Unendlich viele Primzahlen

Satz 1: Euklid

s sein $n \in \mathbb{N}$. Die Zahl $m := n! + 1$ hat einen Primteiler, aber dieser kann nicht $\leq n$ sein, denn sonst müsste er mit $n!$ auch $1 = m - n!$ teilen. Also gibt es eine Primzahl $> n$■

Satz 2: Euler

Annahme: Es gibt nur endlich viele Primzahlen $\{p_1, \dots, p_k\}$ mit $p_1 < \dots < p_k$

Es gilt:

$$\begin{aligned}\prod_{i=1}^{k} \frac{1}{1 - p_i^{-1}} &= \prod_{i=1}^{k} \left(\sum_{i=1}^{\infty} p_i^{j_i} \right) \\ &= \sum_{j_1=0}^{\infty} \sum_{j_2=0}^{\infty} \cdots \sum_{j_k=0}^{\infty} p_1^{-j_1} \cdot p_2^{-j_2} \cdot \dots \cdot p_k^{-j_k} \\ &= \sum_{n=1}^{\infty} \frac{1}{n}\end{aligned}$$

Sylowsätze

Satz 3: Erster Sylowsatz

s seien G eine endliche Gruppe und p eine Primzahl. Dann existiert in G mindestens eine p-Sylowgruppe.

Satz 4: Zweiter Sylowsatz

s seien G eine endliche Gruppe und p eine Primzahl. Weiter sei $\#G = p^e \cdot f$ die Zerlegung von $\#G$ in eine p-Potenz und eine Zahl f, die kein Vielfaches von p ist.

Dann gelten die folgenden Aussagen:

1. Jede p-Untergruppe H von G ist in einer p-Sylowgruppe von G enthalten.
2. Je zwei p-Sylowgruppen von G sind zueinander konjugiert.
3. Die Anzahl der p-Sylowgruppen ist ein Teiler von f.
4. Die Anzahl der p-Sylowgruppen von G lässt bei Division durch p Rest 1.

Endliche Körper

Definition 1: Legendre-Symbol

Es sein $p \geq 3$ eine Primzahl. Für $a \in \mathbb{Z}$ sei

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{wenn } a \text{ quadratischer Rest modulo } p \text{ ist} \\ -1 & \text{wenn } a \text{ quadratischer Nichtrest modulo } p \text{ ist} \\ 0 & \text{wenn } a \text{ ein Vielfaches von } p \text{ ist} \end{cases}$$

- Restklassenkörper

Weiteres

In alten Klausuren begegnen uns desöfteren Ringe der Form ZZ adjungiert Wurzel aus d – in diesem Zusammenhang begegnet uns die Normabbildung. (Ein Beispiel, das in der Vorlesung gesehen wurde, waren die gauß'schen

Zahlen.) Wie können wir die Norm dafür benutzen, um Zerlegungen von Elementen zu finden oder deren Unzerlegbarkeit zu zeigen?