От малката теорема на Ферма имаме, че $a^p \equiv a \pmod p$ или еквивалентно на това (разделено почленно на a), равенството добива вида $a^{p-1} \equiv 1 \pmod p$, където a е някакво цяло число, а p е просто число и $\gcd(a, p) = 1$.

Нека d е някакво цяло число. Тогава ще имаме, че
$d^{p-1} \equiv 1 \pmod p$, което умножено почленно по $\underbrace{\left(a \pmod p\right)}_{k}$ дава

$k \times d^{p-1} \equiv k \pmod p$, което е еквивалентно на

$\underbrace{\left(a \pmod p\right) \times d^{p-2}}_{a \times d^{p-2} \pmod p} \equiv \underbrace{\left(a \pmod p\right)/d}_{\substack{\text{число по модулно деление} \\ \textbf{разделено}\text{ на друго число} \\ \text{го представихме като умножение}}}$, което искахме да докажем.