加法： $(a+b) \bmod p = (a \bmod p + b \bmod p) \bmod p$

減法： $(a-b) \bmod p = (a \bmod p - b \bmod p + p) \bmod p$

乗法： $(a*b) \bmod p = (a \bmod p \cdot b \bmod p) \bmod p$

次方： $(a^b) \bmod p = ((a \bmod p)^b) \bmod p$

加法結合律： $((a+b) \bmod p + c) \bmod p = (a + (b+c)) \bmod p$

乗法結合律： $((a \cdot b) \bmod p \cdot c) \bmod p = (a \cdot (b \cdot c)) \bmod p$

加法交換律： $(a+b) \bmod p = (b+a) \bmod p$

乗法交換律： $(a \cdot b) \bmod p = (b \cdot a) \bmod p$

結合律： $((a+b) \bmod p \cdot c) = ((a \cdot c) \bmod p + (b \cdot c) \bmod p) \bmod p$