

2. In diesem Abschnitt sei

$$Q(x) = \sum_{1 \leq i \leq j \leq r} a_{ij} x_i x_j \quad \left(x = \begin{bmatrix} x_1 \\ \vdots \\ x_r \end{bmatrix} \right)$$

eine quadratische Form mit ganzzahligen Koeffizienten a_{ij} ; Q sei positiv, d.h. $Q(x) > 0$ für alle $x \in \mathbb{Z}^r$. Q heißt primitiv, falls der größte gemeinsame Teiler der a_{ij} ($1 \leq i \leq j \leq r$) die Zahl 1 ist.

Mit l bezeichnen wir weiterhin eine Primzahl mit $l \geq 5$; es sei

$$R = \bigcap_{p \equiv 0, -1 \pmod{l}} \mathbb{Z}_p,$$

d.h. R ist der Durchschnitt der bei p lokalisierten rationalen Zahlen \mathbb{Z}_p , wo p sämtliche Primzahlen mit der Eigenschaft $p \equiv 0$ oder $p \equiv -1 \pmod{l}$ durchläuft.

R ist ein Hauptidealring; mit R^* sei wie üblich die Gruppe der Einheiten von R bezeichnet.

Lemma 1

Ist Q primitiv, so gilt es ein $y \in \mathbb{Z}^r$,
so daß $Q(y) \in R^*$.

(Das Lemma 1 ist für $l=3$ i.A. falsch; ein Gegenbeispiel ist $Q = 2x_1^2 + 3x_2^2$.)

Beweis

Ist $Q(x)$ Form in einer Variablen, so folgt der Satz aus der Existenz von Primzahlen p mit $p \not\equiv 0, -1 \pmod{l}$. Wir nehmen daher an, daß $Q(x)$ von mehr als einer