TECHNISCHE UNIVERSITÄT DRESDEN

Fachrichtung Mathematik • Institut für Algebra • Prof. Bodirsky, Dr. Noack

Einführung in die Mathematik für Informatiker: Diskrete Strukturen INF 110
Wintersemester 2019/20

5. Lösungsblatt

für die Woche 18.11. - 24.11.2019

Euklidischer Algorithmus, Rechnen mod n

Ü25 (b) Wir betrachten die durch $F_{n+1} = F_n + F_{n-1}$ für $n \in \mathbb{N}$ mit $F_0 = F_1 = 1$ rekursiv definierten Fibonacci-Zahlen. Aus Übung 4, H23, ist bereits bekannt, dass $\text{ggT}(F_{n+1}, F_n) = 1$ für alle $n \in \mathbb{N}$ ist. Beweisen Sie, dass für alle $n \in \mathbb{N}, n \geq 2$ gilt:

$$1 = (-1)^n F_{n-2} \cdot F_{n+1} + (-1)^{n+1} F_{n-1} \cdot F_n.$$

Lösung:

(b) Mit vollständiger Induktion: Aussage A_n: $1 = (-1)^n F_{n-2} \cdot F_{n+1} + (-1)^{n+1} F_{n-1} \cdot F_n$.
IA: Es gilt A_2, denn $1 = (-1)^2 \cdot 1 \cdot 3 + (-1)^3 \cdot 1 \cdot 2$.
IS: Für alle $n \in \mathbb{N}$ gilt: Wenn $\underbrace{A_n \text{ gilt}}_{IV}$, dann gilt auch A_{n+1}, d.h.

$$(-1)^{n+1} F_{n-1} F_{n+2} + (-1)^n F_n \cdot F_{n+1} = 1.$$

Beweis: Es gelte A_n für ein beliebiges, aber festes $n \geq 2$. Dann folgt:

$$\begin{aligned}
&(-1)^{n+1} F_{n-1} \cdot F_{n+2} + (-1)^{n+2} F_n \cdot F_{n+1} \\
&= (-1)^{n+1} F_{n-1}(F_{n+1} + F_n) + (-1)^n F_n \cdot F_{n+1} \\
&= (-1)^{n+1} F_{n-1} F_{n+1} + \underbrace{(-1)^{n+1} F_{n-1} F_n}_{(IV)\ = 1-(-1)^n F_{n-2} F_{n+1}} + (-1)^n F_n \cdot F_{n+1} \\
&= 1 + (-1)^{n+1} F_{n-1} F_{n+1} - (-1)^n F_{n-2} F_{n+1} + (-1)^n F_n \cdot F_{n+1} \\
&= 1 + (-1)^{n+1} F_{n+1} \underbrace{(F_{n-1} + F_{n-2})}_{=F_n} + (-1)^n F_n \cdot F_{n+1} \\
&= 1 + (-1)^{n+1} F_{n+1} F_n + (-1)^n F_n \cdot F_{n+1} = 1. \quad \square
\end{aligned}$$

Ü26 (b) Berechnen Sie $z = 47^{201} \bmod 11$ und die letzte Ziffer der Zahl 2^{1000}.

Lösung:

(b) Letzte Ziffer von 2^{1000} durch Betrachtung modulo 10:
$1000 = 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^3$, $[1000]_2 = 1111101000$,

$$\begin{aligned}
2^{1000} &= 2^{2^9+2^8+2^7+2^6+2^5+2^3} \\
&= 2^{(((((2+1)2+1)2+1)2+1)2^2+1)2^3} \\
&= (((((2^2 \cdot 2)^2 \cdot 2)^2 \cdot 2)^2 \cdot 2)^{2\cdot 2} \cdot 2)^{2\cdot 2\cdot 2} \\
&\equiv ((((8^2 \cdot 2)^2 \cdot 2)^2 \cdot 2)^{2\cdot 2} \cdot 2)^{2\cdot 2\cdot 2} (\text{mod } 10) \\
&\equiv (((6^2 \cdot 2)^2 \cdot 2)^{2\cdot 2} \cdot 2)^{2\cdot 2\cdot 2} (\text{mod } 10) \\
&\equiv ((2^2 \cdot 2)^{2\cdot 2} \cdot 2)^{2\cdot 2\cdot 2} (\text{mod } 10) \\
&\equiv (8^{2\cdot 2} \cdot 2)^{2\cdot 2\cdot 2} \equiv 2^{2\cdot 2\cdot 2} \equiv 6 (\text{mod } 10)
\end{aligned}$$

oder alternativ gerechnet:

Zerlegung	Binärcode	k	$2^{2^k} \bmod 10$
$1000 = 2 \cdot 500 + 0$	0	0	2
$500 = 2 \cdot 250 + 0$	0	1	4
$250 = 2 \cdot 125 + 0$	0	2	$16 \equiv 6$
$125 = 2 \cdot 62 + \boxed{1}$	1	3	$36 \equiv 6$ $\leftarrow$
$62 = 2 \cdot 31 + 0$	0	4	$36 \equiv 6$
$31 = 2 \cdot 15 + \boxed{1}$	1	5	$36 \equiv 6$ $\leftarrow$
$15 = 2 \cdot 7 + \boxed{1}$	1	6	$36 \equiv 6$ $\leftarrow$
$7 = 2 \cdot 3 + \boxed{1}$	1	7	$36 \equiv 6$ $\leftarrow$
$3 = 2 \cdot 1 + \boxed{1}$	1	8	$36 \equiv 6$ $\leftarrow$
$1 = 2 \cdot 0 + \boxed{1}$	1	9	$36 \equiv 6$ $\leftarrow$

$\Rightarrow \quad 2^{1000} \equiv 6 \cdot 6 \cdot 6 \cdot 6 \cdot 6 \cdot 6 \equiv 6 \pmod{10}$.

Ü27 (a) Beweisen Sie: Eine Zahl ist genau dann durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist. (Analoges gilt für die Zahl 9.)

(b) Beweisen Sie, dass für alle $a, b \in \mathbb{Z}$ und alle $m, n \in \mathbb{N} \setminus \{0\}$ gilt:

$$m \cdot a \equiv m \cdot b \,(\mathrm{mod}\, m \cdot n) \;\Leftrightarrow\; a \equiv b \,(\mathrm{mod}\, n).$$

(c) Bestimmen Sie die Menge aller $a \in \mathbb{Z}_{28}$, so dass $14a \equiv 21 \,(\mathrm{mod}\, 28)$.

Lösung:

(a) $10 \equiv 1 \pmod 3 \Rightarrow 10^k \equiv 1 \pmod 3$ für alle $k \in \mathbb{N}$, und mit der Dezimaldarstellung: $n = \sum_{k=0}^{m} z_k \cdot 10^k \equiv z_0 + z_1 + z_2 + ... + z_m \pmod 3$.

(b) Es seien $a, b \in \mathbb{Z}$, $m, n \in \mathbb{N} \setminus \{0\}$ beliebig. Dann gilt

$$\begin{aligned} m \cdot a \equiv m \cdot b \,(\mathrm{mod}\, m \cdot n) \quad &\Leftrightarrow \quad \exists k \in \mathbb{Z} : ma = mb + kmn \\ &\Leftrightarrow \quad \exists k \in \mathbb{Z} : a = b + kn \quad (\text{da } m \neq 0) \\ &\Leftrightarrow \quad a \equiv b \,(\mathrm{mod}\, n). \end{aligned}$$

(c) Wenden (b) an: $a \in \mathbb{Z}_{28}$ erfüllt $14a \equiv 21 \,(\mathrm{mod}\, 28)$ genau dann, wenn $2a \equiv 3 \,(\mathrm{mod}\, 4)$. Letzreres ist für kein a erfüllbar, da $2a$ mod 4 stets gerade ist. Die Lösungsmenge ist also $\mathcal{L} = \emptyset$.

H29 Zu zeigen ist, dass $n^5 - n$ für alle $n \in \mathbb{N}$ durch 5 teilbar ist. Beweisen Sie dies auf zwei Wegen, einerseits mit vollständiger Induktion, andererseits ohne Induktion durch Fallunterscheidung für n mod 5.

Lösung:

1. Weg: $\boxed{\text{Fallunterscheidung}}$

n mod 5	n^5 mod 5
0	0
1	1
2	$2^5 = 32 \equiv 2$
3	$3^5 = 9 \cdot 9 \cdot 3 \equiv 3$
4	$4^5 = (2^5)^2 \equiv 4$

2. Weg: Mit vollständiger Induktion

(IA) $n = 0$: $\quad n^5 - n = 0$ und $5|0$

(IS) Zu zeigen. Für alle $n \in \mathbb{N}$ gilt: Wenn $5 \,|\, (5n^5 - n)$, dann auch $5 \,|\, (n+1)^5 - (n+1)$.

Beweis:

$$\begin{aligned}(n+1)^5 - (n+1) &= n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1 - n - 1 \\ &= \underbrace{n^5 - n}_{\text{nach IV durch 5 teilbar}} + \underbrace{5(n^4 + 2n^3 + 2n^2 + n)}_{\text{durch 5 teilbar}}\end{aligned}$$

H30 (a) Beweisen Sie: Eine Zahl ist genau dann durch 11 teilbar, wenn ihre alternierende Quersumme durch 11 teilbar ist (z.B. für 924 ist dies 9-2+4 = 11).

(b) Finden Sie die kleinste natürliche Zahl n, die bei der Division durch 3 den Rest 1, bei Division durch 4 den Rest 2 und bei Division durch 5 den Rest 3 lässt. Verwenden Sie dazu den chinesischen Restsatz.

Lösung:

(a) $10 \equiv -1 \pmod{11} \Rightarrow 10^k \equiv (-1)^k \pmod{11}$, und mit der Dezimaldarstellung: $n = \sum_{k=0}^{m} z_k \cdot 10^k \equiv z_0 - z_1 + z_2 - ... + s \cdot z_m \pmod{11}$, wobei $s = 1$ falls m gerade, sonst $s = -1$.

(b) $x \equiv 1 \pmod 3$
$x \equiv 2 \pmod 4$ 3, 4, 5 sind paarweise teilerfremd, $m = 3 \cdot 4 \cdot 5 = 60$
$x \equiv 3 \pmod 5$

$a_1 = 4 \cdot 5,\ a_2 = 3 \cdot 5,\ a_3 = 3 \cdot 4$

$4 \cdot 5 \cdot x_1 \equiv 1 \pmod 3 \quad \curvearrowright \quad 2x_1 \equiv 1 \pmod 3 \quad \curvearrowright \quad x_1 = 2$ ($2^{-1} = 2$ in $\mathbb{Z}_3$)

$3 \cdot 5 \cdot x_2 \equiv 2 \pmod 4 \quad \curvearrowright \quad 3x_2 \equiv 2 \pmod 4 \quad \curvearrowright \quad x_2 = 2$ ($3^{-1} = 3$ in $\mathbb{Z}_4$)

$3 \cdot 4 \cdot x_3 \equiv 3 \pmod 5 \quad \curvearrowright \quad 4x_3 \equiv 1 \pmod 5 \quad \curvearrowright \quad x_3 = 4$ ($4^{-1} = 4$ in $\mathbb{Z}_5$)

$\Longrightarrow\ x = 2a_1 + 2a_2 + 4a_3 = 40 + 30 + 48 \equiv 58 \pmod{60}$. Also ist $x = 58$ die kleinste solche Zahl.