

Prob set 3 page 84 #56:

Let p be a prime, Then

$x^2 \equiv y^2 \pmod{p}$ if and only if
 $x \equiv y \pmod{p}$ OR
 $x \equiv -y \pmod{p}$.

(\Leftarrow) If $x \equiv y \pmod{p}$ then $x - y \equiv 0 \pmod{p}$

If $x \equiv -y \pmod{p}$ then $x + y \equiv 0 \pmod{p}$

Hence if $x \equiv y \pmod{p}$ OR $x \equiv -y \pmod{p}$

then $(x^2 - y^2) = (x - y)(x + y) \equiv 0 \pmod{p}$

We conclude that $x^2 \equiv y^2 \pmod{p}$.

(\Rightarrow) If the statement is equivalent to

° If $x^2 \equiv y^2 \pmod{p}$ and $x \not\equiv y \pmod{p}$, then
 $x \equiv -y \pmod{p}$.

Assume $x^2 \equiv y^2 \pmod{p}$ and $x \not\equiv y \pmod{p}$.

Then $p \mid x^2 - y^2 = (x - y)(x + y)$ and

$p \nmid (x - y)$.

Thus, $p \mid (x + y)$, by Theorem 2.53.

So $x \equiv -y \pmod{p}$.

Q.E.D.