Factorization of N

$$N = 2^k N' \qquad N' \text{ odd}$$

N' is either $\equiv 1 \pmod 4$

or $\equiv 3 \pmod 4$

1) If $N' \equiv 1 \pmod 4$

$\Delta = N'$

$$b = 2\left\lfloor \frac{\lfloor\sqrt{\Delta}\rfloor - 1}{2} \right\rfloor + 1$$

$N' \equiv 3 \pmod 4$

$\Delta = 4N'$

$$b = 2\left\lfloor \frac{\lfloor\sqrt{\Delta}\rfloor}{2} \right\rfloor$$

Define $Q(x,y) = x^2 + bxy + \left(\frac{b^2 - \Delta}{4}\right) y^2$

Define $i = 2$

2) Apply reduction operator to Q

$$Q := \rho(Q) = Ax^2 + Bxy + Cy^2$$

3) If i is odd or i is even & C is not a square then

$i := i+1$, go to 2

4) If i is even & C is a square then

Inverse square root

$$G(x,y) := -A\sqrt{C}\,x^2 - Bxy - \sqrt{C}\,y^2$$

5) $b' = b$

& $G(x,y) = \rho(G)$

If b' is still equal to b, go to step 6
else go to step 5

6) Output $|C|$ or $\frac{|C|}{2}$ (if even)

Reduction Operator

$$Q(x,y) = Ax^2 + Bxy + Cy^2 \qquad \boxed{AC \neq 0}$$

$$\rho(Q) = Cx^2 + (-B + 2nC)\,xy + (n^2C - nB + A)\,y^2$$

$n = -\left\lfloor \frac{-(\sqrt{\Delta} + B)}{2C} \right\rfloor$ $\quad$ $C < 0$

$n = \left\lfloor \frac{b + \sqrt{\Delta}}{2C} \right\rfloor$ $\quad$ $C > 0$

(properly)
→ $\wp(Q)$ is equivalent to Q.

Inverse square root operator

$$Q(x,y) = Ax^2 + Bxy + C^2xy$$

$$Q'(x,y) = -A \cdot C x^2 - Bxy - Cxy$$

Q' need not be equivalent to Q.

but $\Delta(Q') = \Delta(Q)$

$N = 11111 \equiv 3 \pmod 4$

$\Delta = 44444$

$b = 210$

1)

$Q(x, y) = x^2 + 210\,xy - 86\,y^2$

Short hand $(1, 210, -86)$

2) $(1, 210, -86) \to (-86, 134, 77)$

$\downarrow$

$(-46, 194, 37) \leftarrow (77, 174, -46)$

$\downarrow$

$(37, 176, -91) \to (-91, 188, 25)$

3) Inverse square root

$(-91, 188, 25) \to (-91.5, -188, -5)$

4) $(-91.5, -188, -5) \to (-5, 208, 59)$

$\downarrow$

$(-98, 50, 107) \leftarrow (59, 146, -98)$

$\downarrow$

$(107, 164, -41) \leftarrow$ Take c of second last form

$\downarrow$

$(-41, 164, 107)$

$11111 = 41 \times \underbrace{271}$

Apply algorithm to this again (or maybe this is already a prime?)

A visual description of this algorithm using topographs

$N>0$

$x^2 - Ny^2$

$\Delta = 4N$

Say $N = pq$

Want to find p, q

$px^2 - qy^2$

$\Delta = 4pq = 4N$

Idea is to apply a series of transformations that preserve Δ.