n = \prod_p p^{\nu_p(n)}$$

schreiben, wobei das Produkt in Wirklichkeit endlich ist, da in der Primfaktorzerlegung nur endlich viele Primfaktoren mit einem positiven Exponenten vorkommen.

LEMMA 3. *Es seien n und k positive natürliche Zahlen. Dann wird n von k genau dann geteilt, wenn für jede Primzahl p die Beziehung*

$$\nu_p(n) \geq \nu_p(k)$$

gilt.

Beweis. (1) $\Rightarrow$ (2). Aus der Beziehung $n = kt$ folgt in Verbindung mit der eindeutigen Primfaktorzerlegung (Satz 14.2), dass die Primfaktoren von k mit mindestens ihrer Vielfachheit auch in n vorkommen müssen. (2) $\Rightarrow$ (1). Wenn die Exponentenbedingung erfüllt ist, so ist $t = \prod_p p^{\nu_p(n)-\nu_p(k)}$ eine natürliche Zahl mit $n = kt$. □

KOROLLAR 4. *Es seien n und m positive natürliche Zahlen mit den Primfaktorzerlegungen $n = \prod_p p^{\nu_p(n)}$ und $m = \prod_p p^{\nu_p(m)}$. Dann ist*

$$\mathrm{kgV}(n,m) = \prod_p p^{\max(\nu_p(n),\nu_p(m))}$$

und

$$\mathrm{ggT}(n,m) = \prod_p p^{\min(\nu_p(n),\nu_p(m))}$$

Beweis. Dies folgt direkt aus Lemma 15.3. □

Produktringe

Um die Restklassenringe von $\mathbb{Z}$ besser verstehen zu können, insbesondere dann, wenn man n als Produkt von kleineren Zahlen schreiben kann - z.B., wenn die Primfaktorzerlegung bekannt ist - , braucht man den Begriff des Produktringes.

DEFINITION 5. 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, $i = 1, \ldots, n$.

Eng verwandt mit dem Begriff des Produktringes ist das Konzept der idempotenten Elemente.

DEFINITION 6. Ein Element e eines kommutativen Ringes heißt *idempotent*, wenn $e^2 = e$ gilt.

Die Elemente 0 und 1 sind trivialerweise idempotent, man nennt sie die trivialen idempotenten Elemente. In einem Produktring sind auch diejenigen Elemente, die in allen Komponenten nur den Wert 0 oder 1 besitzen, idempotent, also bspw. $(1,0)$. In einem Integritätsbereich gibt es nur die beiden trivialen idempotenten Elemente: Ein idempotentes Element e besitzt die Eigenschaft

$$e(1-e) = e - e^2 = e - e = 0.$$

Im nullteilerfreien Fall folgt daraus $e = 1$ oder $e = 0$.

LEMMA 7. *Es sei $R = R_1 \times \cdots \times R_n$ ein Produkt aus kommutativen Ringen. Dann gilt für die Einheitengruppe von R die Beziehung*

$$R^\times = R_1^\times \times \cdots \times R_n^\times$$

Beweis. Dies ist klar, da ein Element genau dann eine Einheit ist, wenn es in jeder Komponente eine Einheit ist. □

Der Chinesische Restsatz für $\mathbb{Z}$

SATZ 8. *(Der Chinesische Restsatz) 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 $\mathbb{Z}/(n) \longrightarrow \mathbb{Z}/(p_i^{r_i})$ 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., es ist ein gemeinsames Vielfaches dieser Potenzen. Daraus folgt aufgrund von Lemma 15.3, dass x ein Vielfaches des Produktes sein muss, also ein Vielfaches von n. Damit ist $x = 0$ in $\mathbb{Z}/(n)$ und die Abbildung ist injektiv. □

Beispiel 9. 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 a der simultanen Kongruenzen

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

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 $269 - 2 \cdot 105 = 59$.

Korollar 10. *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 (Satz 15.8) und Lemma 15.7. □

Die Eulersche φ-Funktion

Satz 11. *(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 dem Lemma von Bezout (Satz 4.1) 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 12. 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 13. Die Eulersche Funktion $\varphi(n)$ gibt also (nach dem Lemma zu modularen Einheiten (Satz 15.10)) an, wie viele Zahlen r, $0 < r < n$, zu n teilerfremd sind.

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

Satz 14. *(Satz von 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 dem Satz von Lagrange (Satz 7.4 bzw. Korollar 7.5) 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 15. *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 $\leq p^r$ 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. *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 15.10 und die zweite aus Lemma 15.15. □

Abbildungsverzeichnis

Quelle = Leonhard Euler by Handmann .png, Autor = Emanuel Handmann (= Benutzer QWerk auf Commons), Lizenz = PD 5