

Theorem. Every prime greater than 2 is odd.

Proof. Fix a prime $p > 2$. Observe that $(p - 1)^2 \equiv 1 \pmod{p}$, since

$$\begin{aligned}(p - 1)^2 &= p^2 - 2p + 1, \\ &= p(p - 2) + 1, \\ &\equiv 0 + 1 \pmod{p}, \\ &= 1 \pmod{p}.\end{aligned}$$

That is, $|p - 1|$ divides 2, where $|p - 1|$ is the order of $p - 1$ in $(\mathbb{Z}/p\mathbb{Z})^\times$, the multiplicative group of integers modulo p . Since $p > 2$, we have that $p - 1 > 1$. Then, certainly $p - 1 \neq 1$. Thus, it cannot be the case that the order of $p - 1$ is 1, so it must be the case that $p - 1$ has order 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$. By Lagrange's Theorem, this gives us that 2 divides the order of $(\mathbb{Z}/p\mathbb{Z})^\times$. But $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$, so this implies that $p - 1$ is even. Therefore, p is odd.

□