§ 12. Polynomkongruenzen

Im folgenden sei $n \in \mathbb{N}$. Wir wollen das folgende Problem behandeln, das in der Algebra dem Lösen von polynomialen Gleichungen entspricht.

Problem: Gegeben sei ein Polynom f mit ganzzahligen Koeffizienten, d.h. $f \in \mathbb{Z}[T]$. Gesucht sind ganze Zahlen $x \in \mathbb{Z}$ mit

$$(\star) \qquad f(x) \equiv 0 \pmod{n}$$

Man nennt $(\star)$ eine **Polynomkongruenz**. Jede ganze Zahl $x_1 \in \mathbb{Z}$ mit $f(x_1) \equiv 0 \pmod{n}$ heißt eine **Lösung** von $(\star)$. Ziel ist es, Aussagen über die Existenz und Anzahl von Lösungen zu erhalten.

(12.1) LEMMA: Seien $f \in \mathbb{Z}[T]$ und $a, b \in \mathbb{Z}$. Dann gilt:

$$a \equiv b \pmod{n} \quad \Longrightarrow \quad f(a) \equiv f(b) \pmod{n}$$

Ist also $x_1 \in \mathbb{Z}$ eine Lösung von $(\star)$, so ist auch jedes Element aus der Restklasse von x_1 modulo n eine Lösung von $(\star)$, d.h. es gibt unendlich viele Lösungen. Daher wollen wir unter der Anzahl der Lösungen modulo n von $(\star)$ die Anzahl der modulo n paarweise inkongruenten Lösungen von $(\star)$ verstehen.

Lineare Kongruenzen Wir behandeln zunächst den Fall $\operatorname{grad}(f) = 1$.

(12.2) LEMMA: Sind $a \in \mathbb{Z}$ und n teilerfremd, so besitzt die lineare Kongruenz

$$(\star\star) \qquad ax \equiv b \pmod{n}$$

genau eine Lösung modulo n.

(12.3) LEMMA: Sei $g := \operatorname{ggT}(a, n)$. Genau dann ist die lineare Kongruenz

$$(\star\star) \qquad ax \equiv b \pmod{n}$$

lösbar, wenn $g \mid b$ gilt.

(12.4) SATZ: Sei $g := \operatorname{ggT}(a, n)$ und gelte $g \mid b$. Dann besitzt die lineare Kongruenz

$$(\star\star) \qquad ax \equiv b \pmod{n}$$

genau g Lösungen modulo n. Diese sind gegeben durch

$$t + k \cdot \frac{n}{g} \quad (k = 0, 1, 2, \ldots, g-1),$$

wobei t die modulo $\dfrac{n}{g}$ eindeutig bestimmte Lösung der linearen Kongruenz

$$(\star\star\star) \qquad \frac{a}{g} \cdot x \;\equiv\; \frac{b}{g} \quad \left(\operatorname{mod} \frac{n}{g}\right)$$

ist.

(12.5) SATZ: Chinesischer Restsatz

$n_1, \ldots, n_r$ $(r \geq 2)$ seien paarweise teilerfremde natürliche Zahlen und $b_1, \ldots, b_r$ seien beliebige ganze Zahlen. Dann besitzt das folgende System lineraer Kongruenzen genau eine Lösung modulo $n := n_1 \cdot n_2 \cdot \ldots \cdot n_r$:

$$(\star) \qquad \begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \qquad \vdots \\ x \equiv b_r \pmod{n_r} \end{cases}$$

Polynomkongruenzen höheren Grades

Aus einem Polynom $f = \sum_{i=0}^{m} a_i T^i \in \mathbb{Z}[T]$ mit ganzzahligen Koeffizienten wird durch Übergang zu den Restklassen modulo n ein Polynom $\overline{f} = \sum_{i=0}^{m} [a_i]_n T^i \in \mathbb{Z}_n[T]$

(12.6) LEMMA: Sei $f \in \mathbb{Z}[T]$. Dann sind für $x_1 \in \mathbb{Z}$ folgende Aussagen äquivalent:

a) x_1 ist eine Lösung der Polynomkongruenz $f(x) \equiv 0 \pmod{n}$

b) $[x_1]_n$ ist eine Nullstelle des Polynoms $\overline{f} \in \mathbb{Z}_n[T]$.

(12.7) SATZ: von Lagrange

Sei p eine Primzahl und $f \in \mathbb{Z}[T]$ ein Polynom, dessen Leitkoeffizient nicht von p geteilt wird. Dann hat die Polyomkongruenz

$$(\star) \qquad f(x) \equiv 0 \pmod{p}$$

höchstens $\operatorname{grad}(f)$ Lösungen modulo p.

(12.8) LEMMA: Sei $f = \sum_{i=0}^{m} a_i T^i \in \mathbb{Z}[T]$ ein Polynom vom Grade m, und p sei eine Primzahl. Besitzt dann die Polyomkongruenz

$$(\star) \qquad f(x) \equiv 0 \pmod{p}$$

mehr als m Lösungen modulo p, so gilt

$$p \mid a_i \quad (\forall\, i = 0, 1, \ldots, m).$$

(12.9) KOROLLAR: Sei p eine Primzahl. Dann sind alle Koeffizienten des Polynoms

$$f := (T-1) \cdot (T-2) \cdot \ldots \cdot (T-p+1) - T^{p-1} + 1 \in \mathbb{Z}[T]$$

durch p teilbar.

(12.10) KOROLLAR: **Satz von Wilson**

Für jede Primzahl p gilt $\quad (p-1)! \equiv -1 \pmod{p}$.

(12.11) SATZ: $n_1, \ldots, n_r$ $(r \geq 2)$ seien paarweise teilerfremde natürliche Zahlen und es sei $n := n_1 \cdot n_2 \cdot \ldots \cdot n_r$. Ferner sei $f \in \mathbb{Z}[T]$. Dann gilt:

a) Die Polynomkongruenz

$$(\star) \qquad f(x) \equiv 0 \pmod{n}$$

besitzt genau dann eine Lösung, wenn die Polynomkongruenzen

$$(\star\star) \qquad f(x) \equiv 0 \pmod{n_i}$$

für jedes $i = 1, 2, \ldots, r$ eine Lösung besitzen.

b) Ist $\alpha(n)$ die Anzahl der Lösungen von $(\star)$ modulo n und $\alpha(n_i)$ die Anzahl der Lösungen von $(\star\star)$ modulo n_i, so folgt

$$\alpha(n) \;=\; \alpha(n_1) \cdot \alpha(n_2) \cdot \ldots \cdot \alpha(n_r)\,.$$

(12.12) KOROLLAR: Die natürliche Zahl $n \geq 2$ besitze die kanonische Primfaktorzerlegung $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$. Dann gilt:

a) Die Polynomkongruenz

$$(\star) \qquad f(x) \equiv 0 \pmod{n}$$

besitzt genau dann eine Lösung, wenn die Polynomkongruenzen

$$(\star\star) \qquad f(x) \equiv 0 \pmod{p_i^{k_i}}$$

für jedes $i = 1, 2, \ldots, r$ eine Lösung besitzen.

b) Ist $a_i \in \mathbb{Z}$ eine Lösung von $(\star\star)$, so ist jede Zahl $a \in \mathbb{Z}$ mit $a \equiv a_i \pmod{p_i^{k_i}}$ für alle $i = 1, 2, \ldots, r$ eine Lösung von $(\star)$.

Wir wollen die spezielle Polynomkongruenz $x^m - a \equiv 0 \pmod{n}$ untersuchen.

(12.13) DEF: Seien $m, n \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$. Die Zahl a heißt m–**ter Potenzrest modulo** n, wenn die Kongruenz

$$(\star) \qquad x^m \equiv a \pmod{n}$$

lösbar ist.

Probleme: a) Wann existieren m–te Potenzreste modulo n?

b) Wie groß ist die Anzahl der m–ten Potenzreste modulo n?

c) Wie lassen sich m–te Potenzreste modulo n berechnen?

(12.14) SATZ: Seien $m, n \in \mathbb{N}$. $w \in \mathbb{Z}$ sei eine Primitivwurzel modulo n, und es sei $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$. Ferner sei $g := \mathrm{ggT}(m, \varphi(n))$. Dann sind folgende Aussagen äquivalent:

a) a ist ein m–ter Potenzrest modulo n

b) $g \mid \mathrm{ind}_w(a)$

c) $a^{\frac{\varphi(n)}{g}} \equiv 1 \pmod{n}$.

Ist eine dieser drei Bedingungen erfüllt (und damit alle), so hat die Kongruenz $(\star)$ genau g Lösungen modulo n.

(12.15) BEM: Sei $p > 2$ eine ungerade Primzahl. Da es nach (11.14) Primitivwurzeln modulo p^k $(k \in \mathbb{N})$ gibt, gilt (12.14) insbesondere für den Fall $n = p^k$.

(12.16) SATZ: $a \in \mathbb{Z}$ sei ungerade. Ferner seien $k \in \mathbb{N}$, $k \geq 3$ und $g := \mathrm{ggT}(m, 2^{k-2})$. Dann gilt für die Lösbarkeit der Kongruenz

$$(\star\star) \qquad x^m \equiv a \pmod{2^k}$$

folgendes:

a) Ist m ungerade, so ist $(\star\star)$ eindeutig lösbar.

b) Ist m gerade, so ist $(\star\star)$ genau dann lösbar, wenn gilt

i) $a \equiv 1 \pmod{4}$

ii) $a^{\frac{2^{k-2}}{g}} \equiv 1 \pmod{2^k}$.

Ist $(\star\star)$ lösbar, so ist die Anzahl der Lösungen von $(\star\star)$ modulo 2^k gleich $2 \cdot g$.

(12.17) BEM: Unter den Voraussetzungen des Satzes (12.16) gilt also:

a) Ist m ungerade, so ist jede ungerade ganze Zahl m–ter Potenzrest modulo 2^k $(k \geq 3)$.

b) Ist m gerade, so ist eine ungerade ganze Zahl a genau dann ein m–ter Potenzrest modulo 2^k, wenn die beiden Bedingungen i) und ii) erfüllt sind. Die Anzahl der Lösungen von $(\star\star)$ modulo 2^k ist dann gleich

$$2 \cdot \mathrm{ggT}(m, 2^{k-2}).$$