Proving RSA's correctness using Fermat's Little Theorem

Fermat's Little Theorem states that, if p is a prime, then in the group Z_n, $a^{p-1} \equiv 1$. Stated using modulo:

$$a^{p-1} \equiv 1 \pmod p$$

We aim to show that

$$M^{ed} \equiv M \pmod n$$

where $n = pq$.

Note that since $ed \equiv 1 \pmod{\phi(n)}$, $M^{ed} = M^{k\phi(n)+1}$.

Since $\phi(n) = (p-1)(q-1)$, we know that $\phi(n)$ is a multiple of $p-1$. Thus, $k\phi(n)$ is also a multiple of $p-1$. Since p is prime, and by Fermat's Little Theorem, we have the following:

$$M^{k\phi(n)+1} = M^1 \pmod p$$

By an identical argument, we have the same for q:

$$M^{k\phi(n)+1} = M^1 \pmod q$$

Thus, we know that $p \mid \left(M^{k\phi(n)+1} - M\right)$ and $q \mid \left(M^{k\phi(n)+1} - M\right)$.

Since p and q are both primes and are not equal, they are relatively prime. Note that, for a and b relatively prime, $a \mid c \wedge b \mid c \implies ab \mid c$. Therefore,

$$pq \mid \left(M^{k\phi(n)+1} - M\right)$$

which leads to $M^{k\phi(n)+1} - M^1 \equiv 0 \pmod{pq}$, and thus to our end goal:

$$M^{ed} \equiv M^{k\phi(n)+1} \equiv M \pmod n$$