Die Definition der Restklassen wird in "natürlicher Weise" auf die ganzen Zahlen zurückgeführt. Daher überträgt sich die Assoziativität und die Kommutativität sowohl für + als auch für $\bullet$. $(Z,+,\bullet)$ ist ein Ring, es gilt das Distributivgesetz $a\cdot(b+c)=a\cdot b+a\cdot c$ in $(Z,+,\bullet)$. Wegen der Homomorphie in beiden Operationen überträgt sich auch dieses auf die Restklassenstrukturen. Neutrale Elemente sind die Bilder von 0 und 1, also wieder 0 und 1 in $(Z_m,+,\bullet)$ b.z.w $\bar{0}$ *und* $\bar{1}$ *in* $(Z/_{mZ},+,\bullet)$ Zusammengefasst:

$(Z_m,+,\bullet)$ und $(Z/_{mZ},+,\bullet)$ sind untereinander isomorphe kommutative Ringe mit Einselement, die sogenannten "Restklassenringe".

*Ein **Ring ist eine algebraische Struktur** mit zwei Verknüpfungen, genannt Addition und Multiplikation, gekoppelt mit dem Distributivgesetz. Bezüglich der Addition wird eine kommutative Gruppe verlangt, bzgl. der Multiplikation reicht eine Halbgruppe. Sie braucht keine 1 zu haben und muss nicht kommutativ sein (dann werden aber beide Distributivgestze gefordert).* Die ganzen Zahlen und die Restklassenringe sind die bekanntesten Ringe.

Bemerkung: In der Schule lassen sich die Eigenschaften der Restklassenringe sehr schön an Verknüpfungstafeln erkunden.

Eigenschaften: Die (+)-Tafeln sind alle gleich aufgebaut, es entstehen immer Diagonalen mit gleichen Zahlen. Man kann bald ohne zu rechnen weiterschreiben. $(Z_m,+)$ heißt zyklische Gruppe. Die Ursache dafür ist, dass die Zahlen aus der 1 additiv entstanden sind. Ganz allgemein heißen Gruppen, die von einem Element erzeugt werden können, "zyklische Gruppen". Es ist ein Satz der Algebra, dass alle zyklischen Gruppen zu $(Z_m,+)$ oder $(Z,+)$ isomorph sind.

Interessanter sind die Mal-Tafeln. In Ringen sind Nullelemente stets anullierend, d.h. $a\cdot 0=0\ \ \forall a$. Darum lässt man bei Mal-Tafeln die 0-Zeile und die 0-Spalte weg. Dennoch kommt die 0 als Ergebnis zustande z.B. $2\cdot 3\underset{6}{\equiv}0$. Lernende finden leicht heraus, dass es solche "Nullteiler" genau dann gibt, wenn der Modul keine Primzahl ist. (2 und 3 heißen in dem Beispiel Nullteiler, weil aus z.B. aus 2*3=6 folgt, dass 2 und 3 die 6 teilen). und 6 =0 modulo 6.

Satz: $(Z_m,+,\cdot)$ ist genau dann nullteilerfrei, wenn m eine Primzahl p ist.

Folgerung Dann ist $(Z_p,+,\cdot)$ ein Körper, ein primer Restklassenkörper.

*Ein **Körper** ist ein Ring, bei dem auch die multiplikative Struktur eine Gruppe ist.*

Bew.: $"\Leftarrow"\ \ p\ \ prim\ \wedge\ a\cdot b\underset{p}{\equiv}0\Rightarrow a\cdot b=k\cdot p\ \underset{Fund.L.}{\Rightarrow}\ p\,|\,a\vee p\,|\,b$. Widerspruch. zu $0<a,b<p$

$"Nullteilerfrei\Rightarrow prim"$ Ist logisch gleichwertig mit

$"nicht\ \ prim\Rightarrow nicht\ \ Nullteilerfrei"$ Sei also $m=a\cdot b\Rightarrow 0\underset{m}{\equiv}a\cdot b$ q.e.d.

Beweis "Körper".: Es fehlt nur die Inverseneigenschaft. p sei prim. Behauptung: in jeder Zeile der Tafel kommen alle Elemente vor. [Gäbe es zwei gleiche $ab=ac\Rightarrow ab-ac=0\Rightarrow a(b-c)=0$ Nullteiler gibt es aber nicht]. Also kommt auch die 1 vor, also gibt es für jedes a ein Inverses. Die Betrachtung der Zeilen reicht wegen der Kommutativität. Rechnungen erlaubt, da Ring gesichert. (Der Beweis hätte auch über die Vielfachsummendarstellung geführt werden können, s.u.)