

Prop. *Rolling n dice of m faces yields a uniform distribution mod n if and only if n divides m .*

Proof. Suppose n divides m . Then a single dice has a uniform distribution mod n . When you add a uniform distribution on $\mathbb{Z}/n\mathbb{Z}$ to any distribution on $\mathbb{Z}/n\mathbb{Z}$ you get a uniform distribution on $\mathbb{Z}/n\mathbb{Z}$.

Conversely suppose the distribution is uniform. Observe the coefficient of x^i in the following polynomial is the number of ways you can roll i by rolling n dice with faces from 0 to $m-1$,

$$(1 + x + x^2 + \dots + x^{m-1})^n.$$

We can rewrite this polynomial as,

$$\frac{(1 - x^m)^n}{(1 - x)^n}.$$

Now substitute a primitive n^{th} root of unity ζ_n into the original polynomial. The distribution being uniform means $\zeta_n^0, \zeta_n^1, \dots, \zeta_n^{n-1}$ all have the same coefficient. But $\zeta_n^0 + \zeta_n^1 + \dots + \zeta_n^{n-1} = 0$. Therefore we must have the rewritten polynomial is also 0 when evaluated at a primitive n^{th} root of unity. But that implies $(1 - \zeta_n^m) = 0$ which implies n divides m as desired. \square