Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Dr. Max Pitz
WS 2017/18

Grundlagen der Mathematik

Kleiner Satz von Fermat

Theorem 1. *Für jedes $m \in \mathbb{N}$ formen die Restklassen modulo m eine $(\mathbb{N}_0/\sim_m, \odot)$ kommutative Halbgruppe mit neutralem Element $\overline{1}$. Falls $m = p$ eine Primzahl ist, so existiert zu jedem $\overline{a} \neq \overline{0}$ ein $\overline{b} \neq \overline{0}$ mit $\overline{a} \odot \overline{b} = \overline{1}$.*

Später werden wir sagen: $(\mathbb{N}_0/\sim_m, \oplus, \odot)$ ist ein Körper.

Beweis. Der erste Teil folgt sofort aus den jeweiligen Rechenregeln für $(\mathbb{N}_0, \cdot)$. Für den zweiten Teil sei nun $m = p$ eine Primzahl, und $\overline{a} \neq \overline{0}$ fest gewählt. Wir wollen zeigen, dass die $a$te Zeile in der Verknüpfungstabelle, welche aus den Elementen

$$\overline{a} \odot \overline{0},\ \overline{a} \odot \overline{1},\ \ldots,\ \overline{a} \odot \overline{p-1}$$

besteht, die *Sudoku-Eigenschaft* hat, dass also jede Restklasse genau einmal vorkommt. Denn dann kommt ja insbesondere die $\overline{1}$ an sagen wir der $b$ten Stelle vor, also $\overline{a} \odot \overline{b} = \overline{1}$ wie gewünscht. Für die Sudoku-Eigenschaft reicht es wiederum zu zeigen, dass alle Einträge verschieden sind! Denn dann haben wir p verschiedene Einträge aus der Menge $\{\overline{0}, \ldots, \overline{p-1}\}$ gefunden. also muss jeder Eintrag mindestens einmal vorkommen.

Um zu sehen, dass die Einträge wirklich verschieden sind, betrachte $0 \leq k \leq \ell \leq p-1$ mit

$$\overline{a} \odot \overline{k} = \overline{a} \odot \overline{\ell}.$$

Nach Definition bedeutet dies

$$\overline{a \cdot k} = \overline{a \cdot \ell},$$

also lassen $a \cdot k$ und $a \cdot \ell$ bei Division durch p den gleichen Rest. Es folgt

$$p | a \cdot \ell - a \cdot k = a \cdot (\ell - k).$$

Nach Euklids Lemma teilt die Primzahl p dann einen der Faktoren. Da $0 < a < p$ gilt $p \not| a$, also muss $p | \ell - k$ gelten. Da aber $0 \leq \ell - k < p$ muss nun $\ell - k = 0$, also $\ell = k$ gelten. □

Theorem 2 (Kleiner Satz von Fermat)**.** *Es sei p eine Primzahl. Für alle $a \in \mathbb{N}_0 \setminus p\mathbb{N}_0$ gilt $a^{p-1} \equiv 1 \pmod{p}$.*

Beweis. Idee: Man kommt auf diese Aussage, indem man alle von $\overline{0}$ verschiedene Element der $\overline{a}$ten Zeile der Verknüfungstabelle miteinander multiplizert.

Denn nach Theorem 1 gilt, dass in der $\overline{a}$ten Zeile der Verknüpfungstabelle jede Restklasse genau einmal vorkommt. Und da $\overline{a} \odot \overline{0} = \overline{0}$, folgt somit, dass

$$\{\overline{a} \odot \overline{1}, \overline{a} \odot \overline{2}, \ldots, \overline{a} \odot \overline{p-1}\} = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}.$$

Wenn wir jeweils das Produkt auf beiden Seiten bilden, so sehen wir, dass wir auf der linken Seite den Faktor a genau $p-1$ mal erhalten, also

$$\overline{a}^{p-1} \odot \overline{1} \odot \overline{2} \odot \cdots \odot \overline{p-1} = \overline{1} \odot \overline{2} \odot \cdots \odot \overline{p-1}.$$

Da alle $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ invertierbar sind (Theorem 1) können wir die Kürzregel für invertierbare Elemente in Halbgruppen anwenden, und erhalten

$$\overline{a}^{p-1} = \overline{1},$$

also

$$a^{p-1} \equiv 1 \pmod{p}$$

wie gewünscht. □