3. Ist Q eine quadratische Form in r Variablen, ist A ein Automorphismus von Q, d.h. $A \in GL_r(\mathbb{Z})$ mit $Q(Ax) = Q(x)$ für alle $x \in \mathbb{Z}^r$, so können wir eine Form Q^A folgendermaßen definieren: sei $M = \{x \in \mathbb{Z}^r \mid Ax = x\}$; dann ist M ein freier $\mathbb{Z}$-Modul – etwa vom Rang t; sei $x_1, \ldots, x_t$ eine Basis von M, $\{x_1, \ldots, x_t\}$ die aus den Spalten $x_1, \ldots, x_t$ gebildete Matrix; wir setzen $Q^A(y) = Q(\{x_1, \ldots, x_t\} y)$ für $y \in \mathbb{Z}^t$.

Ist Q' eine weitere Form, so schreiben wir $Q' = Q^A$, falls Q' unimodular äquivalent ist zu einer der bis auf unimodulare Äquivalenz eindeutig bestimmten Formen Q^A.

Sei nun wieder Q eine positive quadratische Form in r Variablen mit ganzzahligen Koeffizienten und $d(Q) = \ell^n$ für eine Primzahl $\ell \geqq 5$. Es ist dann $e(Q) = \frac{1}{2}\{\ell^{d_1} + \ldots + \ell^{d_r}\}$ für geeignete Zahlen $d_1, \ldots, d_r$. Wir beweisen:

Lemma 3

Es gibt eine positive quadratische Form $\hat{Q}$ mit ganzzahligen Koeffizienten und einen Automorphismus A von $\hat{Q}$, dessen Ordnung eine Potenz von ℓ ist, sodaß $Q = \hat{Q}^A$ und $d(\hat{Q}) \in \bigcap_{p \not\equiv 0, -1 \bmod \ell} \mathbb{Z}_p^*$ gilt.

Dabei kann $\hat{Q}$ so gewählt werden, daß $r(\hat{Q}) = 2e(Q)$.

Beweis

Nach Lemma 3 gibt es ein $T \in GL_r\left(\bigcap_{p \not\equiv 0,-1(\ell)} \mathbb{Z}_p^*\right)$, sodaß

$$Q(x) = Q_1(Tx),$$

wo

$$Q_1(x) = \alpha_1 \ell^{d_1} x_1^2 + \ldots + \alpha_r \ell^{d_r} x_r^2 \qquad \left(x = \begin{bmatrix} x_1 \\ \vdots \\ x_r \end{bmatrix} \right)$$

für Zahlen $\alpha_1, \ldots, \alpha_r \in \bigcap_{p \not\equiv 0,-1(\ell)} \mathbb{Z}_p^*$.