

Gauss's method for solving $x^2 - Dy^2 = N$.

Suppose $\alpha^2 - D\gamma^2 = N$, where $N \neq 0$ and $D > 0$ and not a perfect square. Also assume $\gcd(\alpha, \gamma) = 1$. Let $\alpha\delta - \beta\gamma = 1$. Then if $P = \alpha\beta - D\gamma\delta$, we have

- (a) $\alpha \equiv -P\gamma \pmod{|N|}$,
- (b) $P^2 - D = N(\beta^2 - D\delta^2)$.

In particular, $P^2 \equiv D \pmod{|N|}$.

Proof.

$$\begin{aligned}
 N(\beta^2 - D\delta^2) &= (\alpha^2 - D\gamma^2)(\beta^2 - D\delta^2) \\
 &= (\alpha + \sqrt{D}\gamma)(\alpha - \sqrt{D}\gamma)(\beta + \sqrt{D}\delta)(\beta - \sqrt{D}\delta) \\
 &= (\alpha + \sqrt{D}\gamma)(\beta - \sqrt{D}\delta)(\alpha - \sqrt{D}\gamma)(\beta + \sqrt{D}\delta) \\
 &= (\alpha\beta - D\gamma\delta - \sqrt{D}(\alpha\delta - \beta\gamma)) \times \\
 &\quad (\alpha\beta - D\gamma\delta + \sqrt{D}(\alpha\delta - \beta\gamma)) \\
 &= (\alpha\beta - D\gamma\delta - \sqrt{D})(\alpha\beta - D\gamma\delta + \sqrt{D}) \\
 &= (\alpha\beta - D\gamma\delta)^2 - D \\
 &= P^2 - D.
 \end{aligned}$$

Then the unimodular transformation

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

converts $x^2 - Dy^2$ to $NX^2 + 2PXY + \frac{(P^2-D)}{N}Y^2$.

There is a procedure for testing if two binary quadratic forms of the same discriminant D are equivalent. So for solubility of $x^2 - Dy^2 = N$ with $\gcd(x, y) = 1$, one has to test all P in the range $0 \leq P \leq |N|/2$.

Conversely if $P^2 \equiv D \pmod{|N|}$ and $x^2 - Dy^2$ can be converted to $NX^2 + PXY + \frac{(P^2-D)}{N}Y^2$ using a transformation such as (1), where $\alpha\delta - \beta\gamma = 1$, then

$$(a) \alpha^2 - D\gamma^2 = N,$$

$$(b) P = \alpha\beta - D\beta\delta,$$

$$(c) \alpha \equiv -P\gamma \pmod{|N|}.$$