Subtracting the latter congruence from the former yields

$$\zeta^{-c}x_0 + \zeta^{1-c}y_0 - \zeta^{c}x_0 - \zeta^{c-1}y_0 \equiv 0 \ (p) \tag{2.2}$$

Now an element of $\mathcal{O}_K = \mathbb{Z}[\zeta]$ is divisible by p if and only if all of the coefficients as a polynomial in ζ are divisible by p. $p \nmid x_0, y_0$ since $p \nmid x_0y_0z_0$, so we must check the cases where one of $\{c, -c, 1-c, c-1\}$ is congruent to -1 modulo p or where two of $\{c, -c, 1-c, c-1\}$ are equal modulo p. These cases can be split as follows:

- $c \equiv 0 \ (p)$ (so that $c \equiv -c \ (p)$). Then $p \mid y_0(\zeta - \zeta^{-1}) = y_0(\sum_{i=2}^{p-2} \zeta^i + 1) \Rightarrow p \mid y_0$ (even if $p = 3$) $\Rightarrow$ contradiction.
- $c \equiv 1 \ (p)$ (so that $1-c \equiv c-1 \ (p)$). Then $p \mid x_0(\zeta^{-1} - \zeta) \Rightarrow p \mid x_0$ as in the previous case $\Rightarrow$ contradiction.
- $c \equiv 2^{-1} \ (p)$ (so that $c \equiv 1-c \ (p)$). Then $p \mid (y_0 - x_0)\zeta^c + \zeta^{-c}(x_0 - y_0)$. So $p \mid (x_0 - y_0)$. We then rewrite 2.1 as $x_0^p + (-z_0)^p = (-y_0)^p$ (since p is odd). Then with the same argument we will get $p \mid (x_0 + z_0)$. But 2.1 yields $x_0^p + y_0^p - z_0^p \equiv 0 \ (p)$ and so $x_0 + y_0 - z_0 \equiv 0 \ (p)$. This yields $3x_0 \equiv 0 \ (p)$. We suppose for now that $p > 3$. Then this yields $p \mid x_0 \Rightarrow$ contradiction.
- Letting one of $\{c, -c, 1-c, c-1\}$ be congruent to -1 modulo p will yield one of the coefficients of the terms of (2.2) as $\pm(x_0 - y_0)$, giving the same contradiction as in the previous case.

We therefore obtain a contradiction in all cases. We have, however, supposed that $p > 3$. A general study of the case where $p = 3$ is done elegantly in [4].

3. An Approach to Pell's Equation using cyclotomy

Pell's Equation is

$$x^2 - dy^2 = 1, \quad x, y \in \mathbb{Z}$$

in x and y, where $d \in \mathbb{Z}^+$. $d \leq 0$ trivially yields the single solution $(1, 0)$, and we can consider d to be square-free, since any square factor of d can be incorporated into y.