

Using the set up from the lectures, one easily finds that

$$\text{for } z = \frac{ax + nby}{q} \quad w = \frac{ay - bx}{q}, \text{ one has}$$

$$N/q = z^2 + nw^2.$$

Now, since $ay \equiv bx \pmod{q}$, it follows that $w \in \mathbb{Z}$. But since

$$z^2 = N/q - nw^2 \in \mathbb{Z}, \quad z \in \mathbb{Z} \text{ as well.}$$

Finally, we want to prove that $(z, w) = 1$.

Claim 3: $(z, w) = 1$.

Proof: Say $d \mid ay - bx$, and $d \mid ax + nby$. Then

$$d \mid (ay - bx) \cdot ny + (ax + nby)x = a(x^2 + ny^2) = aq$$

$$d \mid (ay - bx)x + (ax + nby)y = b(x^2 + ny^2) = bq$$

But since $(a, b) = 1$, it follows that $d \mid q$.

From this argument, we see that if $d \mid \frac{ay - bx}{q}$, $d \mid \frac{ax + nby}{q}$,

then $d = 1$, which proves the claim 3.

(b) Everything said for part (a) carries over, except for Claim 1.
Replace claim 1 by Claim 0 below and argue the same way.

Claim 0: Assume $4 \mid N = a^2 + 3b^2$, $(a, b) = 1$. Then b is odd.

Proof: Otherwise, a would be even as well, which in return would imply that $2 \mid (a, b)$; which is impossible.

(In fact, using this, now choose $(x, y) \in \{\pm 1\}$ so that $ay \equiv bx \pmod{4}$. Then z, w are again as above) \square