中国剩余定理（**CRT**）计算 **RSA** 解密模幂

证明. $M \equiv C^d (\bmod n)$,（$n = p \cdot q$）

$$\overset{\text{CRT}}{\Leftrightarrow} \begin{cases} M_1 \equiv C^d (\bmod p) \\ M_2 \equiv C^d (\bmod q) \end{cases} \overset{\text{Fermat}}{\Leftrightarrow} \begin{cases} M_1 \equiv C^{d (\bmod p-1)} (\bmod p) \\ M_2 \equiv C^{d (\bmod q-1)} (\bmod q) \end{cases}$$

$$\overset{\text{CRT}}{\Leftrightarrow} M = M_1 (q^{-1} (\bmod p)) \cdot q + M_2 (p^{-1} (\bmod q)) \cdot p$$

$$\Leftrightarrow M = M_2 + [((M_2 - M_1) \cdot q^{-1} (\bmod p))(\bmod p)] \cdot q$$