

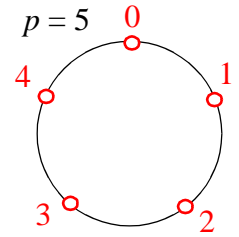
Folie 11. Der endliche Körper \mathbf{Z}_p, p prim

31.10.00 P.Vachenaue

Modell Äquidistant verteilt p Punkte auf einer Kreislinie

Anwendungen Kalenderrechnung, Kodierungstheorie, Graphentheorie

Realisierung Restklassenrechnung modulo p :



$$m \equiv n \pmod{p} \quad \text{d.h. „}m \text{ ist kongruent } n \text{ modulo } p\text{“}$$

: \Leftrightarrow m und n lassen bei der Division durch p denselben Rest

$[n]_p := \{m \in \mathbf{Z} ; m - n \text{ ist in } \mathbf{Z} \text{ durch } p \text{ teilbar}\} \subset \mathbf{Z}$ ist eine **Restklasse**

$\mathbf{Z}_p := \{[0]_p, [1]_p, [2]_p, \dots, [p-1]_p\}$ ist die **Menge der Restklassen**

salopp: \mathbf{Z}_p ist die „Menge der Reste bei der ganzzahligen Division durch p “

Arithmetik $[n]_p + [m]_p := [n + m]_p ; [n]_p \cdot [m]_p := [n \cdot m]_p$

Hierfür sind die 9 Axiome für einen Körper erfüllt:

(1) Assoziativität der Addition	$x + (y + z) = (x + y) + z$
(2) Existenz der Null	$\exists 0 \in \mathbf{Z}_p \quad \forall a \in \mathbf{Z}_p \quad a + 0 = a$
(3) Existenz des Negativen	$\forall a \in \mathbf{Z}_p \quad \exists (-a) \in \mathbf{Z}_p \quad a + (-a) = 0$
(4) Kommutativität der Addition	$x + y = y + x$
(5) Assoziativität der Multiplikation	$x \cdot (y \cdot z) = (x \cdot y) \cdot z$
(6) Existenz der Eins	$\exists 1 \in \mathbf{Z}_p \quad \forall a \in \mathbf{Z}_p \quad a \cdot 1 = a$
(7) Existenz des Inversen	$\forall a \in \mathbf{Z}_p \setminus \{0\} \quad \exists a^{-1} \in \mathbf{Z}_p \quad a \cdot a^{-1} = 1$
(8) Kommutativität der Multiplikation	$x \cdot y = y \cdot x$
(9) Distributivgesetz	$x \cdot (y + z) = x \cdot y + x \cdot z$

Der Körper \mathbf{Z}_p **kann nicht angeordnet werden**, da $1 \neq 0$ und $1 + 1 + \dots + 1 = 0$ (p mal die 1)

Beispiel $p = 5 \quad \mathbf{Z}_5 = \{0, 1, 2, 3, 4\}$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

.	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Wir haben hier zur Abkürzung einfach $n = [n]_p$ gesetzt.