Ringen und Körper

Def. 13

Ringen und Körper

Def. 13 Eine Menge $\mathbb{K}$ mit zwei Abbildungen

Ringen und Körper

Def. 13 Eine Menge $\mathbb{K}$ mit zwei Abbildungen $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ und $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$

Ringen und Körper

Def. 13 Eine Menge $\mathbb{K}$ mit zwei Abbildungen $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ und $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ (heißen Addition und Multiplikation;

Ringen und Körper

Def. 13 Eine Menge $\mathbb{K}$ mit zwei Abbildungen $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ und $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ (heißen Addition und Multiplikation; wir werden $a \cdot b$ bzw. $a + b$ statt $\cdot(a, b)$, $+(a, b)$ schreiben)

Ringen und Körper

Def. 13 Eine Menge $\mathbb{K}$ mit zwei Abbildungen $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ und $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ (heißen Addition und Multiplikation; wir werden $a \cdot b$ bzw. $a + b$ statt $\cdot(a, b)$, $+(a, b)$ schreiben) ist ein kommutativer Ring,

Ringen und Körper

Def. 13 Eine Menge $\mathbb{K}$ mit zwei Abbildungen $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ und $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ (heißen Addition und Multiplikation; wir werden $a \cdot b$ bzw. $a + b$ statt $\cdot(a, b)$, $+(a, b)$ schreiben) ist ein kommutativer Ring, falls:

Ringen und Körper

Def. 13 Eine Menge $\mathbb{K}$ mit zwei Abbildungen $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ und $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ (heißen Addition und Multiplikation; wir werden $a \cdot b$ bzw. $a + b$ statt $\cdot(a, b)$, $+(a, b)$ schreiben) ist ein kommutativer Ring, falls:

(R1) $(\mathbb{K}, +)$ ist eine abel'sche Gruppe, deren neutrales Element werden wir 0 bezeichen;

Ringen und Körper

Def. 13 Eine Menge $\mathbb{K}$ mit zwei Abbildungen $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ und $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ (heißen Addition und Multiplikation; wir werden $a \cdot b$ bzw. $a + b$ statt $\cdot(a, b)$, $+(a, b)$ schreiben) ist ein kommutativer Ring, falls:

(R1) $(\mathbb{K}, +)$ ist eine abel'sche Gruppe, deren neutrales Element werden wir 0 bezeichen;

(R2) die Multiplikation „$\cdot$“ ist assoziativ und kommutativ.

Ringen und Körper

Def. 13 Eine Menge $\mathbb{K}$ mit zwei Abbildungen $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ und $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ (heißen Addition und Multiplikation; wir werden $a \cdot b$ bzw. $a + b$ statt $\cdot(a, b)$, $+(a, b)$ schreiben) ist ein kommutativer Ring, falls:

(R1) $(\mathbb{K}, +)$ ist eine abel'sche Gruppe, deren neutrales Element werden wir 0 bezeichen;

(R2) die Multiplikation „$\cdot$“ ist assoziativ und kommutativ.

(R3) es gilt das Distributivgesetz,

Ringen und Körper

Def. 13 Eine Menge $\mathbb{K}$ mit zwei Abbildungen $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ und $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ (heißen Addition und Multiplikation; wir werden $a \cdot b$ bzw. $a + b$ statt $\cdot(a, b)$, $+(a, b)$ schreiben) ist ein kommutativer Ring, falls:

(R1) $(\mathbb{K}, +)$ ist eine abel'sche Gruppe, deren neutrales Element werden wir 0 bezeichen;

(R2) die Multiplikation „$\cdot$“ ist assoziativ und kommutativ.

(R3) es gilt das Distributivgesetz, d. h. für alle $a, b, c \in \mathbb{K}$ ist $a \cdot (b + c) = a \cdot b + a \cdot c$.

Ringen und Körper

Def. 13 Eine Menge $\mathbb{K}$ mit zwei Abbildungen $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ und $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ (heißen Addition und Multiplikation; wir werden $a \cdot b$ bzw. $a + b$ statt $\cdot(a, b)$, $+(a, b)$ schreiben) ist ein kommutativer Ring, falls:

(R1) $(\mathbb{K}, +)$ ist eine abel'sche Gruppe, deren neutrales Element werden wir 0 bezeichen;

(R2) die Multiplikation „$\cdot$“ ist assoziativ und kommutativ.

(R3) es gilt das Distributivgesetz, d. h. für alle $a, b, c \in \mathbb{K}$ ist $a \cdot (b + c) = a \cdot b + a \cdot c$.

Bsp.

Ringen und Körper

Def. 13 Eine Menge $\mathbb{K}$ mit zwei Abbildungen $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ und $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ (heißen Addition und Multiplikation; wir werden $a \cdot b$ bzw. $a + b$ statt $\cdot(a, b)$, $+(a, b)$ schreiben) ist ein kommutativer Ring, falls:

(R1) $(\mathbb{K}, +)$ ist eine abel'sche Gruppe, deren neutrales Element werden wir 0 bezeichen;

(R2) die Multiplikation „$\cdot$“ ist assoziativ und kommutativ.

(R3) es gilt das Distributivgesetz, d. h. für alle $a, b, c \in \mathbb{K}$ ist $a \cdot (b + c) = a \cdot b + a \cdot c$.

Bsp. $(\mathbb{R}, \cdot, +)$ und $(\mathbb{C}, \cdot, +)$

Ringen und Körper

Def. 13 Eine Menge $\mathbb{K}$ mit zwei Abbildungen $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ und $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ (heißen Addition und Multiplikation; wir werden $a \cdot b$ bzw. $a + b$ statt $\cdot(a, b)$, $+(a, b)$ schreiben) ist ein kommutativer Ring, falls:

(R1) $(\mathbb{K}, +)$ ist eine abel'sche Gruppe, deren neutrales Element werden wir 0 bezeichen;

(R2) die Multiplikation „$\cdot$“ ist assoziativ und kommutativ.

(R3) es gilt das Distributivgesetz, d. h. für alle $a, b, c \in \mathbb{K}$ ist $a \cdot (b + c) = a \cdot b + a \cdot c$.

Bsp. $(\mathbb{R}, \cdot, +)$ und $(\mathbb{C}, \cdot, +)$ sind kommutative Ringe.

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren.

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\mod q}{+})$

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\mod q}{+})$ ist schon eine abel'sche Gruppe,

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\mod q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$“ definieren.

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\mathrm{mod}\ q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$“ definieren. Setze
$[a] \overset{\mathrm{mod}\ q}{\cdot} [b] := [a \cdot b]$.

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\mod q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$“ definieren. Setze
$[a] \overset{\mod q}{\cdot} [b] := [a \cdot b]$.
Bsp.

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\mathrm{mod}\ q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$“ definieren. Setze

$[a] \overset{\mathrm{mod}\ q}{\cdot} [b] := [a \cdot b]$.

Bsp. $[1] \overset{\mathrm{mod}\ 5}{\cdot} [2] = [2]$,

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\mathrm{mod}\ q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$“ definieren. Setze

$[a] \overset{\mathrm{mod}\ q}{\cdot} [b] := [a \cdot b]$.

Bsp. $[1] \overset{\mathrm{mod}\ 5}{\cdot} [2] = [2]$, $[2] \overset{\mathrm{mod}\ 5}{\cdot} [3] = [6] = [1]$,

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\mathrm{mod}\ q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$“ definieren. Setze

$[a] \overset{\mathrm{mod}\ q}{\cdot} [b] := [a \cdot b]$.

Bsp. $[1] \overset{\mathrm{mod}\ 5}{\cdot} [2] = [2]$, $[2] \overset{\mathrm{mod}\ 5}{\cdot} [3] = [6] = [1]$, $[4] \overset{\mathrm{mod}\ 5}{\cdot} [3] = [12] = [2]$.

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\mathrm{mod}\ q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$“ definieren. Setze

$[a] \overset{\mathrm{mod}\ q}{\cdot} [b] := [a \cdot b]$.

Bsp. $[1] \overset{\mathrm{mod}\ 5}{\cdot} [2] = [2]$, $[2] \overset{\mathrm{mod}\ 5}{\cdot} [3] = [6] = [1]$, $[4] \overset{\mathrm{mod}\ 5}{\cdot} [3] = [12] = [2]$.

Bemerkung

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\mathrm{mod}\ q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$“ definieren. Setze

$[a] \overset{\mathrm{mod}\ q}{\cdot} [b] := [a \cdot b]$.

Bsp. $[1] \overset{\mathrm{mod}\ 5}{\cdot} [2] = [2]$, $[2] \overset{\mathrm{mod}\ 5}{\cdot} [3] = [6] = [1]$, $[4] \overset{\mathrm{mod}\ 5}{\cdot} [3] = [12] = [2]$.

Bemerkung Die Multiplikation $\overset{\mathrm{mod}\ q}{\cdot}$ ist wohldefinieret:

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\mathrm{mod}\ q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$“ definieren. Setze

$[a] \overset{\mathrm{mod}\ q}{\cdot} [b] := [a \cdot b]$.

Bsp. $[1] \overset{\mathrm{mod}\ 5}{\cdot} [2] = [2]$, $[2] \overset{\mathrm{mod}\ 5}{\cdot} [3] = [6] = [1]$, $[4] \overset{\mathrm{mod}\ 5}{\cdot} [3] = [12] = [2]$.

Bemerkung Die Multiplikation $\overset{\mathrm{mod}\ q}{\cdot}$ ist wohldefinieret: falls wir statt a und b

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\mathrm{mod}\ q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$“ definieren. Setze

$[a] \overset{\mathrm{mod}\ q}{\cdot} [b] := [a \cdot b]$.

Bsp. $[1] \overset{\mathrm{mod}\ 5}{\cdot} [2] = [2]$, $[2] \overset{\mathrm{mod}\ 5}{\cdot} [3] = [6] = [1]$, $[4] \overset{\mathrm{mod}\ 5}{\cdot} [3] = [12] = [2]$.

Bemerkung Die Multiplikation $\overset{\mathrm{mod}\ q}{\cdot}$ ist wohldefinieret: falls wir statt a und b die andere Repräsentanten des Äquivalenzklassen $[a]$ und $[b]$ nehmen,

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\mathrm{mod}\ q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$“ definieren. Setze

$[a] \overset{\mathrm{mod}\ q}{\cdot} [b] := [a \cdot b]$.

Bsp. $[1] \overset{\mathrm{mod}\ 5}{\cdot} [2] = [2]$, $[2] \overset{\mathrm{mod}\ 5}{\cdot} [3] = [6] = [1]$, $[4] \overset{\mathrm{mod}\ 5}{\cdot} [3] = [12] = [2]$.

Bemerkung Die Multiplikation $\overset{\mathrm{mod}\ q}{\cdot}$ ist wohldefinieret: falls wir statt a und b die andere Repräsentanten des Äquivalenzklassen $[a]$ und $[b]$ nehmen, wird die Ergebnis nicht geändert.

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\mathrm{mod}\ q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$“ definieren. Setze

$[a] \overset{\mathrm{mod}\ q}{\cdot} [b] := [a \cdot b]$.

Bsp. $[1] \overset{\mathrm{mod}\ 5}{\cdot} [2] = [2]$, $[2] \overset{\mathrm{mod}\ 5}{\cdot} [3] = [6] = [1]$, $[4] \overset{\mathrm{mod}\ 5}{\cdot} [3] = [12] = [2]$.

Bemerkung Die Multiplikation $\overset{\mathrm{mod}\ q}{\cdot}$ ist wohldefinieret: falls wir statt a und b die andere Repräsentanten des Äquivalenzklassen $[a]$ und $[b]$ nehmen, wird die Ergebnis nicht geändert.

Tatsächlich, $[a + k_1 \cdot q] \overset{\mathrm{mod}\ q}{\cdot} [b + k_2 \cdot q] =$

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\text{mod } q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$“ definieren. Setze

$[a] \overset{\text{mod } q}{\cdot} [b] := [a \cdot b]$.

Bsp. $[1] \overset{\text{mod } 5}{\cdot} [2] = [2]$, $[2] \overset{\text{mod } 5}{\cdot} [3] = [6] = [1]$, $[4] \overset{\text{mod } 5}{\cdot} [3] = [12] = [2]$.

Bemerkung Die Multiplikation $\overset{\text{mod } q}{\cdot}$ ist wohldefinieret: falls wir statt a und b die andere Repräsentanten des Äquivalenzklassen $[a]$ und $[b]$ nehmen, wird die Ergebnis nicht geändert.

Tatsächlich, $[a + k_1 \cdot q] \overset{\text{mod } q}{\cdot} [b + k_2 \cdot q] = [(a + k_1 \cdot q) \cdot (b + k_2 \cdot q)] =$

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\text{mod } q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$“ definieren. Setze

$[a] \overset{\text{mod } q}{\cdot} [b] := [a \cdot b]$.

Bsp. $[1] \overset{\text{mod } 5}{\cdot} [2] = [2]$, $[2] \overset{\text{mod } 5}{\cdot} [3] = [6] = [1]$, $[4] \overset{\text{mod } 5}{\cdot} [3] = [12] = [2]$.

Bemerkung Die Multiplikation $\overset{\text{mod } q}{\cdot}$ ist wohldefinieret: falls wir statt a und b die andere Repräsentanten des Äquivalenzklassen $[a]$ und $[b]$ nehmen, wird die Ergebnis nicht geändert.

Tatsächlich, $[a + k_1 \cdot q] \overset{\text{mod } q}{\cdot} [b + k_2 \cdot q] = [(a + k_1 \cdot q) \cdot (b + k_2 \cdot q)] =$

$[a \cdot b + \underbrace{(k_1 \cdot b + k_2 \cdot a + k_1 \cdot k_2 \cdot q)}_{\in \mathbb{Z}} \cdot q] =$

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\text{mod } q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$“ definieren. Setze

$[a] \overset{\text{mod } q}{\cdot} [b] := [a \cdot b]$.

Bsp. $[1] \overset{\text{mod } 5}{\cdot} [2] = [2]$, $[2] \overset{\text{mod } 5}{\cdot} [3] = [6] = [1]$, $[4] \overset{\text{mod } 5}{\cdot} [3] = [12] = [2]$.

Bemerkung Die Multiplikation $\overset{\text{mod } q}{\cdot}$ ist wohldefinieret: falls wir statt a und b die andere Repräsentanten des Äquivalenzklassen $[a]$ und $[b]$ nehmen, wird die Ergebnis nicht geändert.

Tatsächlich, $[a + k_1 \cdot q] \overset{\text{mod } q}{\cdot} [b + k_2 \cdot q] = [(a + k_1 \cdot q) \cdot (b + k_2 \cdot q)] =$
$[a \cdot b + \underbrace{(k_1 \cdot b + k_2 \cdot a + k_1 \cdot k_2 \cdot q)}_{\in \mathbb{Z}} \cdot q] = [a \cdot b]$.

(R1) folgt aus Def. 10 von $(\mathbb{Z}_p, \overset{\text{mod } q}{+})$.

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\text{mod } q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$" definieren. Setze

$[a] \overset{\text{mod } q}{\cdot} [b] := [a \cdot b]$.

Bsp. $[1] \overset{\text{mod } 5}{\cdot} [2] = [2]$, $[2] \overset{\text{mod } 5}{\cdot} [3] = [6] = [1]$, $[4] \overset{\text{mod } 5}{\cdot} [3] = [12] = [2]$.

Bemerkung Die Multiplikation $\overset{\text{mod } q}{\cdot}$ ist wohldefinieret: falls wir statt a und b die andere Repräsentanten des Äquivalenzklassen $[a]$ und $[b]$ nehmen, wird die Ergebnis nicht geändert.

Tatsächlich, $[a + k_1 \cdot q] \overset{\text{mod } q}{\cdot} [b + k_2 \cdot q] = [(a + k_1 \cdot q) \cdot (b + k_2 \cdot q)] =$
$[a \cdot b + \underbrace{(k_1 \cdot b + k_2 \cdot a + k_1 \cdot k_2 \cdot q)}_{\in \mathbb{Z}} \cdot q] = [a \cdot b]$.

(R1) folgt aus Def. 10 von $(\mathbb{Z}_p, \overset{\text{mod } q}{+})$.
(R2) ist wie in Satz 15

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\text{mod } q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$" definieren. Setze

$[a] \overset{\text{mod } q}{\cdot} [b] := [a \cdot b]$.

Bsp. $[1] \overset{\text{mod } 5}{\cdot} [2] = [2]$, $[2] \overset{\text{mod } 5}{\cdot} [3] = [6] = [1]$, $[4] \overset{\text{mod } 5}{\cdot} [3] = [12] = [2]$.

Bemerkung Die Multiplikation $\overset{\text{mod } q}{\cdot}$ ist wohldefinieret: falls wir statt a und b die andere Repräsentanten des Äquivalenzklassen $[a]$ und $[b]$ nehmen, wird die Ergebnis nicht geändert.

Tatsächlich, $[a + k_1 \cdot q] \overset{\text{mod } q}{\cdot} [b + k_2 \cdot q] = [(a + k_1 \cdot q) \cdot (b + k_2 \cdot q)] =$
$[a \cdot b + \underbrace{(k_1 \cdot b + k_2 \cdot a + k_1 \cdot k_2 \cdot q)}_{\in \mathbb{Z}} \cdot q] = [a \cdot b]$.

(R1) folgt aus Def. 10 von $(\mathbb{Z}_p, \overset{\text{mod } q}{+})$.
(R2) ist wie in Satz 15

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\text{mod } q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$“ definieren. Setze

$[a] \overset{\text{mod } q}{\cdot} [b] := [a \cdot b]$.

Bsp. $[1] \overset{\text{mod } 5}{\cdot} [2] = [2]$, $[2] \overset{\text{mod } 5}{\cdot} [3] = [6] = [1]$, $[4] \overset{\text{mod } 5}{\cdot} [3] = [12] = [2]$.

Bemerkung Die Multiplikation $\overset{\text{mod } q}{\cdot}$ ist wohldefinieret: falls wir statt a und b die andere Repräsentanten des Äquivalenzklassen $[a]$ und $[b]$ nehmen, wird die Ergebnis nicht geändert.

Tatsächlich, $[a + k_1 \cdot q] \overset{\text{mod } q}{\cdot} [b + k_2 \cdot q] = [(a + k_1 \cdot q) \cdot (b + k_2 \cdot q)] =$
$[a \cdot b + \underbrace{(k_1 \cdot b + k_2 \cdot a + k_1 \cdot k_2 \cdot q)}_{\in \mathbb{Z}} \cdot q] = [a \cdot b]$.

(R1) folgt aus Def. 10 von $(\mathbb{Z}_p, \overset{\text{mod } q}{+})$.
(R2) ist wie in Satz 15
(R3) $[a] \overset{\text{mod } q}{\cdot} ([b] \overset{\text{mod } q}{+} [c]) =$

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\text{mod } q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$“ definieren. Setze

$[a] \overset{\text{mod } q}{\cdot} [b] := [a \cdot b]$.

Bsp. $[1] \overset{\text{mod } 5}{\cdot} [2] = [2]$, $[2] \overset{\text{mod } 5}{\cdot} [3] = [6] = [1]$, $[4] \overset{\text{mod } 5}{\cdot} [3] = [12] = [2]$.

Bemerkung Die Multiplikation $\overset{\text{mod } q}{\cdot}$ ist wohldefinieret: falls wir statt a und b die andere Repräsentanten des Äquivalenzklassen $[a]$ und $[b]$ nehmen, wird die Ergebnis nicht geändert.

Tatsächlich, $[a + k_1 \cdot q] \overset{\text{mod } q}{\cdot} [b + k_2 \cdot q] = [(a + k_1 \cdot q) \cdot (b + k_2 \cdot q)] =$
$[a \cdot b + \underbrace{(k_1 \cdot b + k_2 \cdot a + k_1 \cdot k_2 \cdot q)}_{\in \mathbb{Z}} \cdot q] = [a \cdot b]$.

(R1) folgt aus Def. 10 von $(\mathbb{Z}_p, \overset{\text{mod } q}{+})$.

(R2) ist wie in Satz 15

(R3) $[a] \overset{\text{mod } q}{\cdot} ([b] \overset{\text{mod } q}{+} [c]) = [a \cdot (b + c)] =$

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\text{mod } q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$“ definieren. Setze

$[a] \overset{\text{mod } q}{\cdot} [b] := [a \cdot b]$.

Bsp. $[1] \overset{\text{mod } 5}{\cdot} [2] = [2]$, $[2] \overset{\text{mod } 5}{\cdot} [3] = [6] = [1]$, $[4] \overset{\text{mod } 5}{\cdot} [3] = [12] = [2]$.

Bemerkung Die Multiplikation $\overset{\text{mod } q}{\cdot}$ ist wohldefinieret: falls wir statt a und b die andere Repräsentanten des Äquivalenzklassen $[a]$ und $[b]$ nehmen, wird die Ergebnis nicht geändert.

Tatsächlich, $[a + k_1 \cdot q] \overset{\text{mod } q}{\cdot} [b + k_2 \cdot q] = [(a + k_1 \cdot q) \cdot (b + k_2 \cdot q)] =$
$[a \cdot b + \underbrace{(k_1 \cdot b + k_2 \cdot a + k_1 \cdot k_2 \cdot q)}_{\in \mathbb{Z}} \cdot q] = [a \cdot b]$.

(R1) folgt aus Def. 10 von $(\mathbb{Z}_p, \overset{\text{mod } q}{+})$.
(R2) ist wie in Satz 15
(R3) $[a] \overset{\text{mod } q}{\cdot} ([b] \overset{\text{mod } q}{+} [c]) = [a \cdot (b + c)] = [a \cdot b + a \cdot c] =$

$\mathbb{Z}_q$ ist ein kommutativer Ring

Wir werden auf $\mathbb{Z}_q$ ein Struktur des Rings definieren. $(\mathbb{Z}, \overset{\text{mod } q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$“ definieren. Setze
$[a] \overset{\text{mod } q}{\cdot} [b] := [a \cdot b]$.

Bsp. $[1] \overset{\text{mod } 5}{\cdot} [2] = [2]$, $[2] \overset{\text{mod } 5}{\cdot} [3] = [6] = [1]$, $[4] \overset{\text{mod } 5}{\cdot} [3] = [12] = [2]$.

Bemerkung Die Multiplikation $\overset{\text{mod } q}{\cdot}$ ist wohldefinieret: falls wir statt a und b die andere Repräsentanten des Äquivalenzklassen $[a]$ und $[b]$ nehmen, wird die Ergebnis nicht geändert.

Tatsächlich, $[a + k_1 \cdot q] \overset{\text{mod } q}{\cdot} [b + k_2 \cdot q] = [(a + k_1 \cdot q) \cdot (b + k_2 \cdot q)] =$
$[a \cdot b + \underbrace{(k_1 \cdot b + k_2 \cdot a + k_1 \cdot k_2 \cdot q)}_{\in \mathbb{Z}} \cdot q] = [a \cdot b]$.

(R1) folgt aus Def. 10 von $(\mathbb{Z}_p, \overset{\text{mod } q}{+})$.
(R2) ist wie in Satz 15
(R3) $[a] \overset{\text{mod } q}{\cdot} ([b] \overset{\text{mod } q}{+} [c]) = [a \cdot (b + c)] = [a \cdot b + a \cdot c] =$
$[a] \overset{\text{mod } q}{\cdot} [b] \overset{\text{mod } q}{+} [a] \overset{\text{mod } q}{\cdot} [c]$.

Anwendung: Teilbarkeitregeln in Dezimalsystem

Anwendung: Teilbarkeitregeln in Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.

Anwendung: Teilbarkeitregeln in Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl

.

Anwendung: Teilbarkeitregeln in Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl $\alpha_n \cdot 10^n + ... + \alpha_0$.

.

Anwendung: Teilbarkeitregeln in Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl $\alpha_n \cdot 10^n + ... + \alpha_0$.
(Bsp. 237).

.

Anwendung: Teilbarkeitregeln in Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl $\alpha_n \cdot 10^n + ... + \alpha_0$.
(Bsp. $237 = 2 \cdot 100 + 3 \cdot 10 + 7$).

.

Anwendung: Teilbarkeitregeln in Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl $\alpha_n \cdot 10^n + ... + \alpha_0$.
(Bsp. $237 = 2 \cdot 100 + 3 \cdot 10 + 7$).
Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 2?$

Anwendung: Teilbarkeitregeln in Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl $\alpha_n \cdot 10^n + ... + \alpha_0$.
(Bsp. $237 = 2 \cdot 100 + 3 \cdot 10 + 7$).
Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 2?$
Frage umformulieren:

.

Anwendung: Teilbarkeitregeln in Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl $\alpha_n \cdot 10^n + ... + \alpha_0$.
(Bsp. $237 = 2 \cdot 100 + 3 \cdot 10 + 7$).
Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 2$*?*
Frage umformulieren: *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_2$*?*

.

Anwendung: Teilbarkeitregeln in Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl $\alpha_n \cdot 10^n + ... + \alpha_0$.
(Bsp. $237 = 2 \cdot 100 + 3 \cdot 10 + 7$).
Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 2$*?*
Frage umformulieren: *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_2$*?*
Weil $[a] = [0]$ (in $\mathbb{Z}_2$) g.d.w. $a - 0 \ \vdots \ 2$.

.

Anwendung: Teilbarkeitregeln in Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl $\alpha_n \cdot 10^n + ... + \alpha_0$.
(Bsp. $237 = 2 \cdot 100 + 3 \cdot 10 + 7$).
Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 2$*?*
Frage umformulieren: *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_2$*?*
Weil $[a] = [0]$ (in $\mathbb{Z}_2$) g.d.w. $a - 0 \ \vdots \ 2$.
Frage umformulieren:

.

Anwendung: Teilbarkeitregeln in Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl $\alpha_n \cdot 10^n + ... + \alpha_0$.
(Bsp. $237 = 2 \cdot 100 + 3 \cdot 10 + 7$).
Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 2$*?*
Frage umformulieren: *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_2$*?*
Weil $[a] = [0]$ (in $\mathbb{Z}_2$) g.d.w. $a - 0 \ \vdots \ 2$.
Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_2$*?*

.

Anwendung: Teilbarkeitregeln in Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl $\alpha_n \cdot 10^n + ... + \alpha_0$.
(Bsp. $237 = 2 \cdot 100 + 3 \cdot 10 + 7$).
Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 2$*?*
Frage umformulieren: *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_2$*?*
Weil $[a] = [0]$ (in $\mathbb{Z}_2$) g.d.w. $a - 0 \ \vdots \ 2$.
Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_2$*?*
Ausrechnen:

.

Anwendung: Teilbarkeitregeln in Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl $\alpha_n \cdot 10^n + ... + \alpha_0$.
(Bsp. $237 = 2 \cdot 100 + 3 \cdot 10 + 7$).
Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 2$*?*
Frage umformulieren: *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_2$*?*
Weil $[a] = [0]$ (in $\mathbb{Z}_2$) g.d.w. $a - 0 \ \vdots \ 2$.
Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_2$*?*
Ausrechnen:

$$[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1]$$

.

Anwendung: Teilbarkeitregeln in Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl $\alpha_n \cdot 10^n + ... + \alpha_0$.
(Bsp. $237 = 2 \cdot 100 + 3 \cdot 10 + 7$).
Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 2$*?*
Frage umformulieren: *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_2$*?*
Weil $[a] = [0]$ (in $\mathbb{Z}_2$) g.d.w. $a - 0 \ \vdots \ 2$.
Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_2$*?*
Ausrechnen:

$$[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [\alpha_n \cdot 10^n] \overset{\text{mod } 5}{+} ... \overset{\text{mod } 5}{+} [\alpha_0 \cdot 1]$$

.

Anwendung: Teilbarkeitregeln in Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl $\alpha_n \cdot 10^n + ... + \alpha_0$.
(Bsp. $237 = 2 \cdot 100 + 3 \cdot 10 + 7$).
Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 2$*?*
Frage umformulieren: *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_2$*?*
Weil $[a] = [0]$ (in $\mathbb{Z}_2$) g.d.w. $a - 0 \ \vdots \ 2$.
Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_2$*?*
Ausrechnen:

$$[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [\alpha_n \cdot 10^n] \overset{\text{mod } 5}{+} ... \overset{\text{mod } 5}{+} [\alpha_0 \cdot 1]$$

$$= [\alpha_n] \overset{\text{mod } 2}{\cdot} [10^n] \overset{\text{mod } 5}{+} ... \overset{\text{mod } 5}{+} [\alpha_1] \overset{\text{mod } 2}{\cdot} [10] \overset{\text{mod } 5}{+} [\alpha_0] \overset{\text{mod } 2}{\cdot} [1]$$

.

Anwendung: Teilbarkeitregeln in Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl $\alpha_n \cdot 10^n + ... + \alpha_0$.
(Bsp. $237 = 2 \cdot 100 + 3 \cdot 10 + 7$).
Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 2$*?*
Frage umformulieren: *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_2$*?*
Weil $[a] = [0]$ (in $\mathbb{Z}_2$) g.d.w. $a - 0 \ \vdots \ 2$.
Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_2$*?*
Ausrechnen:

$$[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [\alpha_n \cdot 10^n] \overset{\text{mod } 5}{+} ... \overset{\text{mod } 5}{+} [\alpha_0 \cdot 1]$$

$$= [\alpha_n] \overset{\text{mod } 2}{\cdot} [10^n] \overset{\text{mod } 5}{+} ... \overset{\text{mod } 5}{+} [\alpha_1] \overset{\text{mod } 2}{\cdot} [10] \overset{\text{mod } 5}{+} [\alpha_0] \overset{\text{mod } 2}{\cdot} [1]$$

$$= [\alpha_n] \overset{\text{mod } 2}{\cdot} [0] \overset{\text{mod } 5}{+} ... \overset{\text{mod } 5}{+} [\alpha_1] \overset{\text{mod } 2}{\cdot} [0] \overset{\text{mod } 5}{+} [\alpha_0] \overset{\text{mod } 2}{\cdot} [1]$$

.

Anwendung: Teilbarkeitregeln in Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl $\alpha_n \cdot 10^n + ... + \alpha_0$.
(Bsp. $237 = 2 \cdot 100 + 3 \cdot 10 + 7$).
Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 2$*?*
Frage umformulieren: *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_2$*?*
Weil $[a] = [0]$ (in $\mathbb{Z}_2$) g.d.w. $a - 0 \ \vdots \ 2$.
Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_2$*?*
Ausrechnen:

$$[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [\alpha_n \cdot 10^n] \overset{\text{mod } 5}{+} ... \overset{\text{mod } 5}{+} [\alpha_0 \cdot 1]$$
$$= [\alpha_n] \overset{\text{mod } 2}{\cdot} [10^n] \overset{\text{mod } 5}{+} ... \overset{\text{mod } 5}{+} [\alpha_1] \overset{\text{mod } 2}{\cdot} [10] \overset{\text{mod } 5}{+} [\alpha_0] \overset{\text{mod } 2}{\cdot} [1]$$
$$= [\alpha_n] \overset{\text{mod } 2}{\cdot} [0] \overset{\text{mod } 5}{+} ... \overset{\text{mod } 5}{+} [\alpha_1] \overset{\text{mod } 2}{\cdot} [0] \overset{\text{mod } 5}{+} [\alpha_0] \overset{\text{mod } 2}{\cdot} [1]$$
$$= [\alpha_n \cdot 0 + ... + \alpha_1 \cdot 0 + \alpha_0 \cdot 1] \quad .$$

Anwendung: Teilbarkeitregeln in Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl $\alpha_n \cdot 10^n + ... + \alpha_0$.
(Bsp. $237 = 2 \cdot 100 + 3 \cdot 10 + 7$).
Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 2$*?*
Frage umformulieren: *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_2$*?*
Weil $[a] = [0]$ (in $\mathbb{Z}_2$) g.d.w. $a - 0 \ \vdots \ 2$.
Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_2$*?*
Ausrechnen:

$$[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [\alpha_n \cdot 10^n] \overset{\text{mod } 5}{+} ... \overset{\text{mod } 5}{+} [\alpha_0 \cdot 1]$$
$$= [\alpha_n] \overset{\text{mod } 2}{\cdot} [10^n] \overset{\text{mod } 5}{+} ... \overset{\text{mod } 5}{+} [\alpha_1] \overset{\text{mod } 2}{\cdot} [10] \overset{\text{mod } 5}{+} [\alpha_0] \overset{\text{mod } 2}{\cdot} [1]$$
$$= [\alpha_n] \overset{\text{mod } 2}{\cdot} [0] \overset{\text{mod } 5}{+} ... \overset{\text{mod } 5}{+} [\alpha_1] \overset{\text{mod } 2}{\cdot} [0] \overset{\text{mod } 5}{+} [\alpha_0] \overset{\text{mod } 2}{\cdot} [1]$$
$$= [\alpha_n \cdot 0 + ... + \alpha_1 \cdot 0 + \alpha_0 \cdot 1] = [\alpha_0].$$

Anwendung: Teilbarkeitregeln in Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl $\alpha_n \cdot 10^n + ... + \alpha_0$.
(Bsp. $237 = 2 \cdot 100 + 3 \cdot 10 + 7$).
Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 2$*?*
Frage umformulieren: *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_2$*?*
Weil $[a] = [0]$ (in $\mathbb{Z}_2$) g.d.w. $a - 0 \ \vdots \ 2$.
Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_2$*?*
Ausrechnen:

$$[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [\alpha_n \cdot 10^n] \overset{\text{mod } 5}{+} ... \overset{\text{mod } 5}{+} [\alpha_0 \cdot 1]$$
$$= [\alpha_n] \overset{\text{mod } 2}{\cdot} [10^n] \overset{\text{mod } 5}{+} ... \overset{\text{mod } 5}{+} [\alpha_1] \overset{\text{mod } 2}{\cdot} [10] \overset{\text{mod } 5}{+} [\alpha_0] \overset{\text{mod } 2}{\cdot} [1]$$
$$= [\alpha_n] \overset{\text{mod } 2}{\cdot} [0] \overset{\text{mod } 5}{+} ... \overset{\text{mod } 5}{+} [\alpha_1] \overset{\text{mod } 2}{\cdot} [0] \overset{\text{mod } 5}{+} [\alpha_0] \overset{\text{mod } 2}{\cdot} [1]$$
$$= [\alpha_n \cdot 0 + ... + \alpha_1 \cdot 0 + \alpha_0 \cdot 1] = [\alpha_0].$$

Antwort: $[\alpha_n\alpha_{n-1}...\alpha_0] = [\alpha_0]$ in $\mathbb{Z}_2$

Anwendung: Teilbarkeitregeln in Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl $\alpha_n \cdot 10^n + ... + \alpha_0$.
(Bsp. $237 = 2 \cdot 100 + 3 \cdot 10 + 7$).
Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 2$*?*
Frage umformulieren: *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_2$*?*
Weil $[a] = [0]$ (in $\mathbb{Z}_2$) g.d.w. $a - 0 \ \vdots \ 2$.
Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_2$*?*
Ausrechnen:

$$[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [\alpha_n \cdot 10^n] \overset{\text{mod } 5}{+} ... \overset{\text{mod } 5}{+} [\alpha_0 \cdot 1]$$
$$= [\alpha_n] \overset{\text{mod } 2}{\cdot} [10^n] \overset{\text{mod } 5}{+} ... \overset{\text{mod } 5}{+} [\alpha_1] \overset{\text{mod } 2}{\cdot} [10] \overset{\text{mod } 5}{+} [\alpha_0] \overset{\text{mod } 2}{\cdot} [1]$$
$$= [\alpha_n] \overset{\text{mod } 2}{\cdot} [0] \overset{\text{mod } 5}{+} ... \overset{\text{mod } 5}{+} [\alpha_1] \overset{\text{mod } 2}{\cdot} [0] \overset{\text{mod } 5}{+} [\alpha_0] \overset{\text{mod } 2}{\cdot} [1]$$
$$= [\alpha_n \cdot 0 + ... + \alpha_1 \cdot 0 + \alpha_0 \cdot 1] = [\alpha_0].$$

Antwort: $[\alpha_n\alpha_{n-1}...\alpha_0] = [\alpha_0]$ in $\mathbb{Z}_2$
Antwort umformulieren:

Anwendung: Teilbarkeitregeln in Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl $\alpha_n \cdot 10^n + ... + \alpha_0$.
(Bsp. $237 = 2 \cdot 100 + 3 \cdot 10 + 7$).
Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 2$*?*
Frage umformulieren: *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_2$*?*
Weil $[a] = [0]$ (in $\mathbb{Z}_2$) g.d.w. $a - 0 \ \vdots \ 2$.
Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_2$*?*
Ausrechnen:

$$[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [\alpha_n \cdot 10^n] \overset{\text{mod } 5}{+} ... \overset{\text{mod } 5}{+} [\alpha_0 \cdot 1]$$
$$= [\alpha_n] \overset{\text{mod } 2}{\cdot} [10^n] \overset{\text{mod } 5}{+} ... \overset{\text{mod } 5}{+} [\alpha_1] \overset{\text{mod } 2}{\cdot} [10] \overset{\text{mod } 5}{+} [\alpha_0] \overset{\text{mod } 2}{\cdot} [1]$$
$$= [\alpha_n] \overset{\text{mod } 2}{\cdot} [0] \overset{\text{mod } 5}{+} ... \overset{\text{mod } 5}{+} [\alpha_1] \overset{\text{mod } 2}{\cdot} [0] \overset{\text{mod } 5}{+} [\alpha_0] \overset{\text{mod } 2}{\cdot} [1]$$
$$= [\alpha_n \cdot 0 + ... + \alpha_1 \cdot 0 + \alpha_0 \cdot 1] = [\alpha_0].$$

Antwort: $[\alpha_n\alpha_{n-1}...\alpha_0] = [\alpha_0]$ in $\mathbb{Z}_2$
Antwort umformulieren: $\alpha_n\alpha_{n-1}...\alpha_0$ ist g.d. durch 2 Teilbar, wenn α_0 durch 2 Teilbar ist.

Frage:

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \vdots 3?$

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \vdots 3?$

Frage umformulieren:

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 3?$

Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_3$*?*

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 3?$

Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_3$*?*

Wir rechnen $[10^k] = \underbrace{[10] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{\cdot} ... \overset{\text{mod } 3}{\cdot} [10]}_{k \text{ mal}}$ in $\mathbb{Z}_3$ aus:

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 3?$

Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_3$*?*

Wir rechnen $[10^k] = \underbrace{[10] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{\cdot} ... \overset{\text{mod } 3}{\cdot} [10]}_{k \text{ mal}}$ in $\mathbb{Z}_3$ aus:

k	$[10^k]$ in $\mathbb{Z}_3$

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 3?$

Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_3$*?*

Wir rechnen $[10^k] = \underbrace{[10] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{\cdot} ... \overset{\text{mod } 3}{\cdot} [10]}_{k \text{ mal}}$ in $\mathbb{Z}_3$ aus:

k	$[10^k]$ in $\mathbb{Z}_3$
0	
1	
2	
3	
$\vdots$	

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 3?$

Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_3$*?*

Wir rechnen $[10^k] = \underbrace{[10] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{\cdot} ... \overset{\text{mod } 3}{\cdot} [10]}_{k \text{ mal}}$ in $\mathbb{Z}_3$ aus:

k	$[10^k]$ in $\mathbb{Z}_3$
0	[1]
1	
2	
3	
⋮	

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 3?$

Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_3$*?*

Wir rechnen $[10^k] = \underbrace{[10] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{\cdot} ... \overset{\text{mod } 3}{\cdot} [10]}_{k \text{ mal}}$ in $\mathbb{Z}_3$ aus:

k	$[10^k]$ in $\mathbb{Z}_3$
0	[1]
1	[10]
2	
3	
⋮	

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 3?$

Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_3$*?*

Wir rechnen $[10^k] = \underbrace{[10] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{\cdot} ... \overset{\text{mod } 3}{\cdot} [10]}_{k \text{ mal}}$ in $\mathbb{Z}_3$ aus:

k	$[10^k]$ in $\mathbb{Z}_3$
0	$[1]$
1	$[10] = [3 \cdot 3 + 1]$
2	
3	
$\vdots$	

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 3?$

Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_3$*?*

Wir rechnen $[10^k] = \underbrace{[10] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{\cdot} ... \overset{\text{mod } 3}{\cdot} [10]}_{k \text{ mal}}$ in $\mathbb{Z}_3$ aus:

k	$[10^k]$ in $\mathbb{Z}_3$
0	$[1]$
1	$[10] = [3 \cdot 3 + 1] = [1]$
2	
3	
$\vdots$	

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 3?$

Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_3$*?*

Wir rechnen $[10^k] = \underbrace{[10] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{\cdot} ... \overset{\text{mod } 3}{\cdot} [10]}_{k \text{ mal}}$ in $\mathbb{Z}_3$ aus:

k	$[10^k]$ in $\mathbb{Z}_3$
0	$[1]$
1	$[10] = [3 \cdot 3 + 1] = [1]$
2	$[10^2] = [10] \cdot [10] = [1] \cdot [1] = [1]$
3	
$\vdots$	

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 3?$

Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_3$*?*

Wir rechnen $[10^k] = \underbrace{[10] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{\cdot} ... \overset{\text{mod } 3}{\cdot} [10]}_{k \text{ mal}}$ in $\mathbb{Z}_3$ aus:

k	$[10^k]$ in $\mathbb{Z}_3$
0	$[1]$
1	$[10] = [3 \cdot 3 + 1] = [1]$
2	$[10^2] = [10] \cdot [10] = [1] \cdot [1] = [1]$
3	$[10^3] = [10^2 \cdot 10] = [1] \cdot [1] = [1]$
$\vdots$	

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 3?$

Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_3$*?*

Wir rechnen $[10^k] = \underbrace{[10] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{\cdot} ... \overset{\text{mod } 3}{\cdot} [10]}_{k \text{ mal}}$ in $\mathbb{Z}_3$ aus:

k	$[10^k]$ in $\mathbb{Z}_3$
0	$[1]$
1	$[10] = [3 \cdot 3 + 1] = [1]$
2	$[10^2] = [10] \cdot [10] = [1] \cdot [1] = [1]$
3	$[10^3] = [10^2 \cdot 10] = [1] \cdot [1] = [1]$
$\vdots$	$\vdots$

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 3?$

Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_3$*?*

Wir rechnen $[10^k] = \underbrace{[10] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{\cdot} ... \overset{\text{mod } 3}{\cdot} [10]}_{k \text{ mal}}$ in $\mathbb{Z}_3$ aus:

k	$[10^k]$ in $\mathbb{Z}_3$
0	$[1]$
1	$[10] = [3 \cdot 3 + 1] = [1]$
2	$[10^2] = [10] \cdot [10] = [1] \cdot [1] = [1]$
3	$[10^3] = [10^2 \cdot 10] = [1] \cdot [1] = [1]$
$\vdots$	$\vdots$

Deswegen:

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 3?$

Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_3$*?*

Wir rechnen $[10^k] = \underbrace{[10] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{\cdot} ... \overset{\text{mod } 3}{\cdot} [10]}_{k \text{ mal}}$ in $\mathbb{Z}_3$ aus:

k	$[10^k]$ in $\mathbb{Z}_3$
0	$[1]$
1	$[10] = [3 \cdot 3 + 1] = [1]$
2	$[10^2] = [10] \cdot [10] = [1] \cdot [1] = [1]$
3	$[10^3] = [10^2 \cdot 10] = [1] \cdot [1] = [1]$
$\vdots$	$\vdots$

Deswegen:

$$[\alpha_n \cdot 10^n + ... + \alpha_1 \cdot 10 + \alpha_0 \cdot 1]$$

.

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 3?$

Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_3$*?*

Wir rechnen $[10^k] = \underbrace{[10] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{\cdot} ... \overset{\text{mod } 3}{\cdot} [10]}_{k \text{ mal}}$ in $\mathbb{Z}_3$ aus:

k	$[10^k]$ in $\mathbb{Z}_3$
0	$[1]$
1	$[10] = [3 \cdot 3 + 1] = [1]$
2	$[10^2] = [10] \cdot [10] = [1] \cdot [1] = [1]$
3	$[10^3] = [10^2 \cdot 10] = [1] \cdot [1] = [1]$
$\vdots$	$\vdots$

Deswegen:

$$[\alpha_n \cdot 10^n + ... + \alpha_1 \cdot 10 + \alpha_0 \cdot 1]$$
$$= [\alpha_n] \overset{\text{mod } 3}{\cdot} [10^n] \overset{\text{mod } 3}{+} ... \overset{\text{mod } 3}{+} [\alpha_1] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{+} [\alpha_0] \overset{\text{mod } 3}{\cdot} [1]$$

.

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 3?$

Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_3$*?*

Wir rechnen $[10^k] = \underbrace{[10] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{\cdot} ... \overset{\text{mod } 3}{\cdot} [10]}_{k \text{ mal}}$ in $\mathbb{Z}_3$ aus:

k	$[10^k]$ in $\mathbb{Z}_3$
0	$[1]$
1	$[10] = [3 \cdot 3 + 1] = [1]$
2	$[10^2] = [10] \cdot [10] = [1] \cdot [1] = [1]$
3	$[10^3] = [10^2 \cdot 10] = [1] \cdot [1] = [1]$
$\vdots$	$\vdots$

Deswegen:

$$
\begin{aligned}
& [\alpha_n \cdot 10^n + ... + \alpha_1 \cdot 10 + \alpha_0 \cdot 1] \\
= & [\alpha_n] \overset{\text{mod } 3}{\cdot} [10^n] \overset{\text{mod } 3}{+} ... \overset{\text{mod } 3}{+} [\alpha_1] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{+} [\alpha_0] \overset{\text{mod } 3}{\cdot} [1] \\
= & [\alpha_n] \overset{\text{mod } 3}{\cdot} [1] \overset{\text{mod } 3}{+} ... \overset{\text{mod } 3}{+} [\alpha_1] \overset{\text{mod } 3}{\cdot} [1] \overset{\text{mod } 3}{+} [\alpha_0] \overset{\text{mod } 3}{\cdot} [1]
\end{aligned}
$$

.

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 3?$

Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_3$*?*

Wir rechnen $[10^k] = \underbrace{[10] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{\cdot} ... \overset{\text{mod } 3}{\cdot} [10]}_{k \text{ mal}}$ in $\mathbb{Z}_3$ aus:

k	$[10^k]$ in $\mathbb{Z}_3$
0	$[1]$
1	$[10] = [3 \cdot 3 + 1] = [1]$
2	$[10^2] = [10] \cdot [10] = [1] \cdot [1] = [1]$
3	$[10^3] = [10^2 \cdot 10] = [1] \cdot [1] = [1]$
$\vdots$	$\vdots$

Deswegen:

$$
\begin{aligned}
& [\alpha_n \cdot 10^n + ... + \alpha_1 \cdot 10 + \alpha_0 \cdot 1] \\
= & [\alpha_n] \overset{\text{mod } 3}{\cdot} [10^n] \overset{\text{mod } 3}{+} ... \overset{\text{mod } 3}{+} [\alpha_1] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{+} [\alpha_0] \overset{\text{mod } 3}{\cdot} [1] \\
= & [\alpha_n] \overset{\text{mod } 3}{\cdot} [1] \overset{\text{mod } 3}{+} ... \overset{\text{mod } 3}{+} [\alpha_1] \overset{\text{mod } 3}{\cdot} [1] \overset{\text{mod } 3}{+} [\alpha_0] \overset{\text{mod } 3}{\cdot} [1] \\
= & [\alpha_n + ... + \alpha_1 + \alpha_0].
\end{aligned}
$$

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 3?$

Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_3$*?*

Wir rechnen $[10^k] = \underbrace{[10] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{\cdot} ... \overset{\text{mod } 3}{\cdot} [10]}_{k \text{ mal}}$ in $\mathbb{Z}_3$ aus:

k	$[10^k]$ in $\mathbb{Z}_3$
0	$[1]$
1	$[10] = [3 \cdot 3 + 1] = [1]$
2	$[10^2] = [10] \cdot [10] = [1] \cdot [1] = [1]$
3	$[10^3] = [10^2 \cdot 10] = [1] \cdot [1] = [1]$
$\vdots$	$\vdots$

Deswegen:

$$
\begin{aligned}
&[\alpha_n \cdot 10^n + ... + \alpha_1 \cdot 10 + \alpha_0 \cdot 1] \\
&= [\alpha_n] \overset{\text{mod } 3}{\cdot} [10^n] \overset{\text{mod } 3}{+} ... \overset{\text{mod } 3}{+} [\alpha_1] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{+} [\alpha_0] \overset{\text{mod } 3}{\cdot} [1] \\
&= [\alpha_n] \overset{\text{mod } 3}{\cdot} [1] \overset{\text{mod } 3}{+} ... \overset{\text{mod } 3}{+} [\alpha_1] \overset{\text{mod } 3}{\cdot} [1] \overset{\text{mod } 3}{+} [\alpha_0] \overset{\text{mod } 3}{\cdot} [1] \\
&= [\alpha_n + ... + \alpha_1 + \alpha_0].
\end{aligned}
$$

Antwort: $\alpha_n\alpha_{n-1}...\alpha_0$ *ist g.d. durch 3 Teilbar, wenn* $\alpha_n + \alpha_{n-1} + ... + \alpha_0$ *durch 3 Teilbar ist.*

Frage: $\alpha_n \alpha_{n-1} \ldots \alpha_0 \ \vdots \ 7?$

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*
Ausrechnen 10^k in $\mathbb{Z}_7$:

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
$\vdots$	$\vdots$
$\vdots$	$\vdots$

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	[1]
$\vdots$	$\vdots$
$\vdots$	$\vdots$

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	[1]
1	[3]
⋮	⋮
⋮	⋮

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	[1]
1	[3]
2	
⋮	⋮
⋮	⋮

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	[1]
1	[3]
2	$[3] \overset{\text{mod } 7}{\cdot} [3] = [9] = [2]$
⋮	⋮
⋮	⋮

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7$? *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$?

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	[1]
1	[3]
2	$[3] \overset{\text{mod } 7}{\cdot} [3] = [9] = [2]$
3	
⋮	⋮
⋮	⋮

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\text{mod } 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\text{mod } 7}{\cdot} [2] = [6] = [-1]$
$\vdots$	$\vdots$
$\vdots$	$\vdots$

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\text{mod } 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\text{mod } 7}{\cdot} [2] = [6] = [-1]$
4	
$\vdots$	$\vdots$
$\vdots$	$\vdots$

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\text{mod } 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\text{mod } 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\text{mod } 7}{\cdot} [-1] = [-3]$
$\vdots$	$\vdots$
$\vdots$	$\vdots$

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\text{mod } 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\text{mod } 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\text{mod } 7}{\cdot} [-1] = [-3]$
5	
$\vdots$	$\vdots$
$\vdots$	$\vdots$

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\mod 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\mod 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\mod 7}{\cdot} [-1] = [-3]$
5	$[3] \overset{\mod 7}{\cdot} [-3] = [-9] = [-2]$
$\vdots$	$\vdots$
$\vdots$	$\vdots$

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\mod 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\mod 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\mod 7}{\cdot} [-1] = [-3]$
5	$[3] \overset{\mod 7}{\cdot} [-3] = [-9] = [-2]$
6	
$\vdots$	$\vdots$
$\vdots$	$\vdots$

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\mathrm{mod}\ 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\mathrm{mod}\ 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\mathrm{mod}\ 7}{\cdot} [-1] = [-3]$
5	$[3] \overset{\mathrm{mod}\ 7}{\cdot} [-3] = [-9] = [-2]$
6	$[3] \overset{\mathrm{mod}\ 7}{\cdot} [-2] = [-6] = [1]$
$\vdots$	$\vdots$
$\vdots$	$\vdots$

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\mathrm{mod}\ 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\mathrm{mod}\ 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\mathrm{mod}\ 7}{\cdot} [-1] = [-3]$
5	$[3] \overset{\mathrm{mod}\ 7}{\cdot} [-3] = [-9] = [-2]$
6	$[3] \overset{\mathrm{mod}\ 7}{\cdot} [-2] = [-6] = [1]$
$\vdots$	$\vdots$
$6k$	
$\vdots$	$\vdots$

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\mathrm{mod}\ 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\mathrm{mod}\ 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\mathrm{mod}\ 7}{\cdot} [-1] = [-3]$
5	$[3] \overset{\mathrm{mod}\ 7}{\cdot} [-3] = [-9] = [-2]$
6	$[3] \overset{\mathrm{mod}\ 7}{\cdot} [-2] = [-6] = [1]$
$\vdots$	$\vdots$
$6k$	$[1]$
$\vdots$	$\vdots$

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\text{mod } 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\text{mod } 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\text{mod } 7}{\cdot} [-1] = [-3]$
5	$[3] \overset{\text{mod } 7}{\cdot} [-3] = [-9] = [-2]$
6	$[3] \overset{\text{mod } 7}{\cdot} [-2] = [-6] = [1]$
$\vdots$	$\vdots$
$6k$	$[1]$
$6k+1$	$[3]$
$\vdots$	$\vdots$

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\text{mod } 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\text{mod } 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\text{mod } 7}{\cdot} [-1] = [-3]$
5	$[3] \overset{\text{mod } 7}{\cdot} [-3] = [-9] = [-2]$
6	$[3] \overset{\text{mod } 7}{\cdot} [-2] = [-6] = [1]$
$\vdots$	$\vdots$
$6k$	$[1]$
$6k+1$	$[3]$
$6k+2$	$[2]$
$\vdots$	$\vdots$

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\text{mod } 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\text{mod } 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\text{mod } 7}{\cdot} [-1] = [-3]$
5	$[3] \overset{\text{mod } 7}{\cdot} [-3] = [-9] = [-2]$
6	$[3] \overset{\text{mod } 7}{\cdot} [-2] = [-6] = [1]$
$\vdots$	$\vdots$
$6k$	$[1]$
$6k+1$	$[3]$
$6k+2$	$[2]$
$6k+3$	$[-1]$
$\vdots$	$\vdots$

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\text{mod } 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\text{mod } 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\text{mod } 7}{\cdot} [-1] = [-3]$
5	$[3] \overset{\text{mod } 7}{\cdot} [-3] = [-9] = [-2]$
6	$[3] \overset{\text{mod } 7}{\cdot} [-2] = [-6] = [1]$
$\vdots$	$\vdots$
$6k$	$[1]$
$6k+1$	$[3]$
$6k+2$	$[2]$
$6k+3$	$[-1]$
$6k+4$	$[-3]$
$\vdots$	$\vdots$

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\text{mod } 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\text{mod } 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\text{mod } 7}{\cdot} [-1] = [-3]$
5	$[3] \overset{\text{mod } 7}{\cdot} [-3] = [-9] = [-2]$
6	$[3] \overset{\text{mod } 7}{\cdot} [-2] = [-6] = [1]$
$\vdots$	$\vdots$
$6k$	$[1]$
$6k+1$	$[3]$
$6k+2$	$[2]$
$6k+3$	$[-1]$
$6k+4$	$[-3]$
$6k+5$	$[-2]$
$\vdots$	$\vdots$

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\text{mod } 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\text{mod } 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\text{mod } 7}{\cdot} [-1] = [-3]$
5	$[3] \overset{\text{mod } 7}{\cdot} [-3] = [-9] = [-2]$
6	$[3] \overset{\text{mod } 7}{\cdot} [-2] = [-6] = [1]$
$\vdots$	$\vdots$
$6k$	$[1]$
$6k+1$	$[3]$
$6k+2$	$[2]$
$6k+3$	$[-1]$
$6k+4$	$[-3]$
$6k+5$	$[-2]$
$\vdots$	$\vdots$

Antwort:

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*
Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\text{mod } 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\text{mod } 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\text{mod } 7}{\cdot} [-1] = [-3]$
5	$[3] \overset{\text{mod } 7}{\cdot} [-3] = [-9] = [-2]$
6	$[3] \overset{\text{mod } 7}{\cdot} [-2] = [-6] = [1]$
$\vdots$	$\vdots$
$6k$	$[1]$
$6k+1$	$[3]$
$6k+2$	$[2]$
$6k+3$	$[-1]$
$6k+4$	$[-3]$
$6k+5$	$[-2]$
$\vdots$	$\vdots$

Antwort: $\alpha_n...\alpha_0$ *ist g.d. durch 7 Teilbar,*

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*
Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\mod 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\mod 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\mod 7}{\cdot} [-1] = [-3]$
5	$[3] \overset{\mod 7}{\cdot} [-3] = [-9] = [-2]$
6	$[3] \overset{\mod 7}{\cdot} [-2] = [-6] = [1]$
$\vdots$	$\vdots$
$6k$	$[1]$
$6k+1$	$[3]$
$6k+2$	$[2]$
$6k+3$	$[-1]$
$6k+4$	$[-3]$
$6k+5$	$[-2]$
$\vdots$	$\vdots$

Antwort: $\alpha_n...\alpha_0$ *ist g.d. durch 7 Teilbar, wenn*
$\alpha_0 + 3\alpha_1 + 2\alpha_2 - \alpha_3 - 3\alpha_4 - 2\alpha_5$
$+\alpha_6 + 3\alpha_7 + 2\alpha_8 - \alpha_9 - 3\alpha_{10} - 2\alpha_{11}$
$+... + \alpha_{6k} + 3\alpha_{6k+1} + 2\alpha_{6k+2} - \alpha_{6k+3} - 3\alpha_{6k+4} - 2\alpha_{6k+5} + ...$
durch 7 Teilbar ist.

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*
Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\mod 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\mod 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\mod 7}{\cdot} [-1] = [-3]$
5	$[3] \overset{\mod 7}{\cdot} [-3] = [-9] = [-2]$
6	$[3] \overset{\mod 7}{\cdot} [-2] = [-6] = [1]$
$\vdots$	$\vdots$
$6k$	$[1]$
$6k+1$	$[3]$
$6k+2$	$[2]$
$6k+3$	$[-1]$
$6k+4$	$[-3]$
$6k+5$	$[-2]$
$\vdots$	$\vdots$

Antwort: $\alpha_n...\alpha_0$ *ist g.d. durch 7 Teilbar, wenn*
$\alpha_0 + 3\alpha_1 + 2\alpha_2 - \alpha_3 - 3\alpha_4 - 2\alpha_5$
$+\alpha_6 + 3\alpha_7 + 2\alpha_8 - \alpha_9 - 3\alpha_{10} - 2\alpha_{11}$
$+... + \alpha_{6k} + 3\alpha_{6k+1} + 2\alpha_{6k+2} - \alpha_{6k+3} - 3\alpha_{6k+4} - 2\alpha_{6k+5} + ...$
durch 7 Teilbar ist.

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*
Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\mod 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\mod 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\mod 7}{\cdot} [-1] = [-3]$
5	$[3] \overset{\mod 7}{\cdot} [-3] = [-9] = [-2]$
6	$[3] \overset{\mod 7}{\cdot} [-2] = [-6] = [1]$
$\vdots$	$\vdots$
$6k$	$[1]$
$6k+1$	$[3]$
$6k+2$	$[2]$
$6k+3$	$[-1]$
$6k+4$	$[-3]$
$6k+5$	$[-2]$
$\vdots$	$\vdots$

Antwort: $\alpha_n...\alpha_0$ *ist g.d. durch 7 Teilbar, wenn*
$\alpha_0 + 3\alpha_1 + 2\alpha_2 - \alpha_3 - 3\alpha_4 - 2\alpha_5$
$+\alpha_6 + 3\alpha_7 + 2\alpha_8 - \alpha_9 - 3\alpha_{10} - 2\alpha_{11}$
$+... + \alpha_{6k} + 3\alpha_{6k+1} + 2\alpha_{6k+2} - \alpha_{6k+3} - 3\alpha_{6k+4} - 2\alpha_{6k+5} + ...$
durch 7 Teilbar ist.

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*
Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\mod 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\mod 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\mod 7}{\cdot} [-1] = [-3]$
5	$[3] \overset{\mod 7}{\cdot} [-3] = [-9] = [-2]$
6	$[3] \overset{\mod 7}{\cdot} [-2] = [-6] = [1]$
$\vdots$	$\vdots$
$6k$	$[1]$
$6k+1$	$[3]$
$6k+2$	$[2]$
$6k+3$	$[-1]$
$6k+4$	$[-3]$
$6k+5$	$[-2]$
$\vdots$	$\vdots$

Bsp.

Antwort: $\alpha_n...\alpha_0$ *ist g.d. durch 7 Teilbar, wenn*
$\alpha_0 + 3\alpha_1 + 2\alpha_2 - \alpha_3 - 3\alpha_4 - 2\alpha_5$
$+\alpha_6 + 3\alpha_7 + 2\alpha_8 - \alpha_9 - 3\alpha_{10} - 2\alpha_{11}$
$+... + \alpha_{6k} + 3\alpha_{6k+1} + 2\alpha_{6k+2} - \alpha_{6k+3} - 3\alpha_{6k+4} - 2\alpha_{6k+5} + ...$
durch 7 Teilbar ist.

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*
Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\mod 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\mod 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\mod 7}{\cdot} [-1] = [-3]$
5	$[3] \overset{\mod 7}{\cdot} [-3] = [-9] = [-2]$
6	$[3] \overset{\mod 7}{\cdot} [-2] = [-6] = [1]$
$\vdots$	$\vdots$
$6k$	$[1]$
$6k+1$	$[3]$
$6k+2$	$[2]$
$6k+3$	$[-1]$
$6k+4$	$[-3]$
$6k+5$	$[-2]$
$\vdots$	$\vdots$

Bsp. 938748033764775430564 9 ist durch 7 teilbar,

Antwort: $\alpha_n...\alpha_0$ *ist g.d. durch 7 Teilbar, wenn*
$\alpha_0 + 3\alpha_1 + 2\alpha_2 - \alpha_3 - 3\alpha_4 - 2\alpha_5$
$+\alpha_6 + 3\alpha_7 + 2\alpha_8 - \alpha_9 - 3\alpha_{10} - 2\alpha_{11}$
$+... + \alpha_{6k} + 3\alpha_{6k+1} + 2\alpha_{6k+2} - \alpha_{6k+3} - 3\alpha_{6k+4} - 2\alpha_{6k+5} + ...$
durch 7 Teilbar ist.

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*
Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\text{mod } 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\text{mod } 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\text{mod } 7}{\cdot} [-1] = [-3]$
5	$[3] \overset{\text{mod } 7}{\cdot} [-3] = [-9] = [-2]$
6	$[3] \overset{\text{mod } 7}{\cdot} [-2] = [-6] = [1]$
$\vdots$	$\vdots$
$6k$	$[1]$
$6k+1$	$[3]$
$6k+2$	$[2]$
$6k+3$	$[-1]$
$6k+4$	$[-3]$
$6k+5$	$[-2]$
$\vdots$	$\vdots$

Bsp. 938748033764775430564 9 ist durch 7 teilbar, weil

$$1\cdot 9 + 3\cdot 4 + 2\cdot 6 - 1\cdot 5 - 3\cdot 0 - 2\cdot 3$$
$$+1\cdot 4 + 3\cdot 5 + 2\cdot 7 - 1\cdot 7 - 3\cdot 4 - 2\cdot 6$$
$$+1\cdot 7 + 3\cdot 3 + 2\cdot 3 - 1\cdot 0 - 3\cdot 8 - 2\cdot 4$$
$$+1\cdot 7 + 3\cdot 8 + 2\cdot 3 - 1\cdot 9 - 3\cdot 0 - 2\cdot 0$$

Antwort: $\alpha_n...\alpha_0$ *ist g.d. durch 7 Teilbar, wenn*

$$\alpha_0 + 3\alpha_1 + 2\alpha_2 - \alpha_3 - 3\alpha_4 - 2\alpha_5$$
$$+\alpha_6 + 3\alpha_7 + 2\alpha_8 - \alpha_9 - 3\alpha_{10} - 2\alpha_{11}$$
$$+... + \alpha_{6k} + 3\alpha_{6k+1} + 2\alpha_{6k+2} - \alpha_{6k+3} - 3\alpha_{6k+4} - 2\alpha_{6k+5} + ...$$

durch 7 Teilbar ist.

Frage: $\alpha_n\alpha_{n-1}...\alpha_0 \ \vdots \ 7?$ *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_7$*?*
Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\text{mod } 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\text{mod } 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\text{mod } 7}{\cdot} [-1] = [-3]$
5	$[3] \overset{\text{mod } 7}{\cdot} [-3] = [-9] = [-2]$
6	$[3] \overset{\text{mod } 7}{\cdot} [-2] = [-6] = [1]$
$\vdots$	$\vdots$
$6k$	$[1]$
$6k+1$	$[3]$
$6k+2$	$[2]$
$6k+3$	$[-1]$
$6k+4$	$[-3]$
$6k+5$	$[-2]$
$\vdots$	$\vdots$

Bsp. 938748033764775430564 9 ist durch 7 teilbar, weil

$$\begin{aligned}
&1\cdot 9 + 3\cdot 4 + 2\cdot 6 - 1\cdot 5 - 3\cdot 0 - 2\cdot 3 \\
&+1\cdot 4 + 3\cdot 5 + 2\cdot 7 - 1\cdot 7 - 3\cdot 4 - 2\cdot 6 \\
&+1\cdot 7 + 3\cdot 3 + 2\cdot 3 - 1\cdot 0 - 3\cdot 8 - 2\cdot 4 \\
&+1\cdot 7 + 3\cdot 8 + 2\cdot 3 - 1\cdot 9 - 3\cdot 0 - 2\cdot 0 \\
&= 42 \text{ durch 7 teilbar ist.}
\end{aligned}$$

Antwort: $\alpha_n...\alpha_0$ *ist g.d. durch 7 Teilbar, wenn*

$$\begin{aligned}
&\alpha_0 + 3\alpha_1 + 2\alpha_2 - \alpha_3 - 3\alpha_4 - 2\alpha_5 \\
&+\alpha_6 + 3\alpha_7 + 2\alpha_8 - \alpha_9 - 3\alpha_{10} - 2\alpha_{11} \\
&+ ... + \alpha_{6k} + 3\alpha_{6k+1} + 2\alpha_{6k+2} - \alpha_{6k+3} - 3\alpha_{6k+4} - 2\alpha_{6k+5} + ...
\end{aligned}$$

durch 7 Teilbar ist.

BspAufgabe:

,

,

.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$.

,

,

.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformuleren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

,

,

.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$.

$[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
$\vdots$	$\vdots$
$\vdots$	$\vdots$

Umformuleren: Z.z.:

,

,

.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$.

$[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	[1]
⋮	⋮
⋮	⋮

Umformuleren: Z.z.:

,

,

.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$.

$[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	[1]
1	[10]
⋮	⋮
⋮	⋮

Umformuleren: Z.z.:

,

,

.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$.

$[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	[1]
1	[10]
2	
⋮	⋮
⋮	⋮

Umformuleren: Z.z.:

,

,

.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformulieren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
$\vdots$	$\vdots$
$\vdots$	$\vdots$

,

,

.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformuleren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	
$\vdots$	$\vdots$
$\vdots$	$\vdots$

,

,

.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformulieren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 27}{\cdot} [-8] = [-81 + 1] = [1]$
$\vdots$	$\vdots$
$\vdots$	$\vdots$

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformulieren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 27}{\cdot} [-8] = [-81 + 1] = [1]$
$\vdots$	$\vdots$
$\vdots$	$\vdots$

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformulieren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 27}{\cdot} [-8] = [-81 + 1] = [1]$
$\vdots$	$\vdots$
$\vdots$	$\vdots$

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformulieren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 27}{\cdot} [-8] = [-81 + 1] = [1]$
$\vdots$	$\vdots$
$3k$	
$\vdots$	$\vdots$

,

,

.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformulieren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 27}{\cdot} [-8] = [-81 + 1] = [1]$
⋮	⋮
$3k$	$[1]$
⋮	⋮

,

,

.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformulieren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 27}{\cdot} [-8] = [-81 + 1] = [1]$
$\vdots$	$\vdots$
$3k$	$[1]$
$3k+1$	
$\vdots$	$\vdots$

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformulieren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 27}{\cdot} [-8] = [-81 + 1] = [1]$
⋮	⋮
$3k$	$[1]$
$3k + 1$	$[10]$
⋮	⋮

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformulieren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 27}{\cdot} [-8] = [-81 + 1] = [1]$
$\vdots$	$\vdots$
$3k$	$[1]$
$3k + 1$	$[10]$
$3k + 2$	
$\vdots$	$\vdots$

,

,

.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformulieren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 27}{\cdot} [-8] = [-81 + 1] = [1]$
$\vdots$	$\vdots$
$3k$	$[1]$
$3k + 1$	$[10]$
$3k + 2$	$[-8]$
$\vdots$	$\vdots$

,

,

.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformulieren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 27}{\cdot} [-8] = [-81 + 1] = [1]$
$\vdots$	$\vdots$
$3k$	$[1]$
$3k + 1$	$[10]$
$3k + 2$	$[-8]$
$\vdots$	$\vdots$

,

,

.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformulieren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 27}{\cdot} [-8] = [-81 + 1] = [1]$
$\vdots$	$\vdots$
$3k$	$[1]$
$3k + 1$	$[10]$
$3k + 2$	$[-8]$
$\vdots$	$\vdots$

Für $n = 3k$ ist

,

,

.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformuleren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 27}{\cdot} [-8] = [-81 + 1] = [1]$
$\vdots$	$\vdots$
$3k$	$[1]$
$3k+1$	$[10]$
$3k+2$	$[-8]$
$\vdots$	$\vdots$

Für $n = 3k$ ist $[10^{3k} + 18 \cdot 3 \cdot k - 1]$,

,

.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformuleren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 27}{\cdot} [-8] = [-81 + 1] = [1]$
$\vdots$	$\vdots$
$3k$	$[1]$
$3k+1$	$[10]$
$3k+2$	$[-8]$
$\vdots$	$\vdots$

Für $n = 3k$ ist $[10^{3k} + 18 \cdot 3 \cdot k - 1] = [1 + 0 - 1] = [0]$,

,

.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformuleren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 27}{\cdot} [-8] = [-81 + 1] = [1]$
$\vdots$	$\vdots$
$3k$	$[1]$
$3k+1$	$[10]$
$3k+2$	$[-8]$
$\vdots$	$\vdots$

Für $n = 3k$ ist $[10^{3k} + 18 \cdot 3 \cdot k - 1] = [1 + 0 - 1] = [0]$,

Für $n = 3k + 1$ ist

,

.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformuleren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 27}{\cdot} [-8] = [-81 + 1] = [1]$
$\vdots$	$\vdots$
$3k$	$[1]$
$3k+1$	$[10]$
$3k+2$	$[-8]$
$\vdots$	$\vdots$

Für $n = 3k$ ist $[10^{3k} + 18 \cdot 3 \cdot k - 1] = [1 + 0 - 1] = [0]$,

Für $n = 3k + 1$ ist

$[10^{3k+1} + 18 \cdot (3 \cdot k + 1) - 1]$,

.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformuleren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 27}{\cdot} [-8] = [-81 + 1] = [1]$
$\vdots$	$\vdots$
$3k$	$[1]$
$3k+1$	$[10]$
$3k+2$	$[-8]$
$\vdots$	$\vdots$

Für $n = 3k$ ist $[10^{3k} + 18 \cdot 3 \cdot k - 1] = [1 + 0 - 1] = [0]$,

Für $n = 3k + 1$ ist

$[10^{3k+1} + 18 \cdot (3 \cdot k + 1) - 1] = [10 + 18 - 1] =$,

.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformuleren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 27}{\cdot} [-8] = [-81 + 1] = [1]$
$\vdots$	$\vdots$
$3k$	$[1]$
$3k+1$	$[10]$
$3k+2$	$[-8]$
$\vdots$	$\vdots$

Für $n = 3k$ ist $[10^{3k} + 18 \cdot 3 \cdot k - 1] = [1 + 0 - 1] = [0]$,

Für $n = 3k + 1$ ist

$[10^{3k+1} + 18 \cdot (3 \cdot k + 1) - 1] = [10 + 18 - 1] = [27] = [0]$,

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformuleren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 27}{\cdot} [-8] = [-81 + 1] = [1]$
$\vdots$	$\vdots$
$3k$	$[1]$
$3k+1$	$[10]$
$3k+2$	$[-8]$
$\vdots$	$\vdots$

Für $n = 3k$ ist $[10^{3k} + 18 \cdot 3 \cdot k - 1] = [1 + 0 - 1] = [0]$,

Für $n = 3k + 1$ ist

$[10^{3k+1} + 18 \cdot (3 \cdot k + 1) - 1] = [10 + 18 - 1] = [27] = [0]$,

Für $n = 3k + 2$ ist

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformuleren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 27}{\cdot} [-8] = [-81 + 1] = [1]$
$\vdots$	$\vdots$
$3k$	$[1]$
$3k+1$	$[10]$
$3k+2$	$[-8]$
$\vdots$	$\vdots$

Für $n = 3k$ ist $[10^{3k} + 18 \cdot 3 \cdot k - 1] = [1 + 0 - 1] = [0]$,

Für $n = 3k + 1$ ist

$[10^{3k+1} + 18 \cdot (3 \cdot k + 1) - 1] = [10 + 18 - 1] = [27] = [0]$,

Für $n = 3k + 2$ ist

$[10^{3k+2} + 18 \cdot (3 \cdot k + 2) - 1]$.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformuleren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 27}{\cdot} [-8] = [-81 + 1] = [1]$
$\vdots$	$\vdots$
$3k$	$[1]$
$3k+1$	$[10]$
$3k+2$	$[-8]$
$\vdots$	$\vdots$

Für $n = 3k$ ist $[10^{3k} + 18 \cdot 3 \cdot k - 1] = [1 + 0 - 1] = [0]$,

Für $n = 3k + 1$ ist

$[10^{3k+1} + 18 \cdot (3 \cdot k + 1) - 1] = [10 + 18 - 1] = [27] = [0]$,

Für $n = 3k + 2$ ist

$[10^{3k+2} + 18 \cdot (3 \cdot k + 2) - 1] = [-8 + 18 \cdot 2 - 1] =$.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformuleren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 27}{\cdot} [-8] = [-81 + 1] = [1]$
$\vdots$	$\vdots$
$3k$	$[1]$
$3k+1$	$[10]$
$3k+2$	$[-8]$
$\vdots$	$\vdots$

Für $n = 3k$ ist $[10^{3k} + 18 \cdot 3 \cdot k - 1] = [1 + 0 - 1] = [0]$,

Für $n = 3k + 1$ ist

$[10^{3k+1} + 18 \cdot (3 \cdot k + 1) - 1] = [10 + 18 - 1] = [27] = [0]$,

Für $n = 3k + 2$ ist

$[10^{3k+2} + 18 \cdot (3 \cdot k + 2) - 1] = [-8 + 18 \cdot 2 - 1] = [27] = [0]$.

BspAufgabe: Z.z.: $10^n + 18n - 1 \vdots 27$. **Umformuleren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 27}{\cdot} [-8] = [-81 + 1] = [1]$
$\vdots$	$\vdots$
$3k$	$[1]$
$3k+1$	$[10]$
$3k+2$	$[-8]$
$\vdots$	$\vdots$

Für $n = 3k$ ist $[10^{3k} + 18 \cdot 3 \cdot k - 1] = [1 + 0 - 1] = [0]$,

Für $n = 3k + 1$ ist

$[10^{3k+1} + 18 \cdot (3 \cdot k + 1) - 1] = [10 + 18 - 1] = [27] = [0]$,

Für $n = 3k + 2$ ist

$[10^{3k+2} + 18 \cdot (3 \cdot k + 2) - 1] = [-8 + 18 \cdot 2 - 1] = [27] = [0]$. $\square$

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation,

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp:

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$,

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$,

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen.

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist [1]).

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist $[1]$).

Def 15

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist [1]).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring.

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist [1]).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar,

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist [1]).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar, falls $\exists y \in \mathbb{K}$ so dass $yx = 1$.

Bsp:

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist $[1]$).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar, falls $\exists y \in \mathbb{K}$ so dass $yx = 1$.

Bsp: 0 ist nie invertierbar.

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist [1]).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar, falls $\exists y \in \mathbb{K}$ so dass $yx = 1$.

Bsp: 0 ist nie invertierbar.

Lemma 8

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist [1]).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar, falls $\exists y \in \mathbb{K}$ so dass $yx = 1$.

Bsp: 0 ist nie invertierbar.

Lemma 8

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist [1]).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar, falls $\exists y \in \mathbb{K}$ so dass $yx = 1$.

Bsp: 0 ist nie invertierbar.

Lemma 8 $(\mathbb{K}, \cdot, +)$ sei ein kommutativer Ring.

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist $[1]$).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar, falls $\exists y \in \mathbb{K}$ so dass $yx = 1$.

Bsp: 0 ist nie invertierbar.

Lemma 8 $(\mathbb{K}, \cdot, +)$ sei ein kommutativer Ring. Dann ist $k \cdot 0 = 0$ (für alle $k \in \mathbb{K}$)

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist [1]).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar, falls $\exists y \in \mathbb{K}$ so dass $yx = 1$.

Bsp: 0 ist nie invertierbar.

Lemma 8 $(\mathbb{K}, \cdot, +)$ sei ein kommutativer Ring. Dann ist $k \cdot 0 = 0$ (für alle $k \in \mathbb{K}$)

Beweis:

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\mathrm{mod}\ p}{+}, \overset{\mathrm{mod}\ p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist $[1]$).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar, falls $\exists y \in \mathbb{K}$ so dass $yx = 1$.

Bsp: 0 ist nie invertierbar.

Lemma 8 $(\mathbb{K}, \cdot, +)$ sei ein kommutativer Ring. Dann ist $k \cdot 0 = 0$ (für alle $k \in \mathbb{K}$)

Beweis: $k \cdot 0 = k \cdot (0 + 0)$

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist $[1]$).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar, falls $\exists y \in \mathbb{K}$ so dass $yx = 1$.

Bsp: 0 ist nie invertierbar.

Lemma 8 $(\mathbb{K}, \cdot, +)$ sei ein kommutativer Ring. Dann ist $k \cdot 0 = 0$ (für alle $k \in \mathbb{K}$)

Beweis: $k \cdot 0 = k \cdot (0 + 0) \overset{\text{Distributivgesetz}}{=}$

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist $[1]$).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar, falls $\exists y \in \mathbb{K}$ so dass $yx = 1$.

Bsp: 0 ist nie invertierbar.

Lemma 8 $(\mathbb{K}, \cdot, +)$ sei ein kommutativer Ring. Dann ist $k \cdot 0 = 0$ (für alle $k \in \mathbb{K}$)

Beweis: $k \cdot 0 = k \cdot (0 + 0) \overset{\text{Distributivgesetz}}{=} k \cdot 0 + k \cdot 0 \qquad (*)$

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist $[1]$).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar, falls $\exists y \in \mathbb{K}$ so dass $yx = 1$.

Bsp: 0 ist nie invertierbar.

Lemma 8 $(\mathbb{K}, \cdot, +)$ sei ein kommutativer Ring. Dann ist $k \cdot 0 = 0$ (für alle $k \in \mathbb{K}$)

Beweis: $k \cdot 0 = k \cdot (0 + 0) \overset{\text{Distributivgesetz}}{=} k \cdot 0 + k \cdot 0 \qquad (*)$.
Wir addiren $-(0 \cdot k)$

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist $[1]$).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar, falls $\exists y \in \mathbb{K}$ so dass $yx = 1$.

Bsp: 0 ist nie invertierbar.

Lemma 8 $(\mathbb{K}, \cdot, +)$ sei ein kommutativer Ring. Dann ist $k \cdot 0 = 0$ (für alle $k \in \mathbb{K}$)

Beweis: $k \cdot 0 = k \cdot (0 + 0) \overset{\text{Distributivgesetz}}{=} k \cdot 0 + k \cdot 0 \qquad (*)$.
Wir addiren $-(0 \cdot k)$ zu den Seiten der Gleichung $(*)$:

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist $[1]$).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar, falls $\exists y \in \mathbb{K}$ so dass $yx = 1$.

Bsp: 0 ist nie invertierbar.

Lemma 8 $(\mathbb{K}, \cdot, +)$ sei ein kommutativer Ring. Dann ist $k \cdot 0 = 0$ (für alle $k \in \mathbb{K}$)

Beweis: $k \cdot 0 = k \cdot (0 + 0) \overset{\text{Distributivgesetz}}{=} k \cdot 0 + k \cdot 0 \qquad (*)$.
Wir addiren $-(0 \cdot k)$ zu den Seiten der Gleichung $(*)$: $0 = k \cdot 0$.

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist $[1]$).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar, falls $\exists y \in \mathbb{K}$ so dass $yx = 1$.

Bsp: 0 ist nie invertierbar.

Lemma 8 $(\mathbb{K}, \cdot, +)$ sei ein kommutativer Ring. Dann ist $k \cdot 0 = 0$ (für alle $k \in \mathbb{K}$)

Beweis: $k \cdot 0 = k \cdot (0 + 0) \overset{\text{Distributivgesetz}}{=} k \cdot 0 + k \cdot 0 \qquad (*)$.
Wir addiren $-(0 \cdot k)$ zu den Seiten der Gleichung $(*)$: $0 = k \cdot 0$. □

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist $[1]$).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar, falls $\exists y \in \mathbb{K}$ so dass $yx = 1$.

Bsp: 0 ist nie invertierbar.

Lemma 8 $(\mathbb{K}, \cdot, +)$ sei ein kommutativer Ring. Dann ist $k \cdot 0 = 0$ (für alle $k \in \mathbb{K}$)

Beweis: $k \cdot 0 = k \cdot (0 + 0) \overset{\text{Distributivgesetz}}{=} k \cdot 0 + k \cdot 0 \qquad (*)$.
Wir addiren $-(0 \cdot k)$ zu den Seiten der Gleichung $(*)$: $0 = k \cdot 0$. □

Bsp:

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist $[1]$).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar, falls $\exists y \in \mathbb{K}$ so dass $yx = 1$.

Bsp: 0 ist nie invertierbar.

Lemma 8 $(\mathbb{K}, \cdot, +)$ sei ein kommutativer Ring. Dann ist $k \cdot 0 = 0$ (für alle $k \in \mathbb{K}$)

Beweis: $k \cdot 0 = k \cdot (0 + 0) \overset{\text{Distributivgesetz}}{=} k \cdot 0 + k \cdot 0 \qquad (*)$.
Wir addiren $-(0 \cdot k)$ zu den Seiten der Gleichung $(*)$: $0 = k \cdot 0$. □

Bsp: In $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind alle Elemente außer 0 invertierbar.

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist $[1]$).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar, falls $\exists y \in \mathbb{K}$ so dass $yx = 1$.

Bsp: 0 ist nie invertierbar.

Lemma 8 $(\mathbb{K}, \cdot, +)$ sei ein kommutativer Ring. Dann ist $k \cdot 0 = 0$ (für alle $k \in \mathbb{K}$)

Beweis: $k \cdot 0 = k \cdot (0 + 0) \overset{\text{Distributivgesetz}}{=} k \cdot 0 + k \cdot 0 \qquad (*)$.
Wir addiren $-(0 \cdot k)$ zu den Seiten der Gleichung $(*)$: $0 = k \cdot 0$. □

Bsp: In $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind alle Elemente außer 0 invertierbar.

Bsp:

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist $[1]$).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar, falls $\exists y \in \mathbb{K}$ so dass $yx = 1$.

Bsp: 0 ist nie invertierbar.

Lemma 8 $(\mathbb{K}, \cdot, +)$ sei ein kommutativer Ring. Dann ist $k \cdot 0 = 0$ (für alle $k \in \mathbb{K}$)

Beweis: $k \cdot 0 = k \cdot (0 + 0) \overset{\text{Distributivgesetz}}{=} k \cdot 0 + k \cdot 0 \qquad (*)$.
Wir addiren $-(0 \cdot k)$ zu den Seiten der Gleichung $(*)$: $0 = k \cdot 0$. □

Bsp: In $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind alle Elemente außer 0 invertierbar.

Bsp: In $(\mathbb{Z}_4, \overset{\text{mod } 4}{+}, \overset{\text{mod } 4}{\cdot})$

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist $[1]$).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar, falls $\exists y \in \mathbb{K}$ so dass $yx = 1$.

Bsp: 0 ist nie invertierbar.

Lemma 8 $(\mathbb{K}, \cdot, +)$ sei ein kommutativer Ring. Dann ist $k \cdot 0 = 0$ (für alle $k \in \mathbb{K}$)

Beweis: $k \cdot 0 = k \cdot (0 + 0) \overset{\text{Distributivgesetz}}{=} k \cdot 0 + k \cdot 0 \qquad (*)$.
Wir addiren $-(0 \cdot k)$ zu den Seiten der Gleichung $(*)$: $0 = k \cdot 0$. □

Bsp: In $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind alle Elemente außer 0 invertierbar.

Bsp: In $(\mathbb{Z}_4, \overset{\text{mod } 4}{+}, \overset{\text{mod } 4}{\cdot})$ sind
[1], [3] invertierbar

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist $[1]$).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar, falls $\exists y \in \mathbb{K}$ so dass $yx = 1$.

Bsp: 0 ist nie invertierbar.

Lemma 8 $(\mathbb{K}, \cdot, +)$ sei ein kommutativer Ring. Dann ist $k \cdot 0 = 0$ (für alle $k \in \mathbb{K}$)

Beweis: $k \cdot 0 = k \cdot (0 + 0) \overset{\text{Distributivgesetz}}{=} k \cdot 0 + k \cdot 0 \qquad (*)$.
Wir addiren $-(0 \cdot k)$ zu den Seiten der Gleichung $(*)$: $0 = k \cdot 0$. □

Bsp: In $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind alle Elemente außer 0 invertierbar.

Bsp: In $(\mathbb{Z}_4, \overset{\text{mod } 4}{+}, \overset{\text{mod } 4}{\cdot})$ sind
$[1], [3]$ invertierbar $\quad$ (weil $[1] \cdot [1] = [1]$, $[3] \cdot [3] = [1]$)

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist $[1]$).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar, falls $\exists y \in \mathbb{K}$ so dass $yx = 1$.

Bsp: 0 ist nie invertierbar.

Lemma 8 $(\mathbb{K}, \cdot, +)$ sei ein kommutativer Ring. Dann ist $k \cdot 0 = 0$ (für alle $k \in \mathbb{K}$)

Beweis: $k \cdot 0 = k \cdot (0 + 0) \overset{\text{Distributivgesetz}}{=} k \cdot 0 + k \cdot 0 \qquad (*)$.
Wir addiren $-(0 \cdot k)$ zu den Seiten der Gleichung $(*)$: $0 = k \cdot 0$. □

Bsp: In $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind alle Elemente außer 0 invertierbar.

Bsp: In $(\mathbb{Z}_4, \overset{\text{mod } 4}{+}, \overset{\text{mod } 4}{\cdot})$ sind
$[1]$, $[3]$ invertierbar (weil $[1] \cdot [1] = [1]$, $[3] \cdot [3] = [1]$)
$[0]$, $[2]$ nicht invertierbar

Def 14 Besitzt ein Ring $(\mathbb{K}, +, \cdot)$ ein neutrales Element bezüglich der Multiplikation, so nennt man dieses das Einselement des Ringes (Bez. 1):
$\forall a \in \mathbb{K} \quad 1 \cdot a = a \cdot 1 = a$.
Ein Ring mit Einselement wird unitärer Ring genannt.

Bsp: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_q, \overset{\text{mod } p}{+}, \overset{\text{mod } p}{\cdot})$ sind unitäre Ringen. (1 in $\mathbb{Z}_q$ ist $[1]$).

Def 15 Sei $(\mathbb{K}, +, \cdot)$ ein unitärer kommutativer Ring. Ein $x \in \mathbb{K}$ heißt invertierbar, falls $\exists y \in \mathbb{K}$ so dass $yx = 1$.

Bsp: 0 ist nie invertierbar.

Lemma 8 $(\mathbb{K}, \cdot, +)$ sei ein kommutativer Ring. Dann ist $k \cdot 0 = 0$ (für alle $k \in \mathbb{K}$)

Beweis: $k \cdot 0 = k \cdot (0 + 0) \overset{\text{Distributivgesetz}}{=} k \cdot 0 + k \cdot 0 \qquad (*)$.
Wir addiren $-(0 \cdot k)$ zu den Seiten der Gleichung $(*)$: $0 = k \cdot 0$. □

Bsp: In $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind alle Elemente außer 0 invertierbar.

Bsp: In $(\mathbb{Z}_4, \overset{\text{mod } 4}{+}, \overset{\text{mod } 4}{\cdot})$ sind
$[1]$, $[3]$ invertierbar (weil $[1] \cdot [1] = [1]$, $[3] \cdot [3] = [1]$)
$[0]$, $[2]$ nicht invertierbar (weil $[1] \cdot [2] = [2] \neq [1]$, $[2] \cdot [2] = [0] \neq [1]$, $[2] \cdot [3] = [2] \neq [1]$.) .

Lemma 9

Lemma 9 $(\mathbb{K}, \cdot, +)$ sei ein unitärer kommutativer Ring.

Lemma 9 $(\mathbb{K}, \cdot, +)$ sei ein unitärer kommutativer Ring. Dann ist die Menge $\mathbb{K}^*$

Lemma 9 $(\mathbb{K}, \cdot, +)$ sei ein unitärer kommutativer Ring. Dann ist die Menge $\mathbb{K}^*$ von invertierbaren Elementen eine abel'sche

Lemma 9 $(\mathbb{K}, \cdot, +)$ sei ein unitärer kommutativer Ring. Dann ist die Menge $\mathbb{K}^*$ von invertierbaren Elementen eine abel'sche Gruppe bzgl. „$\cdot$„

Beweis:

Lemma 9 $(\mathbb{K}, \cdot, +)$ sei ein unitärer kommutativer Ring. Dann ist die Menge $\mathbb{K}^*$ von invertierbaren Elementen eine abel'sche Gruppe bzgl. „$\cdot$„

Beweis: Die Menge $\mathbb{K}^*$ ist $\neq \varnothing$:

Lemma 9 $(\mathbb{K}, \cdot, +)$ sei ein unitärer kommutativer Ring. Dann ist die Menge $\mathbb{K}^*$ von invertierbaren Elementen eine abel'sche Gruppe bzgl. „$\cdot$„

Beweis: Die Menge $\mathbb{K}^*$ ist $\neq \varnothing$: tatsächich, $1 \in \mathbb{K}^*$,

Lemma 9 $(\mathbb{K}, \cdot, +)$ sei ein unitärer kommutativer Ring. Dann ist die Menge $\mathbb{K}^*$ von invertierbaren Elementen eine abel'sche Gruppe bzgl. „$\cdot$„
Beweis: Die Menge $\mathbb{K}^*$ ist $\neq \varnothing$: tatsächich, $1 \in \mathbb{K}^*$, weil $1 \cdot 1 = 1$.
Die Verknüpfung „$\cdot$„ beschränkt auf $\mathbb{K}^*$ ist wohldefiniert:

Lemma 9 $(\mathbb{K}, \cdot, +)$ sei ein unitärer kommutativer Ring. Dann ist die Menge $\mathbb{K}^*$ von invertierbaren Elementen eine abel'sche Gruppe bzgl. „$\cdot$„

Beweis: Die Menge $\mathbb{K}^*$ ist $\neq \varnothing$: tatsächich, $1 \in \mathbb{K}^*$, weil $1 \cdot 1 = 1$.
Die Verknüpfung „$\cdot$„ beschränkt auf $\mathbb{K}^*$ ist wohldefiniert:
$a, b \in \mathbb{K}^*$,

Lemma 9 $(\mathbb{K}, \cdot, +)$ sei ein unitärer kommutativer Ring. Dann ist die Menge $\mathbb{K}^*$ von invertierbaren Elementen eine abel'sche Gruppe bzgl. „$\cdot$„

Beweis: Die Menge $\mathbb{K}^*$ ist $\neq \varnothing$: tatsächich, $1 \in \mathbb{K}^*$, weil $1 \cdot 1 = 1$.
Die Verknüpfung „$\cdot$„ beschränkt auf $\mathbb{K}^*$ ist wohldefiniert:
$a, b \in \mathbb{K}^*$, so ist $a \cdot b \in \mathbb{K}^*$.

Lemma 9 $(\mathbb{K}, \cdot, +)$ sei ein unitärer kommutativer Ring. Dann ist die Menge $\mathbb{K}^*$ von invertierbaren Elementen eine abel'sche Gruppe bzgl. „$\cdot$„
Beweis: Die Menge $\mathbb{K}^*$ ist $\neq \varnothing$: tatsächich, $1 \in \mathbb{K}^*$, weil $1 \cdot 1 = 1$.
Die Verknüpfung „$\cdot$„ beschränkt auf $\mathbb{K}^*$ ist wohldefiniert:
$a, b \in \mathbb{K}^*$, so ist $a \cdot b \in \mathbb{K}^*$. Tatsächlich, $b^{-1} \cdot a^{-1}$ ist inverses Element zu ab:

Lemma 9 $(\mathbb{K}, \cdot, +)$ sei ein unitärer kommutativer Ring. Dann ist die Menge $\mathbb{K}^*$ von invertierbaren Elementen eine abel'sche Gruppe bzgl. „$\cdot$„
Beweis: Die Menge $\mathbb{K}^*$ ist $\neq \varnothing$: tatsächich, $1 \in \mathbb{K}^*$, weil $1 \cdot 1 = 1$.
Die Verknüpfung „$\cdot$„ beschränkt auf $\mathbb{K}^*$ ist wohldefiniert:
$a, b \in \mathbb{K}^*$, so ist $a \cdot b \in \mathbb{K}^*$. Tatsächlich, $b^{-1} \cdot a^{-1}$ ist inverses Element zu ab:
$b^{-1} \cdot a^{-1} ab = 1$.

Lemma 9 $(\mathbb{K}, \cdot, +)$ sei ein unitärer kommutativer Ring. Dann ist die Menge $\mathbb{K}^*$ von invertierbaren Elementen eine abel'sche Gruppe bzgl. „$\cdot$„
Beweis: Die Menge $\mathbb{K}^*$ ist $\neq \varnothing$: tatsächich, $1 \in \mathbb{K}^*$, weil $1 \cdot 1 = 1$.
Die Verknüpfung „$\cdot$„ beschränkt auf $\mathbb{K}^*$ ist wohldefiniert:
$a, b \in \mathbb{K}^*$, so ist $a \cdot b \in \mathbb{K}^*$. Tatsächlich, $b^{-1} \cdot a^{-1}$ ist inverses Element zu ab:
$b^{-1} \cdot a^{-1} ab = 1$.
Wir zeigen,

Lemma 9 $(\mathbb{K}, \cdot, +)$ sei ein unitärer kommutativer Ring. Dann ist die Menge $\mathbb{K}^*$ von invertierbaren Elementen eine abel'sche Gruppe bzgl. „$\cdot$„
Beweis: Die Menge $\mathbb{K}^*$ ist $\neq \varnothing$: tatsächich, $1 \in \mathbb{K}^*$, weil $1 \cdot 1 = 1$.
Die Verknüpfung „$\cdot$„ beschränkt auf $\mathbb{K}^*$ ist wohldefiniert:
$a, b \in \mathbb{K}^*$, so ist $a \cdot b \in \mathbb{K}^*$. Tatsächlich, $b^{-1} \cdot a^{-1}$ ist inverses Element zu ab:
$b^{-1} \cdot a^{-1} ab = 1$.
Wir zeigen, dass $(\mathbb{K}^*, \cdot)$ die Gruppeneigenschaften G1, G2, G3, G4 erfüllt:

Lemma 9 $(\mathbb{K}, \cdot, +)$ sei ein unitärer kommutativer Ring. Dann ist die Menge $\mathbb{K}^*$ von invertierbaren Elementen eine abel'sche Gruppe bzgl. „$\cdot$„
Beweis: Die Menge $\mathbb{K}^*$ ist $\neq \varnothing$: tatsächich, $1 \in \mathbb{K}^*$, weil $1 \cdot 1 = 1$.
Die Verknüpfung „$\cdot$„ beschränkt auf $\mathbb{K}^*$ ist wohldefiniert:
$a, b \in \mathbb{K}^*$, so ist $a \cdot b \in \mathbb{K}^*$. Tatsächlich, $b^{-1} \cdot a^{-1}$ ist inverses Element zu ab:
$b^{-1} \cdot a^{-1} ab = 1$.
Wir zeigen, dass $(\mathbb{K}^*, \cdot)$ die Gruppeneigenschaften G1, G2, G3, G4 erfüllt:

(G1) $\Longleftarrow$ (R2)

Lemma 9 $(\mathbb{K}, \cdot, +)$ sei ein unitärer kommutativer Ring. Dann ist die Menge $\mathbb{K}^*$ von invertierbaren Elementen eine abel'sche Gruppe bzgl. „$\cdot$„
Beweis: Die Menge $\mathbb{K}^*$ ist $\neq \varnothing$: tatsächich, $1 \in \mathbb{K}^*$, weil $1 \cdot 1 = 1$.
Die Verknüpfung „$\cdot$„ beschränkt auf $\mathbb{K}^*$ ist wohldefiniert:
$a, b \in \mathbb{K}^*$, so ist $a \cdot b \in \mathbb{K}^*$. Tatsächlich, $b^{-1} \cdot a^{-1}$ ist inverses Element zu ab:
$b^{-1} \cdot a^{-1} ab = 1$.
Wir zeigen, dass $(\mathbb{K}^*, \cdot)$ die Gruppeneigenschaften G1, G2, G3, G4 erfüllt:

(G1) $\Longleftarrow$ (R2)

(G2) $\Longleftarrow$ $1 \in \mathbb{K}^*$

Lemma 9 $(\mathbb{K}, \cdot, +)$ sei ein unitärer kommutativer Ring. Dann ist die Menge $\mathbb{K}^*$ von invertierbaren Elementen eine abel'sche Gruppe bzgl. „$\cdot$„

Beweis: Die Menge $\mathbb{K}^*$ ist $\neq \varnothing$: tatsächich, $1 \in \mathbb{K}^*$, weil $1 \cdot 1 = 1$.

Die Verknüpfung „$\cdot$„ beschränkt auf $\mathbb{K}^*$ ist wohldefiniert:

$a, b \in \mathbb{K}^*$, so ist $a \cdot b \in \mathbb{K}^*$. Tatsächlich, $b^{-1} \cdot a^{-1}$ ist inverses Element zu ab:

$b^{-1} \cdot a^{-1} ab = 1$.

Wir zeigen, dass $(\mathbb{K}^*, \cdot)$ die Gruppeneigenschaften G1, G2, G3, G4 erfüllt:

(G1) $\Longleftarrow$ (R2)

(G2) $\Longleftarrow$ $1 \in \mathbb{K}^*$

(G3) $\Longleftarrow$ Def. 15.

Lemma 9 $(\mathbb{K}, \cdot, +)$ sei ein unitärer kommutativer Ring. Dann ist die Menge $\mathbb{K}^*$ von invertierbaren Elementen eine abel'sche Gruppe bzgl. „$\cdot$„

Beweis: Die Menge $\mathbb{K}^*$ ist $\neq \varnothing$: tatsächich, $1 \in \mathbb{K}^*$, weil $1 \cdot 1 = 1$.

Die Verknüpfung „$\cdot$„ beschränkt auf $\mathbb{K}^*$ ist wohldefiniert:

$a, b \in \mathbb{K}^*$, so ist $a \cdot b \in \mathbb{K}^*$. Tatsächlich, $b^{-1} \cdot a^{-1}$ ist inverses Element zu ab:

$b^{-1} \cdot a^{-1} ab = 1$.

Wir zeigen, dass $(\mathbb{K}^*, \cdot)$ die Gruppeneigenschaften G1, G2, G3, G4 erfüllt:

(G1) $\Longleftarrow$ (R2)

(G2) $\Longleftarrow$ $1 \in \mathbb{K}^*$

(G3) $\Longleftarrow$ Def. 15.

(G4) $\Longleftarrow$ (R2)

Lemma 9 $(\mathbb{K}, \cdot, +)$ sei ein unitärer kommutativer Ring. Dann ist die Menge $\mathbb{K}^*$ von invertierbaren Elementen eine abel'sche Gruppe bzgl. „$\cdot$„
Beweis: Die Menge $\mathbb{K}^*$ ist $\neq \varnothing$: tatsächich, $1 \in \mathbb{K}^*$, weil $1 \cdot 1 = 1$.
Die Verknüpfung „$\cdot$„ beschränkt auf $\mathbb{K}^*$ ist wohldefiniert:
$a, b \in \mathbb{K}^*$, so ist $a \cdot b \in \mathbb{K}^*$. Tatsächlich, $b^{-1} \cdot a^{-1}$ ist inverses Element zu ab:
$b^{-1} \cdot a^{-1} ab = 1$.
Wir zeigen, dass $(\mathbb{K}^*, \cdot)$ die Gruppeneigenschaften G1, G2, G3, G4 erfüllt:

(G1) $\Longleftarrow$ (R2)

(G2) $\Longleftarrow$ $1 \in \mathbb{K}^*$

(G3) $\Longleftarrow$ Def. 15.

(G4) $\Longleftarrow$ (R2) □

Def. 16

Def. 16 *Seien* $a, b \in \mathbb{Z}$.

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler*

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a, b)$ *)*

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a, b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a, b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$.

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a, b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a, b)$ *existiert g.d.w.* $(a, b) \neq (0, 0)$.

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a, b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a, b)$ *existiert g.d.w.* $(a, b) \neq (0, 0)$. *Ist* $ggT(a, b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a, b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a, b)$ *existiert g.d.w.* $(a, b) \neq (0, 0)$. *Ist* $ggT(a, b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a, b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a, b)$ *existiert g.d.w.* $(a, b) \neq (0, 0)$. *Ist* $ggT(a, b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$.

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a, b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a, b)$ *existiert g.d.w.* $(a, b) \neq (0, 0)$. *Ist* $ggT(a, b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$. *Dann gilt:*

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a, b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a, b)$ *existiert g.d.w.* $(a, b) \neq (0, 0)$. *Ist* $ggT(a, b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a, b)$.

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a, b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a, b)$ *existiert g.d.w.* $(a, b) \neq (0, 0)$. *Ist* $ggT(a, b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a, b)$.

Wir beweisen zuerst: $(*)$ $ggT(a, b) = ggT(a - b, b)$.

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a, b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a, b)$ *existiert g.d.w.* $(a, b) \neq (0, 0)$. *Ist* $ggT(a, b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a, b)$.

Wir beweisen zuerst: $(*)$ $ggT(a, b) = ggT(a - b, b)$.

Tatsächlich,

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a, b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a, b)$ *existiert g.d.w.* $(a, b) \neq (0, 0)$. *Ist* $ggT(a, b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a, b)$.

Wir beweisen zuerst: $(*)$ $ggT(a, b) = ggT(a - b, b)$.

Tatsächlich, $a \vdots x$ und $b \vdots x \Rightarrow a - b \vdots x$

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $b \vdots x \Rightarrow a - b \vdots x$

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x}$ $\Rightarrow$ $\underset{}{a-b \vdots x}$

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x}$ $\Rightarrow$ $\underset{(k_1 - k_2)x = a - b,}{a - b \vdots x}$

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x} \Rightarrow \underset{(k_1 - k_2)x = a - b,}{a - b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a - b, b$ sind gleich.

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a, b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a, b)$ *existiert g.d.w.* $(a, b) \neq (0, 0)$. *Ist* $ggT(a, b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a, b)$.

Wir beweisen zuerst: $(*)$ $ggT(a, b) = ggT(a - b, b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x}$ $\Rightarrow$ $\underset{(k_1 - k_2)x = a - b,}{a - b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a - b, b$ sind gleich.

Beweis des Satzes:

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x}$ $\Rightarrow$ $\underset{(k_1 - k_2)x = a - b,}{a-b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a-b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$.

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x}$ $\Rightarrow$ $\underset{(k_1 - k_2)x = a - b,}{a-b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a-b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x}$ $\Rightarrow$ $\underset{(k_1 - k_2)x = a - b,}{a-b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a-b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

IA

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x} \Rightarrow \underset{(k_1 - k_2)x = a - b,}{a - b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a - b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

IA Falls $N = a + b = 2$,

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x} \Rightarrow \underset{(k_1 - k_2)x = a - b,}{a - b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a - b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x} \Rightarrow \underset{(k_1 - k_2)x = a - b,}{a - b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a - b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

IV

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x}$ $\Rightarrow$ $\underset{(k_1 - k_2)x = a - b,}{a-b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a - b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

IV Angenommen für alle $a, b \in \mathbb{Z}$,

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x} \Rightarrow \underset{(k_1 - k_2)x = a - b,}{a-b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a-b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

IV Angenommen für alle $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$, $a + b \leq N$

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x} \Rightarrow \underset{(k_1 - k_2)x = a - b,}{a-b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a - b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

IV Angenommen für alle $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$, $a + b \leq N$ gibt es n, m

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x}$ $\Rightarrow$ $\underset{(k_1 - k_2)x = a - b,}{a - b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a - b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

IV Angenommen für alle $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$, $a + b \leq N$ gibt es n, m s.d. $na + bm = ggT(a,b)$.

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x} \Rightarrow \underset{(k_1 - k_2)x = a - b,}{a - b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a - b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

IV Angenommen für alle $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$, $a + b \leq N$ gibt es n, m s.d. $na + bm = ggT(a,b)$.

IS

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x} \Rightarrow \underset{(k_1 - k_2)x = a - b,}{a - b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a - b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

IV Angenommen für alle $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$, $a + b \leq N$ gibt es n, m s.d. $na + bm = ggT(a,b)$.

IS Z.z.:

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x}$ $\Rightarrow$ $\underset{(k_1 - k_2)x = a - b,}{a - b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a - b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

IV Angenommen für alle $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$, $a + b \leq N$ gibt es n, m s.d. $na + bm = ggT(a,b)$.

IS Z.z.: Für alle $a, b \in \mathbb{Z}$, $a > 0$ $b > 0$, $a + b = N + 1$

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x}$ $\Rightarrow$ $\underset{(k_1 - k_2)x = a - b,}{a - b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a - b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

IV Angenommen für alle $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$, $a + b \leq N$ gibt es n, m s.d. $na + bm = ggT(a,b)$.

IS Z.z.: Für alle $a, b \in \mathbb{Z}$, $a > 0$ $b > 0$, $a + b = N + 1$ gibt es n, m s.d. $na + bm = ggT(a,b)$.

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x}$ $\Rightarrow$ $\underset{(k_1 - k_2)x = a - b,}{a - b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a - b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

IV Angenommen für alle $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$, $a + b \leq N$ gibt es n, m s.d. $na + bm = ggT(a,b)$.

IS Z.z.: Für alle $a, b \in \mathbb{Z}$, $a > 0$ $b > 0$, $a + b = N + 1$ gibt es n, m s.d. $na + bm = ggT(a,b)$.

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x}$ $\Rightarrow$ $\underset{(k_1 - k_2)x = a - b,}{a - b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a - b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

IV Angenommen für alle $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$, $a + b \leq N$ gibt es n, m s.d. $na + bm = ggT(a,b)$.

IS Z.z.: Für alle $a, b \in \mathbb{Z}$, $a > 0$ $b > 0$, $a + b = N + 1$ gibt es n, m s.d. $na + bm = ggT(a,b)$.

Ist $a = b$, so ist die Aussage offensichlich:

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x}$ $\Rightarrow$ $\underset{(k_1 - k_2)x = a - b,}{a - b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a - b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

IV Angenommen für alle $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$, $a + b \leq N$ gibt es n, m s.d. $na + bm = ggT(a,b)$.

IS Z.z.: Für alle $a, b \in \mathbb{Z}$, $a > 0$ $b > 0$, $a + b = N + 1$ gibt es n, m s.d. $na + bm = ggT(a,b)$.

Ist $a = b$, so ist die Aussage offensichlich: $1 \cdot a + 0 \cdot b = ggT(a,b)$.

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x}$ $\Rightarrow$ $\underset{(k_1 - k_2)x = a - b,}{a - b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a - b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

IV Angenommen für alle $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$, $a + b \leq N$ gibt es n, m s.d. $na + bm = ggT(a,b)$.

IS Z.z.: Für alle $a, b \in \mathbb{Z}$, $a > 0$ $b > 0$, $a + b = N + 1$ gibt es n, m s.d. $na + bm = ggT(a,b)$.

Ist $a = b$, so ist die Aussage offensichlich: $1 \cdot a + 0 \cdot b = ggT(a,b)$.

Angennomen,

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x}$ $\Rightarrow$ $\underset{(k_1 - k_2)x = a - b,}{a - b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a - b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

IV Angenommen für alle $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$, $a + b \leq N$ gibt es n, m s.d. $na + bm = ggT(a,b)$.

IS Z.z.: Für alle $a, b \in \mathbb{Z}$, $a > 0$ $b > 0$, $a + b = N + 1$ gibt es n, m s.d. $na + bm = ggT(a,b)$.

Ist $a = b$, so ist die Aussage offensichlich: $1 \cdot a + 0 \cdot b = ggT(a,b)$.

Angennomen, $a \neq b$,

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x}$ $\Rightarrow$ $\underset{(k_1 - k_2)x = a - b,}{a - b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a - b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

IV Angenommen für alle $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$, $a + b \leq N$ gibt es n, m s.d. $na + bm = ggT(a,b)$.

IS Z.z.: Für alle $a, b \in \mathbb{Z}$, $a > 0$ $b > 0$, $a + b = N + 1$ gibt es n, m s.d. $na + bm = ggT(a,b)$.

Ist $a = b$, so ist die Aussage offensichlich: $1 \cdot a + 0 \cdot b = ggT(a,b)$.

Angennomen, $a \neq b$, oBdA sei $a > b$.

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x}$ $\Rightarrow$ $\underset{(k_1 - k_2)x = a - b,}{a-b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a-b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

IV Angenommen für alle $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$, $a + b \leq N$ gibt es n, m s.d. $na + bm = ggT(a,b)$.

IS Z.z.: Für alle $a, b \in \mathbb{Z}$, $a > 0$ $b > 0$, $a + b = N + 1$ gibt es n, m s.d. $na + bm = ggT(a,b)$.

Ist $a = b$, so ist die Aussage offensichlich: $1 \cdot a + 0 \cdot b = ggT(a,b)$.

Angennomen, $a \neq b$, oBdA sei $a > b$. Nach (IV) gibt es n, m_1 s.d.

$n \cdot (a-b) + m_1 \cdot b = ggT(a-b,b) \overset{(*)}{=} ggT(a,b)$.

Def. 16 *Seien $a, b \in \mathbb{Z}$. Grösster gemeinsamer Teiler von a, b (Bezeichnung: $ggT(a, b)$) ist die grosste Zahl $m \in \mathbb{N}$ s.d. $a \vdots m$ und $b \vdots m$. $ggT(a, b)$ existiert g.d.w. $(a, b) \neq (0, 0)$. Ist $ggT(a, b) = 1$, so heißen a und b Teilerfremd.*

Satz 18 *Seien $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$. Dann gilt: $\exists n, m \in \mathbb{Z}$ s.d. $na + mb = ggT(a, b)$.*

Wir beweisen zuerst: $(*)$ $ggT(a, b) = ggT(a - b, b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x} \Rightarrow \underset{(k_1 - k_2)x = a - b,}{a - b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a - b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

IV Angenommen für alle $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$, $a + b \leq N$ gibt es n, m s.d. $na + bm = ggT(a, b)$.

IS Z.z.: Für alle $a, b \in \mathbb{Z}$, $a > 0$ $b > 0$, $a + b = N + 1$ gibt es n, m s.d. $na + bm = ggT(a, b)$.

Ist $a = b$, so ist die Aussage offensichlich: $1 \cdot a + 0 \cdot b = ggT(a, b)$.

Angennomen, $a \neq b$, oBdA sei $a > b$. Nach (IV) gibt es n, m_1 s.d.

$n \cdot (a - b) + m_1 \cdot b = ggT(a - b, b) \overset{(*)}{=} ggT(a, b)$. Also,

$na + \underbrace{(m_1 - n_1)}$

Def. 16 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grosste Zahl* $m \in \mathbb{N}$ *s.d.* $a \vdots m$ *und* $b \vdots m$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *Teilerfremd.*

Satz 18 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt:* $\exists n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst: $(*)$ $ggT(a,b) = ggT(a-b,b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x}$ $\Rightarrow$ $\underset{(k_1 - k_2)x = a - b,}{a-b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a-b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

IV Angenommen für alle $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$, $a + b \leq N$ gibt es n, m s.d. $na + bm = ggT(a,b)$.

IS Z.z.: Für alle $a, b \in \mathbb{Z}$, $a > 0$ $b > 0$, $a + b = N + 1$ gibt es n, m s.d. $na + bm = ggT(a,b)$.

Ist $a = b$, so ist die Aussage offensichlich: $1 \cdot a + 0 \cdot b = ggT(a,b)$.

Angennomen, $a \neq b$, oBdA sei $a > b$. Nach (IV) gibt es n, m_1 s.d.

$n \cdot (a-b) + m_1 \cdot b = ggT(a-b,b) \overset{(*)}{=} ggT(a,b)$. Also,

$na + \underbrace{(m_1 - n_1)}_{m} b = ggT(a,b)$,

Def. 16 *Seien $a, b \in \mathbb{Z}$. Grösster gemeinsamer Teiler von a, b (Bezeichnung: $ggT(a, b)$) ist die grosste Zahl $m \in \mathbb{N}$ s.d. $a \vdots m$ und $b \vdots m$. $ggT(a, b)$ existiert g.d.w. $(a, b) \neq (0, 0)$. Ist $ggT(a, b) = 1$, so heißen a und b Teilerfremd.*

Satz 18 *Seien $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$. Dann gilt: $\exists n, m \in \mathbb{Z}$ s.d. $na + mb = ggT(a, b)$.*

Wir beweisen zuerst: $(*)$ $ggT(a, b) = ggT(a - b, b)$.

Tatsächlich, $\underset{k_1 x = a}{a \vdots x}$ und $\underset{k_2 x = b}{b \vdots x}$ $\Rightarrow$ $\underset{(k_1 - k_2)x = a - b,}{a - b \vdots x}$ also die Menge von gemeisamen Teiler vom Paar a, b und vom Paar $a - b, b$ sind gleich.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion nach $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

IV Angenommen für alle $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$, $a + b \leq N$ gibt es n, m s.d. $na + bm = ggT(a, b)$.

IS Z.z.: Für alle $a, b \in \mathbb{Z}$, $a > 0$ $b > 0$, $a + b = N + 1$ gibt es n, m s.d. $na + bm = ggT(a, b)$.

Ist $a = b$, so ist die Aussage offensichlich: $1 \cdot a + 0 \cdot b = ggT(a, b)$.

Angennomen, $a \neq b$, oBdA sei $a > b$. Nach (IV) gibt es n, m_1 s.d.

$n \cdot (a - b) + m_1 \cdot b = ggT(a - b, b) \overset{(*)}{=} ggT(a, b)$. Also,

$na + \underbrace{(m_1 - n_1)}_{m} b = ggT(a, b)$, □

Folgerung

Folgerung *In* $\mathbb{K} = \mathbb{Z}_q$ *mit* $q \geq 2$ *gilt:*

Folgerung *In* $\mathbb{K} = \mathbb{Z}_q$ *mit* $q \geq 2$ *gilt:*

$$[a] \in \mathbb{K}^* \iff ggT(a, q) = 1$$

Folgerung *In* $\mathbb{K} = \mathbb{Z}_q$ *mit* $q \geq 2$ *gilt:*
$[a] \in \mathbb{K}^* \iff ggT(a, q) = 1$
Beweis: $\Longleftarrow$

Folgerung *In* $\mathbb{K} = \mathbb{Z}_q$ *mit* $q \geq 2$ *gilt:*
$[a] \in \mathbb{K}^* \iff ggT(a, q) = 1$
Beweis: $\Longleftarrow$ Ist $ggT(q, a) = 1$,

Folgerung *In* $\mathbb{K} = \mathbb{Z}_q$ *mit* $q \geq 2$ *gilt:*
$[a] \in \mathbb{K}^* \iff ggT(a, q) = 1$
Beweis: $\Longleftarrow$ Ist $ggT(q, a) = 1$, so gibt es nach Satz 18 die Zahlen n, m mit $1 = m \cdot q + n \cdot a$.

Folgerung *In* $\mathbb{K} = \mathbb{Z}_q$ *mit* $q \geq 2$ *gilt:*
$[a] \in \mathbb{K}^* \iff ggT(a, q) = 1$
Beweis: $\Longleftarrow$ Ist $ggT(q, a) = 1$, so gibt es nach Satz 18 die Zahlen n, m mit $1 = m \cdot q + n \cdot a$. Dann

$$[1] = [m \cdot q + n \cdot a]$$

Folgerung *In* $\mathbb{K} = \mathbb{Z}_q$ *mit* $q \geq 2$ *gilt:*
$[a] \in \mathbb{K}^* \iff ggT(a, q) = 1$

Beweis: $\Longleftarrow$ Ist $ggT(q, a) = 1$, so gibt es nach Satz 18 die Zahlen n, m mit $1 = m \cdot q + n \cdot a$. Dann

$$[1] = [m \cdot q + n \cdot a] = \underbrace{[m] \overset{\text{mod } q}{\cdot} \underbrace{[q]}_{[0]}}_{= [0] \text{ nach Lem. 8}}$$

Folgerung *In* $\mathbb{K} = \mathbb{Z}_q$ *mit* $q \geq 2$ *gilt:*
$[a] \in \mathbb{K}^* \iff ggT(a, q) = 1$

Beweis: $\Longleftarrow$ Ist $ggT(q, a) = 1$, so gibt es nach Satz 18 die Zahlen n, m mit $1 = m \cdot q + n \cdot a$. Dann

$$[1] = [m \cdot q + n \cdot a] = \underbrace{[m] \overset{\text{mod } q}{\cdot} \underbrace{[q]}_{[0]}}_{= [0] \text{ nach Lem. 8}} \overset{\text{mod } q}{+} [n] \overset{\text{mod } q}{\cdot} [a] =$$

Folgerung *In* $\mathbb{K} = \mathbb{Z}_q$ *mit* $q \geq 2$ *gilt:*
$[a] \in \mathbb{K}^* \iff ggT(a, q) = 1$

Beweis: $\Longleftarrow$ Ist $ggT(q, a) = 1$, so gibt es nach Satz 18 die Zahlen n, m mit $1 = m \cdot q + n \cdot a$. Dann

$$[1] = [m \cdot q + n \cdot a] = \underbrace{[m] \overset{\text{mod } q}{\cdot} \underbrace{[q]}_{[0]}}_{= [0] \text{ nach Lem. 8}} \overset{\text{mod } q}{+} [n] \overset{\text{mod } q}{\cdot} [a] = [n] \overset{\text{mod } q}{\cdot} [a].$$

Folgerung *In* $\mathbb{K} = \mathbb{Z}_q$ *mit* $q \geq 2$ *gilt:*
$[a] \in \mathbb{K}^* \iff ggT(a, q) = 1$

Beweis: $\Longleftarrow$ Ist $ggT(q, a) = 1$, so gibt es nach Satz 18 die Zahlen n, m mit $1 = m \cdot q + n \cdot a$. Dann

$$[1] = [m \cdot q + n \cdot a] = \underbrace{[m] \overset{\text{mod } q}{\cdot} \underbrace{[q]}_{[0]}}_{= [0] \text{ nach Lem. 8}} \overset{\text{mod } q}{+} [n] \overset{\text{mod } q}{\cdot} [a] = [n] \overset{\text{mod } q}{\cdot} [a].$$

Also, $[n]$ ist das inverse Element zu $[a]$.

Folgerung *In* $\mathbb{K} = \mathbb{Z}_q$ *mit* $q \geq 2$ *gilt:*
$[a] \in \mathbb{K}^* \iff ggT(a, q) = 1$

Beweis: $\Longleftarrow$ Ist $ggT(q, a) = 1$, so gibt es nach Satz 18 die Zahlen n, m mit $1 = m \cdot q + n \cdot a$. Dann

$$[1] = [m \cdot q + n \cdot a] = \underbrace{[m] \overset{\text{mod } q}{\cdot} \underbrace{[q]}_{[0]}}_{= [0] \text{ nach Lem. 8}} \overset{\text{mod } q}{+} [n] \overset{\text{mod } q}{\cdot} [a] = [n] \overset{\text{mod } q}{\cdot} [a].$$

Also, $[n]$ ist das inverse Element zu $[a]$.

$\Longrightarrow$:

Folgerung *In* $\mathbb{K} = \mathbb{Z}_q$ *mit* $q \geq 2$ *gilt:*
$[a] \in \mathbb{K}^* \iff ggT(a, q) = 1$

Beweis: $\Longleftarrow$ Ist $ggT(q, a) = 1$, so gibt es nach Satz 18 die Zahlen n, m mit $1 = m \cdot q + n \cdot a$. Dann

$$[1] = [m \cdot q + n \cdot a] = [m] \overset{\text{mod } q}{\cdot} \underbrace{[q]}_{[0]} \overset{\text{mod } q}{+} [n] \overset{\text{mod } q}{\cdot} [a] = [n] \overset{\text{mod } q}{\cdot} [a].$$

$$\underbrace{\qquad\qquad\qquad\qquad}_{= [0] \text{ nach Lem. 8}}$$

Also, $[n]$ ist das inverse Element zu $[a]$.

$\Longrightarrow$: Angenommen, $a \in \mathbb{K}^*$,

Folgerung *In* $\mathbb{K} = \mathbb{Z}_q$ *mit* $q \geq 2$ *gilt:*
$[a] \in \mathbb{K}^* \iff ggT(a, q) = 1$

Beweis: $\Longleftarrow$ Ist $ggT(q, a) = 1$, so gibt es nach Satz 18 die Zahlen n, m mit $1 = m \cdot q + n \cdot a$. Dann

$$[1] = [m \cdot q + n \cdot a] = [m] \overset{\text{mod } q}{\cdot} \underbrace{[q]}_{[0]} \overset{\text{mod } q}{+} [n] \overset{\text{mod } q}{\cdot} [a] = [n] \overset{\text{mod } q}{\cdot} [a].$$

$$\underbrace{\qquad\qquad\qquad\qquad}_{= [0] \text{ nach Lem. 8}}$$

Also, $[n]$ ist das inverse Element zu $[a]$.

$\Longrightarrow$: Angenommen, $a \in \mathbb{K}^*$, d.h., $\exists n \in \mathbb{Z}$ mit $[n] \overset{\text{mod } q}{\cdot} [a] = [1]$.

Folgerung *In* $\mathbb{K} = \mathbb{Z}_q$ *mit* $q \geq 2$ *gilt:*
$[a] \in \mathbb{K}^* \iff ggT(a, q) = 1$

Beweis: $\Longleftarrow$ Ist $ggT(q, a) = 1$, so gibt es nach Satz 18 die Zahlen n, m mit $1 = m \cdot q + n \cdot a$. Dann

$$[1] = [m \cdot q + n \cdot a] = \underbrace{[m] \overset{\text{mod } q}{\cdot} \underbrace{[q]}_{[0]}}_{= [0] \text{ nach Lem. 8}} \overset{\text{mod } q}{+} [n] \overset{\text{mod } q}{\cdot} [a] = [n] \overset{\text{mod } q}{\cdot} [a].$$

Also, $[n]$ ist das inverse Element zu $[a]$.

$\Longrightarrow$: Angenommen, $a \in \mathbb{K}^*$, d.h., $\exists n \in \mathbb{Z}$ mit $[n] \overset{\text{mod } q}{\cdot} [a] = [1]$. Dann ist $[n \cdot a] = [1]$.

Folgerung *In* $\mathbb{K} = \mathbb{Z}_q$ *mit* $q \geq 2$ *gilt:*
$[a] \in \mathbb{K}^* \iff ggT(a, q) = 1$

Beweis: $\Longleftarrow$ Ist $ggT(q, a) = 1$, so gibt es nach Satz 18 die Zahlen n, m mit $1 = m \cdot q + n \cdot a$. Dann

$$[1] = [m \cdot q + n \cdot a] = [m] \overset{\text{mod } q}{\cdot} \underbrace{[q]}_{[0]} \overset{\text{mod } q}{+} [n] \overset{\text{mod } q}{\cdot} [a] = [n] \overset{\text{mod } q}{\cdot} [a].$$

$$\underbrace{\qquad\qquad\qquad\qquad}_{= [0] \text{ nach Lem. 8}}$$

Also, $[n]$ ist das inverse Element zu $[a]$.

$\Longrightarrow$: Angenommen, $a \in \mathbb{K}^*$, d.h., $\exists n \in \mathbb{Z}$ mit $[n] \overset{\text{mod } q}{\cdot} [a] = [1]$. Dann ist $[n \cdot a] = [1]$. Dann $n \cdot a + m \cdot q = 1$

Folgerung *In* $\mathbb{K} = \mathbb{Z}_q$ *mit* $q \geq 2$ *gilt:*
$[a] \in \mathbb{K}^* \iff ggT(a, q) = 1$

Beweis: $\Longleftarrow$ Ist $ggT(q, a) = 1$, so gibt es nach Satz 18 die Zahlen n, m mit $1 = m \cdot q + n \cdot a$. Dann

$$[1] = [m \cdot q + n \cdot a] = [m] \overset{\text{mod } q}{\cdot} \underbrace{[q]}_{[0]} \overset{\text{mod } q}{+} [n] \overset{\text{mod } q}{\cdot} [a] = [n] \overset{\text{mod } q}{\cdot} [a].$$

$$\underbrace{\qquad\qquad\qquad\qquad}_{= [0] \text{ nach Lem. 8}}$$

Also, $[n]$ ist das inverse Element zu $[a]$.

$\Longrightarrow$: Angenommen, $a \in \mathbb{K}^*$, d.h., $\exists n \in \mathbb{Z}$ mit $[n] \overset{\text{mod } q}{\cdot} [a] = [1]$. Dann ist $[n \cdot a] = [1]$. Dann $n \cdot a + m \cdot q = 1$ für ein $m \in \mathbb{Z}$.

Folgerung *In* $\mathbb{K} = \mathbb{Z}_q$ *mit* $q \geq 2$ *gilt:*
$[a] \in \mathbb{K}^* \iff ggT(a, q) = 1$

Beweis: $\Longleftarrow$ Ist $ggT(q, a) = 1$, so gibt es nach Satz 18 die Zahlen n, m mit $1 = m \cdot q + n \cdot a$. Dann

$$[1] = [m \cdot q + n \cdot a] = \underbrace{[m] \overset{\text{mod } q}{\cdot} \underbrace{[q]}_{[0]}}_{= [0] \text{ nach Lem. 8}} \overset{\text{mod } q}{+} [n] \overset{\text{mod } q}{\cdot} [a] = [n] \overset{\text{mod } q}{\cdot} [a].$$

Also, $[n]$ ist das inverse Element zu $[a]$.

$\Longrightarrow$: Angenommen, $a \in \mathbb{K}^*$, d.h., $\exists n \in \mathbb{Z}$ mit $[n] \overset{\text{mod } q}{\cdot} [a] = [1]$. Dann ist $[n \cdot a] = [1]$. Dann $n \cdot a + m \cdot q = 1$ für ein $m \in \mathbb{Z}$. □

Satz 19

Satz 19 (Kleiner Satz von Fermat  1607–1665)

Satz 19 (Kleiner Satz von Fermat  1607–1665)

Ist p eine Primzahl,

Satz 19 (Kleiner Satz von Fermat  1607–1665)

Ist p eine Primzahl, so ist $[a^{p-1}] = [1]$

Satz 19 (Kleiner Satz von Fermat  1607–1665)

Ist p eine Primzahl, so ist $[a^{p-1}] = [1]$ für jedes $[a] \in \mathbb{Z}_p \setminus \{[0]\}$.

Satz 19 (Kleiner Satz von Fermat  1607–1665)

Ist p eine Primzahl, so ist $[a^{p-1}] = [1]$ für jedes $[a] \in \mathbb{Z}_p \setminus \{[0]\}$.

Satz 19'

Satz 19 (Kleiner Satz von Fermat  1607–1665)

Ist p eine Primzahl, so ist $[a^{p-1}] = [1]$ für jedes $[a] \in \mathbb{Z}_p \setminus \{[0]\}$.

Satz 19' *Für jede Primzahl p und für jede $a \in \mathbb{Z}$ gilt:*
entweder $a \vdots p$, oder $a^{p-1} - 1 \vdots p$.

Satz 19 (Kleiner Satz von Fermat  1607–1665)

Ist p eine Primzahl, so ist $[a^{p-1}] = [1]$ für jedes $[a] \in \mathbb{Z}_p \setminus \{[0]\}$.

Satz 19' *Für jede Primzahl p und für jede $a \in \mathbb{Z}$ gilt:*
entweder $a \vdots p$, oder $a^{p-1} - 1 \vdots p$.

Beweis:

Satz 19 (Kleiner Satz von Fermat  1607–1665)

Ist p eine Primzahl, so ist $[a^{p-1}] = [1]$ für jedes $[a] \in \mathbb{Z}_p \setminus \{[0]\}$.

Satz 19' *Für jede Primzahl p und für jede $a \in \mathbb{Z}$ gilt:*
entweder $a \vdots p$, oder $a^{p-1} - 1 \vdots p$.

Beweis: Betrachte die Elemente
$a, a \overset{\text{mod } q}{\cdot} [2], a \overset{\text{mod } q}{\cdot} [3], ..., a \overset{\text{mod } q}{\cdot} [p-1]$.

Satz 19 (Kleiner Satz von Fermat  1607–1665)

Ist p eine Primzahl, so ist $[a^{p-1}] = [1]$ für jedes $[a] \in \mathbb{Z}_p \setminus \{[0]\}$.

Satz 19' *Für jede Primzahl p und für jede $a \in \mathbb{Z}$ gilt:*
entweder $a \vdots p$, oder $a^{p-1} - 1 \vdots p$.

Beweis: Betrachte die Elemente
$a, a \overset{\cdot}{}^{\mathrm{mod}\ q} [2], a \overset{\cdot}{}^{\mathrm{mod}\ q} [3], ..., a \overset{\cdot}{}^{\mathrm{mod}\ q} [p-1]$. Da $(\mathbb{Z}_p \setminus [0], \overset{\cdot}{}^{\mathrm{mod}\ q})$ nach Satz 18 und Lemma 9 eine Gruppe ist,

Satz 19 (Kleiner Satz von Fermat  1607–1665)

Ist p eine Primzahl, so ist $[a^{p-1}] = [1]$ für jedes $[a] \in \mathbb{Z}_p \setminus \{[0]\}$.

Satz 19' *Für jede Primzahl p und für jede $a \in \mathbb{Z}$ gilt:*
entweder $a \vdots p$, oder $a^{p-1} - 1 \vdots p$.

Beweis: Betrachte die Elemente
$a, a \overset{\text{mod } q}{\cdot} [2], a \overset{\text{mod } q}{\cdot} [3], ..., a \overset{\text{mod } q}{\cdot} [p-1]$. Da $(\mathbb{Z}_p \setminus [0], \overset{\text{mod } q}{\cdot})$ nach Satz 18 und Lemma 9 eine Gruppe ist, sind diese Elemente verschieden

Satz 19 (Kleiner Satz von Fermat  1607–1665)

Ist p eine Primzahl, so ist $[a^{p-1}] = [1]$ für jedes $[a] \in \mathbb{Z}_p \setminus \{[0]\}$.

Satz 19' *Für jede Primzahl p und für jede $a \in \mathbb{Z}$ gilt:*
entweder $a \vdots p$, oder $a^{p-1} - 1 \vdots p$.

Beweis: Betrachte die Elemente
$a, a \overset{\text{mod } q}{\cdot} [2], a \overset{\text{mod } q}{\cdot} [3], ..., a \overset{\text{mod } q}{\cdot} [p-1]$. Da $(\mathbb{Z}_p \setminus [0], \overset{\text{mod } q}{\cdot})$ nach Satz 18 und Lemma 9 eine Gruppe ist, sind diese Elemente verschieden (weil
$a \overset{\text{mod } q}{\cdot} b = a \overset{\text{mod } q}{\cdot} c$

Satz 19 (Kleiner Satz von Fermat  1607–1665)

Ist p eine Primzahl, so ist $[a^{p-1}] = [1]$ für jedes $[a] \in \mathbb{Z}_p \setminus \{[0]\}$.

Satz 19' *Für jede Primzahl p und für jede $a \in \mathbb{Z}$ gilt:*
entweder $a \vdots p$, oder $a^{p-1} - 1 \vdots p$.

Beweis: Betrachte die Elemente
$a, a \overset{\text{mod } q}{\cdot} [2], a \overset{\text{mod } q}{\cdot} [3], ..., a \overset{\text{mod } q}{\cdot} [p-1]$. Da $(\mathbb{Z}_p \setminus [0], \overset{\text{mod } q}{\cdot})$ nach Satz 18 und Lemma 9 eine Gruppe ist, sind diese Elemente verschieden (weil $a \overset{\text{mod } q}{\cdot} b = a \overset{\text{mod } q}{\cdot} c \overset{\text{Multiplilzieren mit } a^{-1}}{\Longrightarrow}$

Satz 19 (Kleiner Satz von Fermat  1607–1665)

Ist p eine Primzahl, so ist $[a^{p-1}] = [1]$ für jedes $[a] \in \mathbb{Z}_p \setminus \{[0]\}$.

Satz 19' *Für jede Primzahl p und für jede $a \in \mathbb{Z}$ gilt:*
entweder $a \vdots p$, oder $a^{p-1} - 1 \vdots p$.

Beweis: Betrachte die Elemente
$a, a \overset{\text{mod } q}{\cdot} [2], a \overset{\text{mod } q}{\cdot} [3], ..., a \overset{\text{mod } q}{\cdot} [p-1]$. Da $(\mathbb{Z}_p \setminus [0], \overset{\text{mod } q}{\cdot})$ nach Satz 18 und Lemma 9 eine Gruppe ist, sind diese Elemente verschieden (weil $a \overset{\text{mod } q}{\cdot} b = a \overset{\text{mod } q}{\cdot} c \overset{\text{Multiplilzieren mit } a^{-1}}{\Longrightarrow} b = c$.)

Satz 19 (Kleiner Satz von Fermat  1607–1665)

Ist p eine Primzahl, so ist $[a^{p-1}] = [1]$ für jedes $[a] \in \mathbb{Z}_p \setminus \{[0]\}$.

Satz 19' *Für jede Primzahl p und für jede $a \in \mathbb{Z}$ gilt:*
entweder $a \vdots p$, oder $a^{p-1} - 1 \vdots p$.

Beweis: Betrachte die Elemente
$a, a \overset{\text{mod } q}{\cdot} [2], a \overset{\text{mod } q}{\cdot} [3], ..., a \overset{\text{mod } q}{\cdot} [p-1]$. Da $(\mathbb{Z}_p \setminus [0], \overset{\text{mod } q}{\cdot})$ nach Satz 18 und Lemma 9 eine Gruppe ist, sind diese Elemente verschieden (weil $a \overset{\text{mod } q}{\cdot} b = a \overset{\text{mod } q}{\cdot} c \overset{\text{Multiplilzieren mit } a^{-1}}{\Longrightarrow} b = c$.) Dann sind diese Elemente genau die Elemente

Satz 19 (Kleiner Satz von Fermat  1607–1665)

Ist p eine Primzahl, so ist $[a^{p-1}] = [1]$ für jedes $[a] \in \mathbb{Z}_p \setminus \{[0]\}$.

Satz 19' *Für jede Primzahl p und für jede $a \in \mathbb{Z}$ gilt:*
entweder $a \vdots p$, oder $a^{p-1} - 1 \vdots p$.

Beweis: Betrachte die Elemente
$a, a \overset{\text{mod } q}{\cdot} [2], a \overset{\text{mod } q}{\cdot} [3], ..., a \overset{\text{mod } q}{\cdot} [p-1]$. Da $(\mathbb{Z}_p \setminus [0], \overset{\text{mod } q}{\cdot})$ nach Satz 18 und Lemma 9 eine Gruppe ist, sind diese Elemente verschieden (weil $a \overset{\text{mod } q}{\cdot} b = a \overset{\text{mod } q}{\cdot} c \overset{\text{Multiplilzieren mit } a^{-1}}{\Longrightarrow} b = c$.) Dann sind diese Elemente genau die Elemente $[1], [2], \ldots, [p-1]$,

Satz 19 (Kleiner Satz von Fermat  1607–1665)

Ist p eine Primzahl, so ist $[a^{p-1}] = [1]$ für jedes $[a] \in \mathbb{Z}_p \setminus \{[0]\}$.

Satz 19' *Für jede Primzahl p und für jede $a \in \mathbb{Z}$ gilt:*
entweder $a \vdots p$, oder $a^{p-1} - 1 \vdots p$.

Beweis: Betrachte die Elemente
$a, a \overset{\text{mod } q}{\cdot} [2], a \overset{\text{mod } q}{\cdot} [3], ..., a \overset{\text{mod } q}{\cdot} [p-1]$. Da $(\mathbb{Z}_p \setminus [0], \overset{\text{mod } q}{\cdot})$ nach Satz 18 und Lemma 9 eine Gruppe ist, sind diese Elemente verschieden (weil $a \overset{\text{mod } q}{\cdot} b = a \overset{\text{mod } q}{\cdot} c \overset{\text{Multiplilzieren mit } a^{-1}}{\Longrightarrow} b = c$.) Dann sind diese Elemente genau die Elemente $[1], [2], \ldots, [p-1]$, allerdings möglicherweise in anderer Reihenfolge.

Satz 19 (Kleiner Satz von Fermat  1607–1665)

Ist p eine Primzahl, so ist $[a^{p-1}] = [1]$ für jedes $[a] \in \mathbb{Z}_p \setminus \{[0]\}$.

Satz 19' *Für jede Primzahl p und für jede $a \in \mathbb{Z}$ gilt: entweder $a \vdots p$, oder $a^{p-1} - 1 \vdots p$.*

Beweis: Betrachte die Elemente $a, a \overset{\text{mod } q}{\cdot} [2], a \overset{\text{mod } q}{\cdot} [3], ..., a \overset{\text{mod } q}{\cdot} [p-1]$. Da $(\mathbb{Z}_p \setminus [0], \overset{\text{mod } q}{\cdot})$ nach Satz 18 und Lemma 9 eine Gruppe ist, sind diese Elemente verschieden (weil $a \overset{\text{mod } q}{\cdot} b = a \overset{\text{mod } q}{\cdot} c \overset{\text{Multiplilzieren mit } a^{-1}}{\Longrightarrow} b = c$.) Dann sind diese Elemente genau die Elemente $[1], [2], \ldots, [p-1]$, allerdings möglicherweise in anderer Reihenfolge. Also sind die Produkte gleich:

$$a \overset{\text{mod } q}{\cdot} [1] \overset{\text{mod } q}{\cdot} a \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} a \overset{\text{mod } q}{\cdot} [p-1] = [1] \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} [p-1]$$

Satz 19 **(Kleiner Satz von Fermat**  1607–1665)

Ist p eine Primzahl, so ist $[a^{p-1}] = [1]$ *für jedes* $[a] \in \mathbb{Z}_p \setminus \{[0]\}$.

Satz 19' *Für jede Primzahl p und für jede* $a \in \mathbb{Z}$ *gilt:*
entweder $a \vdots p$, *oder* $a^{p-1} - 1 \vdots p$.

Beweis: Betrachte die Elemente
$a, a \overset{\text{mod } q}{\cdot} [2], a \overset{\text{mod } q}{\cdot} [3], ..., a \overset{\text{mod } q}{\cdot} [p-1]$. Da $(\mathbb{Z}_p \setminus [0], \overset{\text{mod } q}{\cdot})$ nach Satz 18 und Lemma 9 eine Gruppe ist, sind diese Elemente verschieden (weil $a \overset{\text{mod } q}{\cdot} b = a \overset{\text{mod } q}{\cdot} c \overset{\text{Multiplilzieren mit } a^{-1}}{\Longrightarrow} b = c$.) Dann sind diese Elemente genau die Elemente $[1], [2], \ldots, [p-1]$, allerdings möglicherweise in anderer Reihenfolge. Also sind die Produkte gleich:

$$a \overset{\text{mod } q}{\cdot} [1] \overset{\text{mod } q}{\cdot} a \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} a \overset{\text{mod } q}{\cdot} [p-1] = [1] \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} [p-1]$$

$$\| \qquad\qquad \|$$

$$a^{p-1} \overset{\text{mod } q}{\cdot} [1] \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} [p-1]$$

Satz 19 (Kleiner Satz von Fermat  1607–1665)

Ist p eine Primzahl, so ist $[a^{p-1}] = [1]$ für jedes $[a] \in \mathbb{Z}_p \setminus \{[0]\}$.

Satz 19' *Für jede Primzahl p und für jede $a \in \mathbb{Z}$ gilt: entweder $a \vdots p$, oder $a^{p-1} - 1 \vdots p$.*

Beweis: Betrachte die Elemente $a, a \overset{\text{mod } q}{\cdot} [2], a \overset{\text{mod } q}{\cdot} [3], ..., a \overset{\text{mod } q}{\cdot} [p-1]$. Da $(\mathbb{Z}_p \setminus [0], \overset{\text{mod } q}{\cdot})$ nach Satz 18 und Lemma 9 eine Gruppe ist, sind diese Elemente verschieden (weil $a \overset{\text{mod } q}{\cdot} b = a \overset{\text{mod } q}{\cdot} c \overset{\text{Multiplilzieren mit } a^{-1}}{\Longrightarrow} b = c$.) Dann sind diese Elemente genau die Elemente $[1], [2], \ldots, [p-1]$, allerdings möglicherweise in anderer Reihenfolge. Also sind die Produkte gleich:

$$a \overset{\text{mod } q}{\cdot} [1] \overset{\text{mod } q}{\cdot} a \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} a \overset{\text{mod } q}{\cdot} [p-1] = [1] \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} [p-1]$$

$$\| \qquad\qquad\qquad\qquad \|$$

$$a^{p-1} \overset{\text{mod } q}{\cdot} [1] \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} [p-1] \qquad [1] \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} [p-1]$$

Satz 19 (Kleiner Satz von Fermat  1607–1665)

Ist p eine Primzahl, so ist $[a^{p-1}] = [1]$ für jedes $[a] \in \mathbb{Z}_p \setminus \{[0]\}$.

Satz 19' *Für jede Primzahl p und für jede $a \in \mathbb{Z}$ gilt: entweder $a \vdots p$, oder $a^{p-1} - 1 \vdots p$.*

Beweis: Betrachte die Elemente $a, a \overset{\text{mod } q}{\cdot} [2], a \overset{\text{mod } q}{\cdot} [3], ..., a \overset{\text{mod } q}{\cdot} [p-1]$. Da $(\mathbb{Z}_p \setminus [0], \overset{\text{mod } q}{\cdot})$ nach Satz 18 und Lemma 9 eine Gruppe ist, sind diese Elemente verschieden (weil $a \overset{\text{mod } q}{\cdot} b = a \overset{\text{mod } q}{\cdot} c \overset{\text{Multiplilzieren mit } a^{-1}}{\Longrightarrow} b = c$.) Dann sind diese Elemente genau die Elemente $[1], [2], \ldots, [p-1]$, allerdings möglicherweise in anderer Reihenfolge. Also sind die Produkte gleich:

$$a \overset{\text{mod } q}{\cdot} [1] \overset{\text{mod } q}{\cdot} a \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} a \overset{\text{mod } q}{\cdot} [p-1] \quad = \quad [1] \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} [p-1]$$

$$\| \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \|$$

$$a^{p-1} \overset{\text{mod } q}{\cdot} [1] \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} [p-1] \qquad\qquad [1] \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} [p-1]$$

Multiplizieren mit $([1] \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} [p-1])^{-1}$

Satz 19 (Kleiner Satz von Fermat  1607–1665)

Ist p eine Primzahl, so ist $[a^{p-1}] = [1]$ für jedes $[a] \in \mathbb{Z}_p \setminus \{[0]\}$.

Satz 19' *Für jede Primzahl p und für jede $a \in \mathbb{Z}$ gilt: entweder $a \vdots p$, oder $a^{p-1} - 1 \vdots p$.*

Beweis: Betrachte die Elemente $a, a \overset{\text{mod } q}{\cdot} [2], a \overset{\text{mod } q}{\cdot} [3], ..., a \overset{\text{mod } q}{\cdot} [p-1]$. Da $(\mathbb{Z}_p \setminus [0], \overset{\text{mod } q}{\cdot})$ nach Satz 18 und Lemma 9 eine Gruppe ist, sind diese Elemente verschieden (weil $a \overset{\text{mod } q}{\cdot} b = a \overset{\text{mod } q}{\cdot} c \overset{\text{Multiplilzieren mit } a^{-1}}{\Longrightarrow} b = c$.) Dann sind diese Elemente genau die Elemente $[1], [2], \ldots, [p-1]$, allerdings möglicherweise in anderer Reihenfolge. Also sind die Produkte gleich:

$$a \overset{\text{mod } q}{\cdot} [1] \overset{\text{mod } q}{\cdot} a \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} a \overset{\text{mod } q}{\cdot} [p-1] = [1] \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} [p-1]$$

$$\| \qquad\qquad\qquad\qquad \|$$

$$a^{p-1} \overset{\text{mod } q}{\cdot} [1] \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} [p-1] \qquad [1] \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} [p-1]$$

Multiplizieren mit $([1] \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} [p-1])^{-1}$ ergibt $a^{p-1} = [1]$.

Satz 19 (Kleiner Satz von Fermat  1607–1665)

Ist p eine Primzahl, so ist $[a^{p-1}] = [1]$ für jedes $[a] \in \mathbb{Z}_p \setminus \{[0]\}$.

Satz 19' *Für jede Primzahl p und für jede $a \in \mathbb{Z}$ gilt: entweder $a \vdots p$, oder $a^{p-1} - 1 \vdots p$.*

Beweis: Betrachte die Elemente $a, a \overset{\text{mod } q}{\cdot} [2], a \overset{\text{mod } q}{\cdot} [3], ..., a \overset{\text{mod } q}{\cdot} [p-1]$. Da $(\mathbb{Z}_p \setminus [0], \overset{\text{mod } q}{\cdot})$ nach Satz 18 und Lemma 9 eine Gruppe ist, sind diese Elemente verschieden (weil $a \overset{\text{mod } q}{\cdot} b = a \overset{\text{mod } q}{\cdot} c \overset{\text{Multiplilzieren mit } a^{-1}}{\Longrightarrow} b = c$.) Dann sind diese Elemente genau die Elemente $[1], [2], \ldots, [p-1]$, allerdings möglicherweise in anderer Reihenfolge. Also sind die Produkte gleich:

$$a \overset{\text{mod } q}{\cdot} [1] \overset{\text{mod } q}{\cdot} a \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} a \overset{\text{mod } q}{\cdot} [p-1] \quad = \quad [1] \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} [p-1]$$

$$\| \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \|$$

$$a^{p-1} \overset{\text{mod } q}{\cdot} [1] \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} [p-1] \qquad\qquad [1] \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} [p-1]$$

Multiplizieren mit $([1] \overset{\text{mod } q}{\cdot} [2] \cdots \overset{\text{mod } q}{\cdot} [p-1])^{-1}$ ergibt $a^{p-1} = [1]$.

□

Def. 16

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper,

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist,

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16'

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16' Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16' Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper,

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16' Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls er unitär ist, und $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16' Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls er unitär ist, und $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Frage: *Mindestens wie viel Elementen hat ein Körper?*

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16' Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls er unitär ist, und $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Frage: *Mindestens wie viel Elementen hat ein Körper?*

Antwort: 2*:*

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16' Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls er unitär ist, und $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Frage: *Mindestens wie viel Elementen hat ein Körper?*

Antwort: 2*:* 0

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16' Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls er unitär ist, und $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Frage: *Mindestens wie viel Elementen hat ein Körper?*

Antwort: 2*:* 0 *und* 1*.*

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16' Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls er unitär ist, und $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Frage: *Mindestens wie viel Elementen hat ein Körper?*

Antwort: 2*:* 0 *und* 1*.*

Bsp. $(\mathbb{Q}, \cdot, +)$, $(\mathbb{R}, \cdot, +)$, $(\mathbb{C}, \cdot, +)$ sind Körper.

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16' Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls er unitär ist, und $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Frage: *Mindestens wie viel Elementen hat ein Körper?*

Antwort: 2*:* 0 *und* 1*.*

Bsp. $(\mathbb{Q}, \cdot, +)$, $(\mathbb{R}, \cdot, +)$, $(\mathbb{C}, \cdot, +)$ sind Körper.

Sazt 20

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16' Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls er unitär ist, und $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Frage: *Mindestens wie viel Elementen hat ein Körper?*

Antwort: 2*:* 0 *und* 1*.*

Bsp. $(\mathbb{Q}, \cdot, +)$, $(\mathbb{R}, \cdot, +)$, $(\mathbb{C}, \cdot, +)$ sind Körper.

Satz 20 $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16' Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls er unitär ist, und $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Frage: *Mindestens wie viel Elementen hat ein Körper?*

Antwort: 2*:* 0 *und* 1*.*

Bsp. $(\mathbb{Q}, \cdot, +)$, $(\mathbb{R}, \cdot, +)$, $(\mathbb{C}, \cdot, +)$ sind Körper.

Sazt 20 $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist g.d. ein Körper,

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16' Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls er unitär ist, und $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Frage: *Mindestens wie viel Elementen hat ein Körper?*

Antwort: 2*:* 0 *und* 1*.*

Bsp. $(\mathbb{Q}, \cdot, +)$, $(\mathbb{R}, \cdot, +)$, $(\mathbb{C}, \cdot, +)$ sind Körper.

Sazt 20 $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist g.d. ein Körper, wenn q eine Primzahl ist.

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16' Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls er unitär ist, und $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Frage: *Mindestens wie viel Elementen hat ein Körper?*

Antwort: 2*:* 0 *und* 1*.*

Bsp. $(\mathbb{Q}, \cdot, +)$, $(\mathbb{R}, \cdot, +)$, $(\mathbb{C}, \cdot, +)$ sind Körper.

Sazt 20 $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist g.d. ein Körper, wenn q eine Primzahl ist.

Beweis:

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16' Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls er unitär ist, und $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Frage: *Mindestens wie viel Elementen hat ein Körper?*

Antwort: 2*:* 0 *und* 1*.*

Bsp. $(\mathbb{Q}, \cdot, +)$, $(\mathbb{R}, \cdot, +)$, $(\mathbb{C}, \cdot, +)$ sind Körper.

Sazt 20 $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist g.d. ein Körper, wenn q eine Primzahl ist.

Beweis: Wir wissen, dass $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16' Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls er unitär ist, und $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Frage: *Mindestens wie viel Elementen hat ein Körper?*

Antwort: 2*:* 0 *und* 1*.*

Bsp. $(\mathbb{Q}, \cdot, +)$, $(\mathbb{R}, \cdot, +)$, $(\mathbb{C}, \cdot, +)$ sind Körper.

Sazt 20 $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist g.d. ein Körper, wenn q eine Primzahl ist.

Beweis: Wir wissen, dass $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ein unitärer kommutativer Ring ist.

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16' Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls er unitär ist, und $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Frage: *Mindestens wie viel Elementen hat ein Körper?*

Antwort: 2*:* 0 *und* 1*.*

Bsp. $(\mathbb{Q}, \cdot, +)$, $(\mathbb{R}, \cdot, +)$, $(\mathbb{C}, \cdot, +)$ sind Körper.

Satz 20 $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist g.d. ein Körper, wenn q eine Primzahl ist.

Beweis: Wir wissen, dass $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ein unitärer kommutativer Ring ist. Dann gilt nach Folgerung aus Satz 18:

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16' Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls er unitär ist, und $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Frage: *Mindestens wie viel Elementen hat ein Körper?*

Antwort: 2*:* 0 *und* 1*.*

Bsp. $(\mathbb{Q}, \cdot, +)$, $(\mathbb{R}, \cdot, +)$, $(\mathbb{C}, \cdot, +)$ sind Körper.

Satz 20 $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist g.d. ein Körper, wenn q eine Primzahl ist.

Beweis: Wir wissen, dass $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ein unitärer kommutativer Ring ist. Dann gilt nach Folgerung aus Satz 18:

$\mathbb{Z}_q^* = \mathbb{Z}_q \setminus \{0\}$

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16' Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls er unitär ist, und $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Frage: *Mindestens wie viel Elementen hat ein Körper?*

Antwort: 2*:* 0 *und* 1*.*

Bsp. $(\mathbb{Q}, \cdot, +)$, $(\mathbb{R}, \cdot, +)$, $(\mathbb{C}, \cdot, +)$ sind Körper.

Satz 20 $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist g.d. ein Körper, wenn q eine Primzahl ist.

Beweis: Wir wissen, dass $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ein unitärer kommutativer Ring ist. Dann gilt nach Folgerung aus Satz 18:

$\mathbb{Z}_q^* = \mathbb{Z}_q \setminus \{0\} \iff q$ eine Primzahl ist.

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16' Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls er unitär ist, und $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Frage: *Mindestens wie viel Elementen hat ein Körper?*

Antwort: 2*:* 0 *und* 1*.*

Bsp. $(\mathbb{Q}, \cdot, +)$, $(\mathbb{R}, \cdot, +)$, $(\mathbb{C}, \cdot, +)$ sind Körper.

Satz 20 $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist g.d. ein Körper, wenn q eine Primzahl ist.

Beweis: Wir wissen, dass $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ein unitärer kommutativer Ring ist. Dann gilt nach Folgerung aus Satz 18:

$\mathbb{Z}_q^* = \mathbb{Z}_q \setminus \{0\} \iff q$ eine Primzahl ist.

Dann gilt:

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16' Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls er unitär ist, und $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Frage: *Mindestens wie viel Elementen hat ein Körper?*

Antwort: 2*:* 0 *und* 1*.*

Bsp. $(\mathbb{Q}, \cdot, +)$, $(\mathbb{R}, \cdot, +)$, $(\mathbb{C}, \cdot, +)$ sind Körper.

Satz 20 $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist g.d. ein Körper, wenn q eine Primzahl ist.

Beweis: Wir wissen, dass $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ein unitärer kommutativer Ring ist. Dann gilt nach Folgerung aus Satz 18:

$\mathbb{Z}_q^* = \mathbb{Z}_q \setminus \{0\} \iff q$ eine Primzahl ist.

Dann gilt:

$(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist ein Körper $\iff$

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16' Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls er unitär ist, und $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Frage: *Mindestens wie viel Elementen hat ein Körper?*

Antwort: 2*:* 0 *und* 1*.*

Bsp. $(\mathbb{Q}, \cdot, +)$, $(\mathbb{R}, \cdot, +)$, $(\mathbb{C}, \cdot, +)$ sind Körper.

Satz 20 $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist g.d. ein Körper, wenn q eine Primzahl ist.

Beweis: Wir wissen, dass $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ein unitärer kommutativer Ring ist. Dann gilt nach Folgerung aus Satz 18:

$\mathbb{Z}_q^* = \mathbb{Z}_q \setminus \{0\} \iff q$ eine Primzahl ist.

Dann gilt:

$(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist ein Körper $\iff$ q ist eine Primzahl.

Def. 16 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Def. 16' Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls er unitär ist, und $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Frage: *Mindestens wie viel Elementen hat ein Körper?*

Antwort: 2*:* 0 *und* 1*.*

Bsp. $(\mathbb{Q}, \cdot, +)$, $(\mathbb{R}, \cdot, +)$, $(\mathbb{C}, \cdot, +)$ sind Körper.

Satz 20 $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist g.d. ein Körper, wenn q eine Primzahl ist.

Beweis: Wir wissen, dass $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ein unitärer kommutativer Ring ist. Dann gilt nach Folgerung aus Satz 18:

$\mathbb{Z}_q^* = \mathbb{Z}_q \setminus \{0\} \iff q$ eine Primzahl ist.

Dann gilt:

$(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist ein Körper $\iff$ q ist eine Primzahl. $\square$

Probe-Klausur am Samstag 24.11.07 von 8^{15} bis 11^{45} in HS 1 CZ

Probe-Klausur am Samstag 24.11.07 von 8^{15} bis 11^{45} in HS 1 CZ

- Die Vorlesung am Do 22.11 fällt aus. Die Vorlesung am Mo wird von Dr. Fricke gehalten.
- Alle Teilnehmer sind zugelassen, keine Anmeldung, kein Pflicht

Probe-Klausur am Samstag 24.11.07 von 8^{15} bis 11^{45} in HS 1 CZ

- Die Vorlesung am Do 22.11 fällt aus. Die Vorlesung am Mo wird von Dr. Fricke gehalten.
- Alle Teilnehmer sind zugelassen, keine Anmeldung, kein Pflicht
- Keine Hilfsmittel sind zugelassen (außer dem Schreibstift/Bleistift).

Probe-Klausur am Samstag 24.11.07 von 8^{15} bis 11^{45} in HS 1 CZ

- Die Vorlesung am Do 22.11 fällt aus. Die Vorlesung am Mo wird von Dr. Fricke gehalten.
- Alle Teilnehmer sind zugelassen, keine Anmeldung, kein Pflicht
- Keine Hilfsmittel sind zugelassen (außer dem Schreibstift/Bleistift). Papier wird gegeben.

Probe-Klausur am Samstag 24.11.07 von 8^{15} bis 11^{45} in HS 1 CZ

- Die Vorlesung am Do 22.11 fällt aus. Die Vorlesung am Mo wird von Dr. Fricke gehalten.
- Alle Teilnehmer sind zugelassen, keine Anmeldung, kein Pflicht
- Keine Hilfsmittel sind zugelassen (außer dem Schreibstift/Bleistift). Papier wird gegeben.
- Ausweiskontrolle: bitte die Ausweise mitbringen

Probe-Klausur am Samstag 24.11.07 von 8^{15} bis 11^{45} in HS 1 CZ

- Die Vorlesung am Do 22.11 fällt aus. Die Vorlesung am Mo wird von Dr. Fricke gehalten.
- Alle Teilnehmer sind zugelassen, keine Anmeldung, kein Pflicht
- Keine Hilfsmittel sind zugelassen (außer dem Schreibstift/Bleistift). Papier wird gegeben.
- Ausweiskontrolle: bitte die Ausweise mitbringen
- Essen/Trinken/Einzeln Raus gehen ist erlaubt, aber nicht erwünscht

Probe-Klausur am Samstag 24.11.07 von 8^{15} bis 11^{45} in HS 1 CZ

- Die Vorlesung am Do 22.11 fällt aus. Die Vorlesung am Mo wird von Dr. Fricke gehalten.
- Alle Teilnehmer sind zugelassen, keine Anmeldung, kein Pflicht
- Keine Hilfsmittel sind zugelassen (außer dem Schreibstift/Bleistift). Papier wird gegeben.
- Ausweiskontrolle: bitte die Ausweise mitbringen
- Essen/Trinken/Einzeln Raus gehen ist erlaubt, aber nicht erwünscht

Punkten

- Neben jeder Aufgabe steht Anzahl von Punkten

Punkten

- Neben jeder Aufgabe steht Anzahl von Punkten
- Auch nicht vollständige gelöste Aufgaben werden gewertet.

Punkten

- Neben jeder Aufgabe steht Anzahl von Punkten
- Auch nicht vollständige gelöste Aufgaben werden gewertet. Es gibt keine “Minus-Punkten”

Punkten

- Neben jeder Aufgabe steht Anzahl von Punkten
- Auch nicht vollständige gelöste Aufgaben werden gewertet. Es gibt keine “Minus-Punkten”
- 50% der möglichen Punkten ist „ausreichend“. 75 % der möglichen Punkten ist „ausgezeichnet“.
- Wir werden versuchen, die Klausur schnell möglichst (vielleicht innerhalb einer Woche) zu korrigieren.

Punkten

- Neben jeder Aufgabe steht Anzahl von Punkten
- Auch nicht vollständige gelöste Aufgaben werden gewertet. Es gibt keine “Minus-Punkten”
- 50% der möglichen Punkten ist „ausreichend“. 75 % der möglichen Punkten ist „ausgezeichnet“.
- Wir werden versuchen, die Klausur schnell möglichst (vielleicht innerhalb einer Woche) zu korrigieren.
- Sie bekommen die Probe-Klausur von Übungsgruppenleitern zurück.

Punkten

- Neben jeder Aufgabe steht Anzahl von Punkten
- Auch nicht vollständige gelöste Aufgaben werden gewertet. Es gibt keine “Minus-Punkten”
- 50% der möglichen Punkten ist „ausreichend“. 75 % der möglichen Punkten ist „ausgezeichnet“.
- Wir werden versuchen, die Klausur schnell möglichst (vielleicht innerhalb einer Woche) zu korrigieren.
- Sie bekommen die Probe-Klausur von Übungsgruppenleitern zurück.

Klausuraufgaben

- Etwa die Hälfte: veränderte Hausaufgaben
- Verständnisaufgaben
- Theoretische Aufgaben: Definitionen werden abgefragt. Sätze werden abgefragt.
- Ein Satz aus
  $\{\text{Satz } 4, \text{ Satz } 7, \text{ Satz } 8, \text{ Satz } 9, \text{ Satz } 12 \text{ und deren Folgerung}\}$
  aus der Vorlesung muß bewiesen werden.

Was müssen sie nicht kennen und andere Ratschläge

Was müssen sie nicht kennen und andere Ratschläge

- Die Nummerierung von Sätze /Aussagen/ Definition (sie sollen trotzdem die benutzte Sätze irgendwie spezifizieren; z.B. nach dem kleinen Satz von Ferma.)

Was müssen sie nicht kennen und andere Ratschläge

- Die Nummerierung von Sätze /Aussagen/ Definition (sie sollen trotzdem die benutzte Sätze irgendwie spezifizieren; z.B. nach dem kleinen Satz von Ferma.)
- Jede Aufgabe zuerst lesen und verstehen und nur dann lösen

Was müssen sie nicht kennen und andere Ratschläge

- Die Nummerierung von Sätze /Aussagen/ Definition (sie sollen trotzdem die benutzte Sätze irgendwie spezifizieren; z.B. nach dem kleinen Satz von Ferma.)
- Jede Aufgabe zuerst lesen und verstehen und nur dann lösen
- Bitte nicht die ganze Zeit mit einer Aufgabe verbringen

Was müssen sie nicht kennen und andere Ratschläge

- Die Nummerierung von Sätze /Aussagen/ Definition (sie sollen trotzdem die benutzte Sätze irgendwie spezifizieren; z.B. nach dem kleinen Satz von Ferma.)
- Jede Aufgabe zuerst lesen und verstehen und nur dann lösen
- Bitte nicht die ganze Zeit mit einer Aufgabe verbringen
- Trotzdem, nach dem Sie die Aufgabe gelöst haben, prüfen Sie sie noch einmal.

Was müssen sie nicht kennen und andere Ratschläge

- Die Nummerierung von Sätze /Aussagen/ Definition (sie sollen trotzdem die benutzte Sätze irgendwie spezifizieren; z.B. nach dem kleinen Satz von Ferma.)
- Jede Aufgabe zuerst lesen und verstehen und nur dann lösen
- Bitte nicht die ganze Zeit mit einer Aufgabe verbringen
- Trotzdem, nach dem Sie die Aufgabe gelöst haben, prüfen Sie sie noch einmal.
- Ruhig bleiben

Viel Erfolg