

Gauss's method for solving $ax^2 + bxy + cy^2 = N$.

Suppose $a\alpha^2 + b\alpha\gamma + c\gamma^2 = N$, where $N \neq 0$ and $d = b^2 - 4ac > 0$ and not a perfect square. Also assume $\gcd(\alpha, \gamma) = 1$. Let $\alpha\delta - \beta\gamma = 1$. Then if

$$P = 2(a\alpha\beta + c\gamma\delta) + b(\alpha\delta + \beta\gamma),$$

we have $P^2 \equiv d \pmod{4|N|}$.

Then the unimodular transformation

$$\begin{aligned} x &= \alpha X + \beta Y \\ y &= \gamma X + \delta Y \end{aligned} \tag{1}$$

converts $ax^2 + bxy + cy^2$ to $NX^2 + PXY + \frac{(P^2-d)}{4N}Y^2$.

If we let $\beta = \beta' + t\alpha$ and $\delta = \delta' + t\beta$, we have $P = P' + 2tN$, where

$$P' = 2(a\alpha\beta' + c\gamma\delta') + b(\alpha\delta' + \beta'\gamma),$$

and there is a unique integer t such that $0 \leq P' < 2|N|$. Also $P'^2 \equiv d \pmod{4|N|}$.

If (α_1, γ_1) is an arbitrary solution with same P as (α, γ) , we have

$$\begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

where $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ corresponds to an automorphism of (a, b, c) . Dickson 111-112 shows that

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} \frac{t+bu}{2} & -cu \\ au & \frac{t-bu}{2} \end{pmatrix},$$

where $t^2 - du^2 = 4$. Hence

$$\alpha_1 = \frac{t+bu}{2}\alpha - cu\gamma, \gamma_1 = au\alpha + \frac{t-bu}{2}\gamma.$$

(Hua has an equivalent explanation which avoids the language of transformations.)

This lead to a method of determining all solutions: Test each P satisfying (2) to see if $ax^2 + bxy + cy^2$ can be converted to $NX^2 + PXY + \frac{(P^2-d)}{4N}Y^2$ using a transformation such as (1), where $\alpha\delta - \beta\gamma = 1$. Then $a\alpha^2 + b\alpha\gamma + c\gamma^2 = N$.