1 Elementare Zahlentheorie

Eulersche φ-Funktion
Definition:

$$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$$

Multiplikativität:

$$(n,m) = 1 \implies \varphi(nm) = \varphi(n)\varphi(m)$$

Für p Primzahl gilt:

$$\varphi(p^k) = (p-1)p^{k-1}$$

Es gilt:

$$\sum_{d|m} \varphi(d) = m$$

Kleiner Fermatscher Satz

$$(a,m) = 1 \implies a^{\varphi(m)} \equiv 1 \qquad \text{mod } m$$

Primitive Wurzel
Definition a primitive Wurzel modulo p:
Die Restklassen $\overline{a}, \overline{a}^2, \ldots, \overline{a}^{p-1} = 1$ durchlaufen alle Restklassen $\neq 0$ mod p.
Satz von Gauß:
Es existieren primitive Wurzeln modulo p.
Legendre für primitive Wurzeln:
Sei a eine primitive Wurzel modulo p . Dann gilt für $r \in \mathbb{N}$

$$\left(\frac{a^r}{p}\right) = (-1)^r.$$

2 Das Quadratische Reziprozitätsgesetz

Quadratisches Reziprozitätsgesetz Es seien $p, q > 2$ Primzahlen. Dann gilt

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

1. Ergänzungssatz zum Quadratischen Reziprozitätsgesetz

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

2. Ergänzungssatz zum Quadratischen Reziprozitätsgesetz

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Primzahlen mit a Quadratischer Rest Zu jeder ganzen Zahl $a \neq 0$ existieren unendlich viele Primzahlen p , so dass a quadratischer Rest modulo p ist.

Primzahlen mit a Quadratischer Nichtrest Sei $a \in \mathbb{Z}$ kein Quadrat. Dann existieren unendlich viele Primzahlen p , so dass a quadratischer Nichtrest modulo p ist.

Norm von Primelementen in $\mathbb{Z}[i]$ Sei $\pi \in \mathbb{Z}[i]$ prim. Dann gilt entweder $N(\pi) = p^2, \pi \hat{=} p$ oder $N(\pi) = \pi\overline{\pi} = p$.

Zerlegungsgesetz in $\mathbb{Z}[i]$ Eine Primzahl p ist in $\mathbb{Z}[i]$

Produkt zweier assoziierter Primelemente	$\Leftrightarrow$	$p = 2$,
Produkt zweier nicht assoziierter Primelemente	$\Leftrightarrow$	$p \equiv 1 \mod 4$,
Primelement	$\Leftrightarrow$	$p \equiv 3 \mod 4$.

Ringe ganzer Zahlen

Ganzheit

(i) $f(b) = 0$ für ein normiertes Polynom $f \in A[X]$.

(ii) $A[b] \subset B$ ist als A-Modul endlich erzeugt.

(iii) $\exists$e.e.A-Untermodul $M \subset B$ mit $1 \in M$, $bM \subset M$.

Endlichkeit $\Longrightarrow$ Ganzheit, faktoriell $\Longrightarrow$ ganzabgeschlossen.

Diskriminante Sei $\alpha_1, \ldots, \alpha_n, n = [L : K]$ eine K-Basis von L. Dann ist die Diskriminante definiert durch $d(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Sp}(\alpha_i\alpha_j)) = (\det(\sigma_i\alpha_j)_{ij})^2$.