Modulare Arithmetik

Michal Mnuk

Rechnen in $\mathbb{Z}_n$ (n=6)

Wir betrachten die Menge der ganzen Zahlen $\mathbb{Z}$

```
ClearAll[ℤ]
ℤ := Table[i, {i, -5, 5}]
```

```
ℤ
```

```
{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5}
```

In $\langle \mathbb{Z},+\rangle$ ist $\langle 6\mathbb{Z},+\rangle$ eine Untergruppe.

```
6 ℤ
```

```
{-30, -24, -18, -12,
 -6, 0, 6, 12, 18, 24, 30}
```

Wir untersuchen jetzt die Menge aller Nebenklassen $\{a+6\mathbb{Z} \mid a\in\mathbb{Z}\}$ bezüglich $6\mathbb{Z}$.

In[1]:=
```
ClearAll[NK]
NK[k_, n_: 6, s_: 5] :=
  Table[Mod[k, n] + i * n, {i, -s, s}]
```

```
NK[3]
```

```
{-27, -21, -15, -9, -3, 3, 9, 15, 21, 27, 33}
```

```
NK[0]
```

```
{-30, -24, -18, -12,
 -6, 0, 6, 12, 18, 24, 30}
```

```
NK[6]
```

```
{-30, -24, -18, -12,
 -6, 0, 6, 12, 18, 24, 30}
```

Addition von Nebenklassen

Definition: $(a+6\mathbb{Z})\oplus(b+6\mathbb{Z}):=(a+b)+6\mathbb{Z}$

In[3]:=
```
ClearAll[CirclePlus]
Attributes[CirclePlus] = {HoldAll};
NK /:
 NK[k1_, n_: 6, s_: 5] ⊕
  NK[k2_, n_: 6, s_: 5] :=
 NK[Mod[k1 + k2, n], n, s]
```

```
NK[3]
NK[4]
NK[3] ⊕ NK[4]
```

```
{-27, -21, -15, -9, -3, 3, 9, 15, 21, 27, 33}
```

```
{-26, -20, -14, -8,
 -2, 4, 10, 16, 22, 28, 34}
```

```
{-29, -23, -17, -11,
 -5, 1, 7, 13, 19, 25, 31}
```

```
(NK[3] ⊕ NK[4]) == NK[7] == NK[1]
```

```
True
```

Notation: a≡b mod 6 steht für die Mengengleichheit a+6ℤ = b+6ℤ.

```
NK[0] (* = 6 ℤ *)
```

```
{-30, -24, -18, -12,
 -6, 0, 6, 12, 18, 24, 30}
```

```
NK[3] ⊕ NK[0]
```

```
{-27, -21, -15, -9, -3, 3, 9, 15, 21, 27, 33}
```

```
NK[3] ⊕ NK[-3]
```

```
{-30, -24, -18, -12,
 -6, 0, 6, 12, 18, 24, 30}
```

Multiplikation von Nebenklassen

Definition: $(a+6\mathbb{Z})\otimes(b+6\mathbb{Z}):=(a\cdot b)+6\mathbb{Z}$

In[6]:=
```
ClearAll[CircleTimes]
Attributes[CircleTimes] = {HoldAll};
NK /:
 NK[k1_, n_: 6, s_: 5] ⊗
  NK[k2_, n_: 6, s_: 5] :=
 NK[Mod[k1 * k2, n], n, s]
```

Berechnen 3·4 mod 6

```
NK[3]
NK[4]
NK[3] ⊗ NK[4]
```

```
{-27, -21, -15, -9, -3, 3, 9, 15, 21, 27, 33}
```

```
{-26, -20, -14, -8,
 -2, 4, 10, 16, 22, 28, 34}
```

```
{-30, -24, -18, -12,
 -6, 0, 6, 12, 18, 24, 30}
```

```
NK[3] ⊗ NK[4] == NK[12] == NK[0]
```

```
True
```

In[9]:=
```
NK[4] ⊗ NK[1]
```

Out[9]=
```
{-26, -20, -14, -8,
 -2, 4, 10, 16, 22, 28, 34}
```

Lösen von linearen Gleichungen

Gibt es eine Nebenklasse x, sodass NK[3]⊗x = NK[1]? (Ist 3x ≡ 1 mod 6 lösbar?)

In[10]:=
```
NK[3] ⊗ NK[0]
```

Out[10]=
```
{-30, -24, -18, -12,
 -6, 0, 6, 12, 18, 24, 30}
```

In[11]:=
```
NK[3] ⊗ NK[1]
```

Out[11]=
```
{-27, -21, -15, -9, -3, 3, 9, 15, 21, 27, 33}
```

```
NK[3] ⊗ NK[2]
```

```
{-30, -24, -18, -12,
 -6, 0, 6, 12, 18, 24, 30}
```

```
NK[3] ⊗ NK[3]
```

```
{-27, -21, -15, -9, -3, 3, 9, 15, 21, 27, 33}
```

```
NK[3] ⊗ NK[4]
```

```
{-30, -24, -18, -12,
 -6, 0, 6, 12, 18, 24, 30}
```

```
NK[3] ⊗ NK[5]
```

```
{-27, -21, -15, -9, -3, 3, 9, 15, 21, 27, 33}
```

Gibt es eine Nebenklasse x, sodass NK[5]⊗x = NK[1]? (Ist 5·x ≡ 1 mod 6 lösbar?)

```
NK[5] ⊗ NK[5]
```

```
{-29, -23, -17, -11,
 -5, 1, 7, 13, 19, 25, 31}
```

Ab jetzt schreiben wir *a* für *NK[a]*

Der erweiterte Euklidische Algorithmus

In[14]:=
```
ClearAll[EGCD]
EGCD[m_, n_] :=
 Block[{d = ExtendedGCD[m, n]},
  {d[[1]],
   ToString[d[[1]]] <> " = " <>
    ToString[d[[2, 1]]] <> "·" <>
    ToString[m] <>
    " + " <> ToString[d[[2, 2]]] <>
    "." <>
    ToString[n]}
 ]
```

Lösen von $5 \cdot x \equiv 1 \bmod 6$

```
EGCD[5, 6]
```

```
{1, 1 = -1·5 + 1·6}
```

```
1 == 5 * 5 - 4 * 6
```

```
True
```

```
Mod[5 * 5, 6]
```

```
1
```

```
ClearAll[ModInv]
ModInv[k_, n_] := PowerMod[k, -1, n]
```

```
ModInv[5, 6]
```

```
5
```

```
ModInv[4, 6]
```

```
PowerMod::ninv :
 4 is not invertible modulo 6.
```

```
PowerMod[4, -1, 6]
```

Der Chinesische Restsatz

Wir rechnet man in $\mathbb{Z}_{55794083012669896096741539 0}$?

```
55794083012669896096741539 0 ==
  20
 ∏  Prime[i] ==
i=1
 2 * 3 * 5 * 7 * 11 * 13 * 17 * 19 * 23 * 29 * 31 *
  37 * 41 * 43 * 47 * 53 * 59 * 61 * 67 * 71
```

```
True
```

Elemente aus $\mathbb{Z}_6$ lassen sich eindeutig als Vektoren $(a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ darstellen.

1. Ein $t \in \mathbb{Z}_6$ wird auf $\varphi(t) = (t \bmod 2, t \bmod 3)$ abgebildet.

2. Ein Vektor (a,b) mit $a \in \mathbb{Z}_2$ und $b \in \mathbb{Z}_3$ wir auf die (eindeutige) Lösung $t = \psi(a,b)$ des Systems:

$$t \equiv a \bmod 2$$

$$t \equiv b \bmod 3$$

abgebildet.

```
ClearAll[φ]
φ[t_] := {Mod[t, 2], Mod[t, 3]}
```

```
0 ↦ φ[0]
1 ↦ φ[1]
2 ↦ φ[2]
3 ↦ φ[3]
4 ↦ φ[4]
5 ↦ φ[5]
```

```
0 ↦ {0, 0}
```

```
1 ↦ {1, 1}
```

```
2 ↦ {0, 2}
```

```
3 ↦ {1, 0}
```

```
4 ↦ {0, 1}
```

```
5 ↦ {1, 2}
```

Lösen jetzt

$$t \equiv 1 \bmod 2$$

$$t \equiv 2 \bmod 3.$$

$$\psi(1,2) :\equiv 1\cdot\left(\left(\frac{2\cdot3}{2}\right)^{-1} \bmod 2\right)\cdot\left(\frac{2\cdot3}{2}\right) + 2\cdot\left(\left(\frac{2\cdot3}{3}\right)^{-1} \bmod 3\right)\cdot\left(\frac{2\cdot3}{3}\right) \bmod 2\cdot3$$

```
ψ[a_, b_] :=
 Mod[a * ModInv[3, 2] * 3 +
      b * ModInv[2, 3] * 2, 2 * 3]
```

```
"(1,2)" ↦ ψ[1, 2]
```

```
(1,2) ↦ 5
```