Ein bisschen was zu **mod** und **div**

n	**div** 3	**mod** 3
0	0	0
1	0	1
2	0	2
3	1	0
4	1	1
5	1	2
6	2	0
7	2	1
8	2	2
9	3	0

Ein bisschen was zu **mod** und **div**

n	**div** 2	**mod** 2
0	0	0
1	0	1
2	1	0
3	1	1
4	2	0
5	2	1
6	3	0
7	3	1
8	4	0
9	4	1

Ein bisschen was zu **mod** und **div**

$\forall n \in \mathbb{N}_0 : \forall k \in \mathbb{N}_+ : n - (n \textbf{ mod } k)$ ist durch k teilbar.

$\to$ n durch k teilbar bzw. k teilt $n \iff \exists m \in \mathbb{N}_0 : km = n$.

.

Ein bisschen was zu **mod** und **div**

$\forall n \in \mathbb{N}_0 : \forall k \in \mathbb{N}_+ : n - (n \textbf{ mod } k)$ ist durch k teilbar.
$\forall n, m \in \mathbb{N}_0 : \forall k \in \mathbb{N}_+ : n \textbf{ mod } k = m \textbf{ mod } k \Rightarrow n - m$ ist durch k teilbar.

$\rightarrow$ n durch k teilbar bzw. k teilt $n \iff \exists m \in \mathbb{N}_0(\mathbb{Z}) : km = n$.

Vergleiche: $\forall n \in \mathbb{N}_0 : \forall k \in \mathbb{N}_+ :$
$k \cdot (n \textbf{ div } k) + (n \textbf{ mod } k) = n$.

.

Ein bisschen was zu **mod** und **div**

k heißt Teiler von n falls gilt: $\exists m \in \mathbb{N}_0(\mathbb{Z}) : km = n$.

k ist gemeinsamer Teiler von a, b: k teilt a und k teilt b.

Jede natürliche Zahl teilt 0.

Ein bisschen was zu ((größten) gemeinsamen) Teilern

k ist größter gemeinsamer Teiler von $a, b(ggt(a, b))$:

- k ist gemeinsamer Teiler von a und b und jeder gemeinsame Teiler k' von a und b erfüllt $k' \leq k$

  ODER

- k ist gemeinsamer Teiler von a und b und jeder gemeinsame Teiler k' von a und b erfüllt k' teilt k.

.

Ein bisschen was zu ((größten) gemeinsamen) Teilern

Formal für $k = ggt(a, b)$:

- $(\exists m_1, m_2 \in \mathbb{N}_0 : m_1 k = a \wedge m_2 k = b) \wedge \forall k' \in \mathbb{N}_0 : ((\exists m'_1, m'_2 \in \mathbb{N}_0 : m'_1 k' = a \wedge m'_2 k' = b) \Rightarrow k' \leq k.$

- $(\exists m_1, m_2 \in \mathbb{N}_0 : m_1 k = a \wedge m_2 k = b) \wedge \forall k' \in \mathbb{N}_0 : ((\exists m'_1, m'_2 \in \mathbb{N}_0 : m'_1 k' = a \wedge m'_2 k' = b) \Rightarrow \exists m_3 \in \mathbb{N}_0 : m_3 k' = k.$

.

Ein bisschen was zu ((größten) gemeinsamen) Teilern

a	b	$ggt(a,b)$
5	5	5
4	4	4
3	3	3
2	2	2
1	1	1
0	0	?

.

Ein bisschen was zu ((größten) gemeinsamen) Teilern

$\forall n \in \mathbb{N}_+ : ggt(0, n) = ggt(n, 0) = n.$

$ggt(0, 0)$ undefiniert nach Definition 1.

$ggt(0, 0) = 0$ nach Definition 2.

$\rightarrow$ Darum auf Übungsblatt: $a + b \geq 1$.

.

Frage: “Ginge das nicht viel einfacher mit while-Schleifen’ ?”

Antwort: “Natürlich, aber while-Schleifen hatten wir noch nicht!”

Algorithmen und so

Idee:

Anfang:	n	0	0	1	1
	x	y	z	e	v
$\rightarrow$	$x \,\mathbf{div}\, 2$	$y + e(x \bmod 2)$	$z + v(x \bmod 2)$	$2e$	$-v$

Wiederhole $1 + \lceil \log_2 n \rceil$ mal.

Algorithmen und so

$n = 5$:

Anfangsbelegung:	5	0	0	1	1
Nach 1. Schleife	2	1	1	2	-1
Nach 2. Schleife	1	1	1	4	1
Nach 3. Schleife	0	5	2	8	-1
Nach 4. Schleife	0	5	2	16	1

Algorithmen und so

$n = 9$:

Anfangsbelegung:	9	0	0	1	1
Nach 1. Schleife	4	1	1	2	-1
Nach 2. Schleife	2	1	1	4	1
Nach 3. Schleife	1	1	1	8	-1
Nach 4. Schleife	0	9	0	16	1
Nach 5. Schleife	0	9	0	32	-1

Algorithmen und so

$n = 16$:

Anfangsbelegung:	16	0	0	1	1
Nach 1. Schleife	8	0	0	2	-1
Nach 2. Schleife	4	0	0	4	1
Nach 3. Schleife	2	0	0	8	-1
Nach 4. Schleife	1	0	0	16	1
Nach 5. Schleife	0	16	1	32	-1
Nach 6. Schleife	0	16	1	64	1

Algorithmen und so

$n = 21$:

Anfangsbelegung:	21	0	0	1	1
Nach 1. Schleife	10	1	1	2	-1
Nach 2. Schleife	5	1	1	4	1
Nach 3. Schleife	2	5	2	8	-1
Nach 4. Schleife	1	5	2	16	1
Nach 5. Schleife	0	21	3	32	-1
Nach 6. Schleife	0	21	3	64	1

Algorithmen und so

Was fällt auf?

-
-
-

.

Algorithmen und so

Was fällt auf?

- Am Ende gilt $y = n$.
-
-

.

Was fällt auf?

- Am Ende gilt $y = n$.
- x wird in jedem Schritt halbiert, e wird in jedem Schritt verdoppelt.
-

.

Was fällt auf?

- Am Ende gilt $y = n$.

- x wird in jedem Schritt halbiert, e wird in jedem Schritt verdoppelt.

- Schleifeninvariante 1: $x \cdot e + y = n$.

.

Algorithmen und so

Was fällt auf?

-

-

.

Was fällt auf?

- $y \bmod 3 = z \bmod 3$
-

.

Was fällt auf?

- y **mod** $3 = z$ **mod** 3

- Schleifeninvariante 2: $y - z$ ist durch 3 teilbar.

.

Skizze Beweis Schleifeninvariante 2:

$$y + e(x \textbf{ mod } 2) - (z + v(x \textbf{ mod } 2)) =$$
$$y - z + (x \textbf{ mod } 2)(e - v)$$

.

Skizze Beweis Schleifeninvariante 2:

$y + e(x \ \mathbf{mod}\ 2) - (z + v(x \ \mathbf{mod}\ 2)) =$
$y - z + (x \ \mathbf{mod}\ 2)(e - v)$

Schön wäre, wenn $e - v$ immer durch 3 teilbar ist.

.

Schleifeninvariante:

- $x \cdot e + y = n \wedge$
- $e - v$ ist durch 3 teilbar $\wedge$
- $y - z$ ist durch 3 teilbar.

.

$x \leftarrow n$

$y \leftarrow 0$

$z \leftarrow 0$

$e \leftarrow 1$

$v \leftarrow 1$

for $i \leftarrow 0$ **to** $\lceil \log_2 n \rceil$ **do**

$\quad x \leftarrow x \,\mathbf{div}\, 2$

$\quad y \leftarrow y + e \cdot x \;\mathbf{mod}\; 2$

$\quad z \leftarrow z + v \cdot x \;\mathbf{mod}\; 2$

$\quad e \leftarrow 2 \cdot e$

$\quad v \leftarrow -v$

od

$x \leftarrow n$

$y \leftarrow 0$

$z \leftarrow 0$

$e \leftarrow 1$

$v \leftarrow 1$

for $i \leftarrow 0$ **to** $\lceil \log_2 n \rceil$ **do**

$\quad y \leftarrow y + e \cdot x \ \mathbf{mod}\ 2$

$\quad z \leftarrow z + v \cdot x \ \mathbf{mod}\ 2$

$\quad x \leftarrow x \ \mathbf{div}\ 2$

$\quad e \leftarrow 2 \cdot e$

$\quad v \leftarrow -v$

od

Schleifeninvariante(n) nachweisen

- Aussage S_i: Aussage der Schleifeninvariante gilt zu **Beginn** des i-ten Schleifendurchlaufs.

- Aussage R_i: Aussage der Schleifeninvariante gilt am **Ende** des i-ten Schleifendurchlaufs.

.

Schleifeninvariante(n) nachweisen

- Aussage S_i: Aussage der Schleifeninvariante gilt zu **Beginn** des i-ten Schleifendurchlaufs.

- Aussage R_i: Aussage der Schleifeninvariante gilt am **Ende** des i-ten Schleifendurchlaufs.

- Wenn es $i+1$-ten Schleifendurchlauf gibt, gilt $R_i = S_{i+1}$.

.

Schleifeninvariante(n) nachweisen

Vorgehen:

- Zeige S_0.

- Zeige für zulässige i: $S_i \Rightarrow R_i$.

.

Schleifeninvariante(n) nachweisen

Vorgehen:

- Zeige S_0.

- Zeige für zulässige i: $S_i \Rightarrow R_i$.

Dazu: Belegung der Variable V zu Anfang des i-ten Schleifendurchlaufs: V_i, am Ende des i-ten Schleifendurchlaufs: V_{i+1}.

.

Schleifeninvariante(n) nachweisen

SI 1: $x_i \cdot e_i + y_i = n$

IA: $i = 0$: $x_0 \cdot e_0 + y_0 = n \cdot 1 + 0 = n$. $\surd$

IV: Für beliebiges, aber festes $i \in \mathbb{N}_0$ gilt:
$i < \lceil \log_2 n \rceil \Rightarrow x_i \cdot e_i + y_i = n$.

IS: Es ist zu zeigen, dass dann auch $x_{i+1} \cdot e_{i+1} + y_{i+1} = n$:

$x_{i+1} \cdot e_{i+1} + y_{i+1} =$
$(x_i \,\mathbf{div}\, 2) \cdot (e_i \cdot 2) + (y_i + e_i \cdot x_i \ \mathbf{mod}\ 2)$
$= y_i + e_i((x_i \,\mathbf{div}\, 2) \cdot 2 + x_i \ \mathbf{mod}\ 2) = y_i + e_i x_i \overset{IV}{=} n$

Schleifeninvariante(n) nachweisen

SI 2: $e_i - v_i$ ist durch 3 teilbar.

IA: $i = 0$: $e_0 - v_0 = 1 - 1 = 0$ ist durch 3 teilbar. $\surd$

IV: Für beliebiges, aber festes $i \in \mathbb{N}_0$ gilt:
$i < \lceil \log_2 n \rceil \Rightarrow e_i - v_i$ ist durch 3 teilbar.

IS: Es ist zu zeigen, dass dann auch $e_{i+1} - v_{i+1}$ durch 3 teilbar ist:

$$e_{i+1} - v_{i+1} = 2 \cdot e_i - (-v_i) = 2 \cdot e_i + v_i = 2(e_i - v_i) + 3v_i.$$

Nach IV ist $e_i - v_i$ durch 3 teilbar,
und damit auch $2(e_i - v_i) + 3v_i$.

Schleifeninvariante(n) nachweisen

SI 3: $y_i - z_i$ ist durch 3 teilbar.

IA: $i = 0$: $y_0 - z_0 = 0 - 0 = 0$ ist durch 3 teilbar. $\surd$

IV: Für beliebiges, aber festes $i \in \mathbb{N}_0$ gilt:
$i < \lceil \log_2 n \rceil \Rightarrow y_i - z_i$ ist durch 3 teilbar.

IS: Es ist zu zeigen, dass dann auch $y_{i+1} - z_{i+1}$ durch 3 teilbar ist:

$y_{i+1} - z_{i+1} = y_i + e_i(x_i \textbf{ mod } 2) - (z_i + v_i(x_i \textbf{ mod } 2)) = (y_i - z_i) + (e_i - v_i)(x_i \textbf{ mod } 2)$

Nach IV beziehungsweise SI 2 sind beide Summanden durch 3 teilbar, also auch $y_{i+1} - z_{i+1}$.

Am Ende gilt:

- $x = 0$
- $y = n$
- $y \textbf{ mod } 3 = z \textbf{ mod } 3$.
- $|z| \leq 1 + \log_2 n$

.

Am Ende gilt:

- $x = 0$
- $y = n$
- $y \textbf{ mod } 3 = z \textbf{ mod } 3.$
- $|z| \leq 1 + \log_2 n$

Algorithmus neu initialisieren mit $x \leftarrow z, y \leftarrow 0, \ldots$, wiederholen
$\rightarrow$ liefert schnell n **mod** 3 in z.

Fragen zu Übungsblatt 2?
(Für nächste Woche)