Unendlich viele Primzahlen

Satz 1: Euklid

Es sein $n \in \mathbb{N}$. Die Zahl $m := n! + 1$ hat einen Primteiler, aber dieser kann nicht $\leq n$ sein, denn sonst müsste er wegen $p|m$ und $p|n!$ 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:

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

Satz 3: Dirichlets Primzahlsatz

Es sei $n \in \mathbb{N}$ beliebig. Dann gibt es unendlich viele Primzahlen $p \equiv 1 \mod n$.

Sylowsätze

Satz 4: Erster Sylowsatz

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

Satz 5: Zweiter Sylowsatz

Es 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

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

Rechenregeln und Beispiele für das Legendre-Symbol

(I) Eulers Kriterium: $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \mod p$

(II) Strikt multiplikativ im Zähler: $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$

(III) $a \equiv b \mod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(IV) $\left(\frac{a}{3}\right) = a \mod 3$

(V) Quadratische Reziprozitätsgesetz: Es seinen $p \neq l$ zwei ungerade Primzahlen. Dann gilt: $\left(\frac{p}{l}\right) \cdot \left(\frac{l}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{l-1}{2}}$

(VI) Erste Ergänzung: $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{, falls } p \equiv 1 \mod 4 \\ -1 & \text{, falls } p \equiv 3 \mod 4 \end{cases}$

(VII) Zweite Ergänzung: $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{, falls } p \equiv \pm 1 \mod 8 \\ -1 & \text{, falls } p \equiv \pm 3 \mod 8 \end{cases}$

- 2 ist quadratischer Rest modulo 7, da: $2 \equiv 3^2 \mod 7$

Elementarteiler

Will man die Elementarteiler einer Matrix M berechnen, so gilt:

- e_1 ist ggT aller Matrixeinträge
- $\prod_{i=1}^{r} e_i = |\det(M)|$

Weiteres

Finden von Zerlegungen von Elementen im Ring $\mathbb{Z}[\sqrt{d}] := \left\{ a + b\sqrt{d} \;\middle|\; a, b \in \mathbb{Z} \right\}$:

$$\begin{aligned} N : \mathbb{Z}[\sqrt{d}] &\to \mathbb{N}_0 \\ N(a + b\sqrt{d}) :&= |(a + b\sqrt{d})(a - b\sqrt{d})| \\ &= |a^2 - b^2 d| \end{aligned}$$

a ist irreduzibel $\Leftrightarrow N(a)$ ist prim