Modulo-Grundaufgaben

1

$37 \ mod \ 10 =$ 7

$231 \ mod \ 11 =$ $(220+11) \bmod 11 = 0$

$89 \ mod \ 9 =$ $(81+8) \bmod 9 = 8$

$78 \ mod \ 7 =$ 1

2

$-7 \ mod \ 10 =$ $(-7+10) \bmod 10 = 3$

$-7 \ mod \ 11 =$ $(-7+11) \bmod 11 = 4$

$89123 \ mod \ 100 =$ 23

$-78 \ mod \ 100 =$ $(-78+22) \bmod 100 = 22$

3

$4 + x \underset{10}{\equiv} 0 \Leftrightarrow x \underset{10}{\equiv}$ 6

$33 + x \underset{50}{\equiv} 0 \Leftrightarrow x \underset{50}{\equiv}$ 17

$13 + x \underset{20}{\equiv} 7 \Leftrightarrow x \underset{20}{\equiv}$ 14

4

denn $4 \cdot 2 = 8 \underset{7}{\equiv} 1$

$4 \cdot x \underset{7}{\equiv} 1 \Leftrightarrow x \underset{7}{\equiv}$ 2

$2 \cdot x \underset{13}{\equiv} 3 \Leftrightarrow x \underset{13}{\equiv}$ 8

$13 \cdot x \underset{20}{\equiv} 19 \Leftrightarrow x \underset{20}{\equiv}$ 3 denn $39 \underset{20}{\equiv} 19$

5

Bei den Verküpfungstafeln für die Multiplikation lässt man die 0-Zeile und die 0-Spalte weg.
Stellen Sie die Verknüfungstafeln für $(\mathbb{Z}_6, \cdot)$ und $(\mathbb{Z}_7, \cdot)$ auf. siehe unten

6

Warum hat die Gleichung $2 \cdot x \underset{7}{\equiv} 5$

eine Lösung, aber $2 \cdot x \equiv 5$ nicht?

$2 \cdot 6 \underset{7}{\equiv} 5$ In Zeile 2^6 ist keine 5

7

Welche Elemente in $(\mathbb{Z}_6, \cdot)$ haben kein Inverses? In Zeilen 2, 3, 4 ist keine 1
Was fällt an diesen Elementen auf?
Sie haben mit 6 gemeinsame Teiler.

8

Elemente, die kein Inverses haben, heißen Nullteiler.

$(\mathbb{Z}_7, \cdot)$ ist also nullteilerfrei.

Woran kann man das an der Tabelle sehen?

In der Tabelle ist keine 0

9

Stellen Sie eine Vermutung auf, welche $(\mathbb{Z}_m, \cdot)$ Nullteiler haben und welche nicht.

$(\mathbb{Z}_m, \cdot)$ hat genau dann keine Nullteiler, wenn m Primzahl ist.

10

$\mathbb{Z}_{10}^* = \{1,3,7,9\}$ ist die Menge der zu 10 teilerfremden Zahlen aus $\mathbb{Z}_{10}$.

Stellen Sie eine Verknüpfungstafel für $(\mathbb{Z}_{10}^*, \cdot)$ auf. siehe unten

Machen Sie sich klar, dass nun alle Elemente Inverse haben und es keine Nullteiler gibt.

Ausblick

Die Inversen sind für die Kryptografie so wichtig, weil sie die inversen Operationen, also das Entschlüsseln bewerkstelligen. Das Arbeiten im Modul hat zwei Vorteile: Es gibt Inverse, die keine Bruchzahlen sind, aber sie sind ohne gewisse Informationen nur schwer zu finden.

5 $(\mathbb{Z}_6,\cdot)$

*	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Dies rechnet man im Kopf:

$5 \cdot 2 = 10 \equiv 4 \pmod 6$

Die Tabellen sind mit Excel berechnet:
Befehl: Rest(vorn*oben; m)

5 $(\mathbb{Z}_7,\cdot)$

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$5 \cdot 3 = 15 \equiv 1 \pmod 7$ $(14+1=15)$

Will man Luxus betreiben, nimmt man Rest($A2* B$1; m) und kopiert diese Formel.

6 2 mal irgendwas steht in der Zeile mit der 2 vorne. Da gibt es aber keine 5. also gibt es keine Lösung.

6 2 mal irgendwas steht in der Zeile mit der 2 vorne. Da gibt es eine 5 in der Spalte 6. Also x=6 ist Lösung.

7 2, 3 und 4 haben keine 1 in ihren Zeilen. Daarum haben sie keine Inversen. Stattdessen haben sie aber eine 0 in ihren Zeilen. 2*3=0 ... Darum heißen sie Nullteiler.

8 In keiner Zeile ist eine 0. Stattdessen ist in jeder Zeile eine 1, Jedes Element hat alo ein Inverses. 2*4=1; 3*5=1; 6*6=1;
6 heißt auch "selbstinvers".

9 a*b=0 ergibt sich modulo m, wenn a*b=m oder a*b=2m... Dann sind a und b beide Teiler von m oder sie haben mit m einen gemeinsamen Teiler. Wenn m keine Primzahl ist, erzeugen ihre Teiler als Produkt eine 0.
Wenn m eine Primzahl ist kann das aber nicht sein. Dann gibt es keine Nullteiler.

In $\mathbb{Z}_{10}^* = \{1,3,7,9\}$ ist m=10 zwar keine Primzahl, aber die "gefährlichen" Zahlen sind weggelassen.

*	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

10 $\mathbb{Z}_{10}^* = \{1,3,7,9\}$ ist die Menge der zu 10 teilerfremden Zahlen zwischen 0 und 10.

Alle Elemente haben Inverse, denn in allen Zeilen kommt die 1 vor.

Merke:

$\mathbb{Z}_m^*$ ist die Menge der zu m teilerfremden Zahlen. Sie spielt eine zentrale Rolle, weil in $(\mathbb{Z}_m^*,\cdot)$ alle Elemente Inverse haben.

*	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

$(\mathbb{Z}_{12}^*,\cdot)$ Hier sind etliche Zahlen nicht dabei. Aber diese haben Inverse.

$5 \cdot 7 = 35 = (24+11) \equiv 11 \pmod{12}$

$5 \cdot 5 = 1 \quad 7 \cdot 7 = 1 \quad 11 \cdot 11 = 121 \equiv 1 \pmod{12}$

Leuphana Universität Lüneburg	Bearbeitet von Ha 15.09.2008
Prof. Dr. Haftendorn	Grunddatum 15.09.2008