Bénédict

Modulare Arithmetik

1.) Berechne

a) $0 \bmod 7$
b) $3 \bmod 5$
c) $17 \bmod 7$
d) $351 \bmod 100$
e) $487 \bmod 20$
f) $-3 \bmod 8$
g) $(-2)\cdot(-4) \bmod 3$
h) $-22 \bmod 17$
i) $-35 \bmod 99$
j) $-1 \bmod 9$

2.) Berechne die Grössen x und y wie folgt:

$$x = a \cdot b \bmod n$$
$$y = [(a \bmod n)\cdot(b \bmod n)] \bmod n$$

für

a) $a = 11, b = 3$ und $n = 5$
b) $a = -6, b = 14$ und $n = 11$
c) $a = -8, b = -15$ und $n = 7$

3.) Bestimme die Elemente in der Additionstafel

$a + b \bmod 7$

a \ b	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

4.) Bestimme die Elemente in der Multiplikationstafel

$a \cdot b \bmod 7$

a \ b	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

5.) Bestimme $y = 3 \cdot x \bmod 7$ für $x \in \{0,1,2,3,4,5,6\}$.
Für $y = 1$ ist x das multiplikative Inverse innerhalb einer Restklasse. Wie gross ist das multiplikative Inverse von 3?

$x =$	0	1	2	3	4	5	6
$3x =$							
$y = 3 \cdot x \bmod 7 =$							

6.) Bestimme das multiplikative Inverse $5^{-1} \bmod 7$ und berechne alsdann $4/5 \bmod 7$ mithilfe der Produktregel $a \cdot b \bmod 7 = [(a \bmod 7) \cdot (b \bmod 7)] \bmod 7$.

7.) Berechne mithilfe der Potenzregel

$$a^k \bmod n = (a \bmod n)^k \bmod n$$

Folgendes:

a) $351^{47} \bmod 7$

b) $482^{10} \bmod 9$

c) $768^{11} \bmod 5$

d) $136^{8} \bmod 6$

8.) Wahr oder falsch?

a) $2 \equiv 3 \bmod 2$

b) $15 \equiv 4 \bmod 11$

c) $12 \equiv 26 \bmod 7$

d) $5 \equiv 7 \bmod 3$

e) $10 \equiv 19 \bmod 9$

f) $13 \equiv 21 \bmod 4$

9.) Die Lösungsmenge von $x \equiv 29 \bmod 11$ definiert eine Restklasse modulo 11. Schreibe diese Restklasse in aufzählender Form. [Grundmenge von x ist $\mathbb{Z}$]

Musterlösungen

1.)

Teil	a	b	c	d	e	f	g	h	i	j
Lösung	0	3	3	51	7	5	2	12	64	8

2a) $x = 11 \cdot 3 \bmod 5 = 33 \bmod 5 = \underline{\underline{3}}$

$y = [(11 \bmod 5) \cdot (3 \bmod 5)] \bmod 5 = 1 \cdot 3 \bmod 5 =$
$3 \bmod 5 = \underline{\underline{3}}$

b) $x = -6 \cdot 14 \bmod 11 = -84 \bmod 11 = \underline{\underline{4}}$

$y = [(-6 \bmod 11) \cdot (14 \bmod 11)] \bmod 11 = 5 \cdot 3 \bmod 11 =$
$15 \bmod 11 = \underline{\underline{4}}$

c) $x = (-8)\cdot(-15) \bmod 7 = 120 \bmod 7 = \underline{\underline{1}}$

$y = [(-8 \bmod 7)\cdot(-15 \bmod 7)] \bmod 7 = 6\cdot 6 \bmod 7$

$= 36 \bmod 7 = \underline{\underline{1}}$

3.)

	a + b mod 7						
	b						
a	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

4.)

	a · b mod 7						
	b						
a	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

5. $x=0$: $y = 3\cdot 0 \bmod 7 = 0 \bmod 7 = 0$
$x=1$: $y = 3\cdot 1 \bmod 7 = 3 \bmod 7 = 3$
$x=2$: $y = 3\cdot 2 \bmod 7 = 6 \bmod 7 = 6$
$x=3$: $y = 3\cdot 3 \bmod 7 = 9 \bmod 7 = 2$
$x=4$: $y = 3\cdot 4 \bmod 7 = 12 \bmod 7 = 5$
$x=5$: $y = 3\cdot 5 \bmod 7 = 15 \bmod 7 = 1 \leftarrow$
$x=6$: $y = 3\cdot 6 \bmod 7 = 18 \bmod 7 = 4$

$\rightarrow \underline{\underline{3^{-1} \bmod 7 = 5}}$

x =	0	1	2	3	4	5	6
3x =	0	3	6	9	12	15	18
y = 3·x mod 7 =	0	3	6	2	5	1	4

6.) $5 \cdot 0 \bmod 7 = 0 \bmod 7 = 0$
$5 \cdot 1 \bmod 7 = 5 \bmod 7 = 5$
$5 \cdot 2 \bmod 7 = 10 \bmod 7 = 3$
$5 \cdot 3 \bmod 7 = 15 \bmod 7 = 1 \leftarrow$
$4/5 \bmod 7 = 4 \cdot 5^{-1} \bmod 7 = [(4 \bmod 7) \cdot$
$(5^{-1} \bmod 7)] \bmod 7 = 4 \cdot 3 \bmod 7 = 12 \bmod 7 = \underline{\underline{5}}$

7a) $351^{47} \bmod 7 = (351 \bmod 7)^{47} \bmod 7 = 1^{47} \bmod 7 = \underline{\underline{1}}$
b) $482^{10} \bmod 9 = (482 \bmod 9)^{10} \bmod 9 = 5^{10} \bmod 9$
$= 9'765'625 \bmod 9 = \underline{\underline{4}}$
c) $768^{11} \bmod 5 = (768 \bmod 5)^{11} \bmod 5 = 3^{11} \bmod 5 =$
$177'147 \bmod 5 = \underline{\underline{2}}$
d) $136^{8} \bmod 6 = (136 \bmod 6)^{8} \bmod 6 = 4^{8} \bmod 6 =$
$65'536 \bmod 6 = \underline{\underline{4}}$

8a) $3-2 = 1 \neq 2 \rightarrow$ falsch
b) $15-4 = 11 = 1 \cdot 11 \rightarrow$ wahr
c) $26-12 = 14 = 2 \cdot 7 \rightarrow$ wahr
d) $7-5 = 2 \neq 3 \rightarrow$ falsch
e) $19-10 = 9 = 1 \cdot 9 \rightarrow$ wahr
f) $21-13 = 8 = 2 \cdot 4 \rightarrow$ wahr

9.) $29 \bmod 11 = 7 \rightarrow \underline{\underline{x \in \{\ldots, -26, \overset{+11}{\curvearrowright} -15, \overset{+11}{\curvearrowright} -4, \overset{+11}{\curvearrowright} 7, 18, 29, \ldots\}}}$