

An interesting property of prime numbers ≥ 5 .

Theorem 1. *If $p \geq 5$ is a prime number, then $24|(p^2 - 1)$.*

Proof. First note that every prime $p \geq 5$ gives an element for the group of units $U(\mathbb{Z}/24\mathbb{Z})$. Now $U(\mathbb{Z}/24\mathbb{Z}) \simeq U(\mathbb{Z}/8\mathbb{Z}) \oplus U(\mathbb{Z}/3\mathbb{Z}) \simeq V \oplus \mathbb{Z}/2\mathbb{Z}$ where V is Klein's four group. Since $V \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $U(\mathbb{Z}/24\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Thus every element other than identity of $U(\mathbb{Z}/24\mathbb{Z})$ has order 2. That is, $p^2 \equiv 1$ in $\mathbb{Z}/24\mathbb{Z}$, or $24|(p^2 - 1)$ for every prime $p \geq 5$. \square