Na wykładzie udowodniliśmy, że dla każdych $x, y, z \in \mathbb{Z}_n$ mamy:

(*) $$r_n(x + y + z) = (x +_n y) +_n z.$$

Powiedziałem w czasie wykładu, że:

(**) $$r_n(x + y + z) = x +_n (y +_n z)$$

dowodzi się analogicznie jak (*) oraz że (oczywiście) (*) i (**) dają łączność $+_n$.

Pan Wojciech Bogobowicz podał szybki dowód tego jak (**) wynika z (*), który to dowód kopiuję poniżej:

$$\begin{aligned} r_n(x + y + z) &= r_n(y + z + x) \\ &= (y +_n z) +_n x \\ &= r_n((y +_n z) + x) \\ &= r_n(x + (y +_n z)) \\ &= x +_n (y +_n z). \end{aligned}$$

Druga równość wynika z (*) a trzecia i piąta z definicji $+_n$.

Bardzo się cieszę, że Pan Wojciech zauważył ten argument!
Jesli ktoś widzi tego typu usprawnienia wykładu, to proszę dawać mi znać.