Summing Dice - Solution

May 8, 2025

Recall that when you have two positive independent random variables X, Y, the distribution of their sum is given by convolution

$$P(X+Y=n) = \sum_{m=0}^{\infty} P(X=m)P(Y=n-m).$$

We can prove that this convolution operation is associative. From this it follows that addition modulo N also induces a convolution operation that is associative. Because convolution is an associative operation, we can use the fast exponentiation algorithm to calculate X convoluted with itself 2^k times. This algorithm consists of doing k convolutions, each time "squaring" the distribution. □