Sprzedawca

$SIG' = M^e \pmod n$

Alice

1. Losuje Z takie, że $(Z, n) = 1$
2. Tworzy $Y = MZ^e \pmod n$
3. Wysyła do Banku Y
4. Bank ślepo podpisuje $V = Y^d \pmod n$ i odsyła Alice V
5. Alice wyprowadza $SIG = VZ^{-1} \pmod n$

Stąd

$$SIG = VZ^{-1}$$
$$SIG = Y^d Z^{-1}$$
$$SIG = (MZ^e)^d Z^{-1}$$
$$SIG = M^d Z^{ed} Z^{-1}$$
$$SIG = M^d Z^1 Z^{-1}$$
$$SIG = M^d \bmod (n)$$

Czy $M^d \pmod n = M^e \pmod n$ **?**