Variablen abhängt.

Zunächst zeigen wir, daß man sich auf den Fall einer linearen Form beschränken kann:

Sei $y \in \mathbb{Z}^r$ mit $Q(y) \neq 0$. Da Q primitiv ist, gibt es keine Primzahl p, so daß $p \mid Q(x)$ für alle $x \in \mathbb{Z}^r$; insbesondere gibt es also zu jedem $p \mid Q(y)$ ein $y_p \in \mathbb{Z}^r$ mit $Q(y_p) \not\equiv 0 \bmod p$. Mit dem chinesischen Restsatz konstruiert man aus den y_p leicht ein $z \in \mathbb{Z}^r$, so daß $Q(z) \equiv Q(y_p) \bmod p$, d.h. $Q(z) \not\equiv 0 \bmod p$ für alle $p \mid Q(y)$. Dann ist aber $Q(my + nz)$ eine primitive binäre Form in m und n, und das Lemma würde folgen, falls es für binäre Formen bewiesen wäre.

Sei also $Q = a x_1^2 + b x_1 x_2 + c x_2^2$ eine (positive) primitive Form.

Wir haben dann

$$b^2 - 4ac = f^2 d$$

für die Diskriminante d des (imaginär) quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{b^2-4ac})$ und eine geeignete ganze Zahl $f > 0$.

Sei $\mathcal{O}_f$ die Ordnung von $\mathbb{Q}(\sqrt{d})$ mit Führer f; sei I_f die Halbgruppe der in $\mathcal{O}_f$ gelegenen vollständigen Moduln von $\mathbb{Q}(\sqrt{d})$ mit Multiplikatorenring $\mathcal{O}_f$, P_f die Halbgruppe der von 0 verschiedenen Hauptideale von $\mathcal{O}_f$. Es gibt dann bekanntlich ein $A \in I_f / P_f$, so daß für jedes $m > 0$ die Gleichung $m = Q(x)$ in $x \in \mathbb{Z}^2$ genau dann lösbar ist, wenn ein $\alpha \in A$ mit $N(\alpha) = m$ existiert (wobei $N(\alpha) = [\mathcal{O}_f : \alpha]$ gilt).

Sei I die Halbgruppe der ganzen Ideale α der Hauptordnung $\mathcal{O}$ von $\mathbb{Q}(\sqrt{d})$, die zu f teilerfremd sind,