5.6 Satz von Fermat

Satz 94

Sei $b \in \mathbb{N}_0$ und $p \in \mathbb{N}$ eine Primzahl. Dann gilt:

$$b^p \equiv b \bmod p, \ \textit{(falls } b \not\equiv 0 \bmod p \ : \ b^{p-1} \equiv 1 \bmod p)$$

(gemeint ist: die Gleichung $b^p = b$ gilt modulo p)

Beweis:

$\mathbb{Z}_p^* := \{n \in \{1, \ldots, p-1\}; \mathrm{ggT}(n,p) = 1\}$

1. Fall: $b = 0$: $0^p = 0 \bmod p$
2. Fall: $1 \leq b < p$: Betrachte $S_b = \langle \{b^0, b^1, \ldots, b^{\mathrm{ord}(b)-1}\}, \cdot \rangle$.
   S_b ist Untergruppe von $\mathbb{Z}_p^*$.
   Lagrange: $\big(\mathrm{ord}(b) =\big)\ |S_b|\ \big||\mathbb{Z}_p^*|\big(= p-1\big)$

$$\Rightarrow (\exists q \in \mathbb{N})[q \cdot \mathrm{ord}(b)] = p - 1$$

   Da $b^{\mathrm{ord}(b)} = 1$ (Einselement) ist, gilt:

$$b^p = b^{p-1} \cdot b = b^{q \cdot \mathrm{ord}(b)} \cdot b = 1^q \cdot b = b \bmod p$$

3. Fall: $b \geq p$: Dann gilt:

$$(\exists q, r \in \mathbb{N}_0, 0 \leq r < p)[b = q \cdot p + r].$$

   Damit:

$$b^p = (q \cdot p + r)^p \overset{(*)}{=} r^p \bmod p \overset{(**)}{=} r \bmod p = b \bmod p$$

   $(*)$ Binomialentwicklung, die ersten p Summanden fallen weg, da jeweils $= 0 \bmod p$;
   $(**)$ Fall 1 bzw. 2

□

Die umgekehrte Richtung

Satz 95

Sei $n \in \mathbb{N}$, $n \geq 2$. Dann gilt:

$$b^{n-1} \equiv 1 \bmod n \text{ für alle } b \in \mathbb{Z}_n \setminus \{0\} \Longrightarrow n \text{ ist prim.}$$

Beweis:

[durch Widerspruch] Annahme: $r|n$ für ein $r \in \mathbb{N}$, $r > 1$. Dann

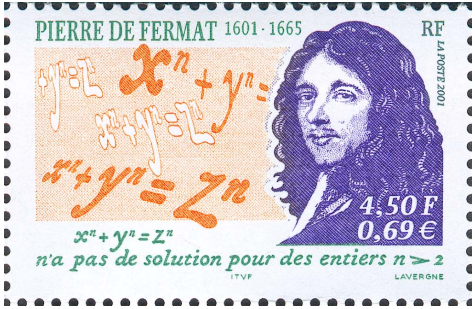
$$r^{n-1} - 1 \equiv (r \bmod n)^{n-1} - 1 \overset{\text{n. V.}}{\equiv} 0 \bmod n \ ,$$

also

$$r^{n-1} - 1 = q \cdot n = q \cdot q' \cdot r \text{ da } r|n \ .$$

Daraus folgt aber, dass $r|1$, n also keinen nichttrivialen Teiler besitzen kann. □

Pierre de Fermat (1601–1665)



Definition 96 (Eulersche phi-Funktion)

Sei $n \in \mathbb{N}$, $n > 1$. Dann bezeichnet

$$\varphi(n) := |\mathbb{Z}_n^*|$$

die Anzahl der zu n teilerfremden Reste.

Satz 97

Sei $n \in \mathbb{N}$, $n > 1$. Dann gilt in der Gruppe $\langle \mathbb{Z}_n^*, \times_n, 1 \rangle$:

$$b^{\varphi(n)} = 1 \text{ für alle } b \in \mathbb{Z}_n^* \ .$$

Beweis:

Folgt sofort aus dem Satz von Lagrange (Satz 93)! □

Leonhard Euler (1707–1783)

Leonhard Euler (1707–1783)

5.7 Zyklische Gruppen

Definition 98

Eine Gruppe $G = \langle S, \circ, 1\rangle$ heißt zyklisch, wenn es ein $b \in G$ gibt, so dass

$$G = S_b$$

wobei $S_b = \langle \{b^i | i \in \mathbb{Z}\}, \circ, 1\rangle$.

Satz 99

Sei G eine zyklische Gruppe. Falls G unendlich ist, ist G zu $\langle \mathbb{Z}, +, 0\rangle$ isomorph; falls G endlich ist, dann ist G isomorph zu $\langle \mathbb{Z}_m, +_m, 0\rangle$ für ein $m \in \mathbb{N}$.

Beweis:

1. Fall: Sei G unendlich. Wir wissen: $G = \{b^i | i \in \mathbb{Z}\}$ für ein geeignetes $b \in G$, nach Voraussetzung.
Betrachte die Abbildung

$$h : \mathbb{Z} \ni i \mapsto b^i \in G$$

Behauptung: h ist bijektiv.
Nach Voraussetzung ist h surjektiv.
Die Injektivität beweisen wir mittels Widerspruch.

Annahme: $(\exists i, j, i \neq j)[b^i = b^j]$
Daraus folgt:

$$b^{i-j} = 1$$

Daher ist G endlich, es gilt nämlich:

$$G \subseteq \{b^k; 0 \leq k < |i - j|\}$$

Dies ist ein Widerspruch zur Annahme, G sei unendlich!

Beweis (Forts.):

2. Fall: G endlich:

Wiederum ist die Abbildung h nach Voraussetzung surjektiv. Nach dem Schubfachprinzip

$$(\exists i, j, i \neq j)[b^i = b^j] \ .$$

Nach der Kürzungsregel können wir $j = 0$ wählen. Falls $i > 0$ und i minimal gewählt wird, folgt sofort

$$G \text{ isomorph } \langle \mathbb{Z}_i, +_i, 0 \rangle \ .$$

□

Satz 100

Jede Untergruppe einer zyklischen Gruppe ist wieder zyklisch.

Beweis:

Sei G zyklisch, $H \subseteq G$ Untergruppe von G.

1. Fall: $|G| = \infty$, also $G \cong \langle \mathbb{Z}, +, 0 \rangle$ ($\cong$ isomorph).

   Sei H' die durch den Isomorphismus gegebene Untergruppe von $\langle \mathbb{Z}, +, 0 \rangle$, die H entspricht.

   Zu zeigen ist: H' ist zyklisch.

   Sei $i := \min\Big\{k \in H'; k > 0\Big\}$.

   Die Behauptung ist:

   $$H' = S_i.$$

   Es gilt sicher:

   $$S_i \subseteq H'.$$

   Falls ein $k \in H' \setminus S_i$ existiert, folgt $k \bmod i \in H'$. Dies stellt einen Widerspruch zur Wahl von i dar. Also ist $H' = S_i$, damit ist gezeigt, dass H' und daher auch H zyklisch ist.

2. Fall: $|G| < \infty$: Der Beweis läuft analog.

□

5.8 Transformationsgruppen

Definition 101

Eine Transformationsgruppe ist eine Gruppe von bijektiven Abbildungen einer Menge U auf sich selbst mit der Komposition $\circ$ als binärem Operator:

$$g \circ f : U \ni x \mapsto g\big(f(x)\big) \in U$$

Satz 102 (Darstellungssatz für Gruppen)

Jede Gruppe ist isomorph zu einer Transformationsgruppe.

Beweis:
Sei $G = \langle S, \circ, 1\rangle$, $g \in G$. Betrachte die Abbildung

$$\tilde{g} : S \ni a \mapsto g \circ a \in S$$

Aus der Kürzungsregel und der Existenz eines Inversen folgt, dass $\tilde{g}$ eine bijektive Abbildung ist.
Wir betrachten nun $\tilde{G} := \langle \tilde{S}, \circ, \tilde{1}\rangle$ mit $\tilde{S} = \{\tilde{g};\ g \in G\}$. Die Abbildung

$$\tilde{}: \ S \ni g \mapsto \tilde{g} \in \tilde{S}$$

ist ein Gruppenisomorphismus. Für $h, g \in G$ gilt:

$$\widetilde{(h \circ g)}(a) = (h \circ g) \circ a = h \circ (g \circ a) = h \circ \tilde{g}(a) = \tilde{h}\big(\tilde{g}(a)\big) = \big(\tilde{h} \circ \tilde{g}\big)(a)$$

□

5.9 Permutationsgruppen

Definition 103

Eine Permutation ist eine bijektive Abbildung einer endlichen Menge auf sich selbst; o. B. d. A. sei dies die Menge $U := \{1, 2, \ldots, n\}$.
S_n (Symmetrische Gruppe für n Elemente) bezeichnet die Menge aller Permutationen auf $\{1, 2, \ldots, n\}$.

Sei nun $\pi \in S_n$. Es existiert folgende naive Darstellung:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ \pi(1) & \pi(2) & \pi(3) & \ldots & \pi(n-1) & \pi(n) \end{pmatrix}$$

Kürzer schreibt man auch

$$\pi = \begin{pmatrix} \pi(1) & \pi(2) & \pi(3) & \ldots & \pi(n-1) & \pi(n) \end{pmatrix}$$

Sei $a \in \{1, 2, 3, \ldots, n\}$. Betrachte die Folge

$$a = \pi^0(a),\ \pi^1(a),\ \pi^2(a),\ \pi^3(a),\ \ldots$$

Aus dem Schubfachprinzip und der Kürzungsregel folgt, dass es ein minimales $r = r(a)$ mit $r \leq n$ gibt, so dass $\pi^r(a) = a$. Damit bildet

$$\Big(a = \pi^0(a)\ \ \pi^1(a)\ \ \pi^2(a)\ \ \pi^3(a)\ \ \ldots\ \ \pi^{r-1}(a)\Big)$$

einen Zyklus der Permutation $\pi \in S_n$.
Umgekehrt liefert

$$\big(a\ \ \pi^1(a)\ \ \pi^2(a)\ \ \pi^3(a)\ \ \ldots\ \ \pi^{r-1}(a)\big)$$

eine zyklische Permutation der Zahlen

$$\{a,\ \pi^1(a),\ \pi^2(a),\ \pi^3(a),\ \ldots,\ \pi^{r-1}(a)\} \subseteq \{1, 2, \ldots, n\}\ .$$

Satz 104

Sei $\pi = \begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \end{pmatrix}$ *eine zyklische Permutation von* $\{1, 2, \dots, n\}$*, also*

$$\pi\colon\ a_i \mapsto a_{(i+1) \bmod n}$$

Dann gilt:

1. $\pi^k(a_i) = a_{(i+k) \bmod n}$
2. π *hat die Ordnung* n*.*

Beweis:

1. Leicht durch Induktion zu zeigen.
2. Aus 1. folgt: $\pi^n = \pi^0 = id$. Wäre $\operatorname{ord} \pi = m < n$, dann hätte der Zyklus die Form $\begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{m-1} \end{pmatrix}$ und a_m wäre gleich a_0, was einen Widerspruch zur Voraussetzung darstellt.

□

Satz 105

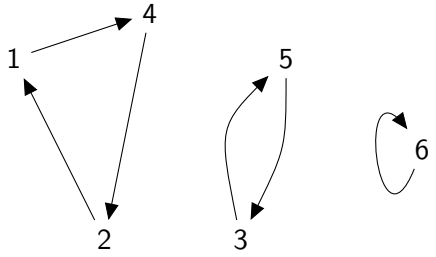
Jede Permutation aus S_n kann als Komposition (von endlich vielen) disjunkten Zyklen dargestellt werden.

Beweis:

Übung! □

Beispiel 106

$\pi = (1\ 4\ 2)(3\ 5)(6)$



In diesem Beispiel ist (6) ein Fixpunkt und $(3\ 5)$ eine Transposition (eine Permutation, die nur 2 Elemente vertauscht und alle anderen auf sich selbst abbildet).

Bemerkung:
Disjunkte Zyklen können vertauscht werden.

Korollar 107
Die Ordnung einer Permutation π ist das kgV der Längen ihrer Zyklen.