Algorithmen

Restklassen

Division mit Rest

Die Division zweier natürlichen Zahlen kann in speziellen Fällen „aufgehen", doch in den meisten Fällen gibt es einen Rest.

Aufgabe 1: Berechne den Rest der Division (ohne Taschenrechner)

a) 17 : 2 b) 143 : 5 c) 755 : 12 d) 286 : 13

Aufgabe 2: Wie gross kann der Rest bei der Division durch 12 höchstens sein? Und bei der Division durch m?

Definition: Teilt man eine ganze Zahl a durch eine ganze Zahl m, so erhält man einen Rest r. Für diesen Rest gilt $0 \leq r \leq m-1$. Die ***Modulo-Funktion*** liefert zu gegebenen Zahlen a und m diesen Rest r. Es gilt also: $a = k \cdot m + r$ mit $k \in \mathbb{Z}$.
Man schreibt: $a \bmod m = r$

Im täglichen Leben rechnet man recht häufig modulo 10, zum Beispiel bei der schriftlichen Division. Eine normale Uhr mit analogem Stundenzeiger zeigt die Anzahl Stunden modulo 12 an.

Aufgabe 3: Es ist 12 Uhr am Mittag und du hast in 50 Stunden einen Tenniskurs und in 70 Stunden einen Computerkurs. Um welche Tageszeit finden die Kurse statt?

Aufgabe 4: Berechne:

a) $273 \bmod 4$ b) $268 \bmod 5$ c) $255 \bmod 20$
d) $2000 \bmod 7$ e) $210 \bmod 9$ f) $743 \bmod 10$
g) $11137 \bmod 10$ h) $1 \bmod 2$ i) $-18 \bmod 4$

Aufgabe 5: Allgemeine Überlegungen

a) Es sei k irgendeine gerade Zahl. Berechne k mod 2.
b) Es sei k irgendeine ungerade Zahl. Berechne k mod 2.
c) Berechne 34 mod 4, 134 mod 4 und 111'134 mod 4.
d) Es sei k irgendeine Zahl die auf die Ziffer r endet. Berechne k mod 10.

Aufgabe 6: Man kann den Rest auch berechnen, wenn der Dividend (Zähler) oder Divisor (Nenner) negativ ist. Das Vorzeichen des Rests wird vom Vorzeichen des Divisors übernommen:

a) –17 mod 3 b) –27 mod 5 c) $37 \bmod (-7)$ d) $-217 \bmod (-8)$

Aufgabe 7: Schlage die Definition des Rests bei Division (Modulo-Funktion) in der Formelsammlung nach. Gibt sie nur für natürliche oder auch für ganze Zahlen?

Die Restklasse

Definition: Zwei ganze Zahlen a und b heissen ***kongruent modulo m***, wenn sie bei der Division durch m den gleichen Rest ergeben. m heisst der Modul. Wir schreiben

$$a \equiv b \pmod m$$

Beispiele:

Betrachten wir nun einen bestimmten Modul m, so können wir alle ganzen Zahlen in „Gruppen" unterteilen, so dass in jeder solcher „Gruppe" nur die ganzen Zahlen sind, die bezüglich m denselben Rest haben.

Als Bsp. betrachten wir m = 4

$$\{\ldots -200, -196, -192, \ldots -12, -8, -4, 0, 4, 8, 12, \ldots 300, 304 \ldots\} = \overline{0}$$

$$\{\ldots -199, -195, -191, \ldots -11, -7, -3, 1, 5, 9, 13, \ldots 301, 305 \ldots\} = \overline{1}$$

$$\{\ldots -198, -194, -190, \ldots -10, -6, -2, 2, 6, 10, 14, \ldots 302, 306 \ldots\} = \overline{2}$$

$$\{\ldots -197, -193, -189, \ldots -9, -5, -1, 3, 7, 11, 15, \ldots 303, 307 \ldots\} = \overline{3}$$

Üblicherweise werden diese „Gruppen" (Klassen) nach dem kleinsten natürlichen Rest benannt.

Definition: Die ***Restklasse von a modulo m*** (oft bezeichnet mit $\overline{a}$) ist die Menge aller ganzen Zahlen k für die gilt $a \equiv k \pmod m$, d.h. die Menge aller ganzen Zahlen, die durch Teilen mit m den gleichen Rest wie a ergeben, wobei $m \in \mathbb{N}$ und $a \in \mathbb{Z}$.

Die Zahl a ist dann ein ***Repräsentant*** der Restklasse $\overline{a}$ (jedes Element der Klasse kann ein Repräsentant sein).

Die ***Menge aller Restklassen modulo m*** wird oft mit $\mathbb{Z}_m = \mathbb{Z} / m\mathbb{Z}$ bezeichnet.

Beispiel: $\mathbb{Z}_4 = \mathbb{Z} / 4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$

wobei
$$\begin{aligned}\overline{0} &= \{-8, -4, 0, 4, \ldots, 160, 164, \ldots\}\\ \overline{1} &= \{-7, -3, 1, 5, \ldots, 161, 165, \ldots\}\\ \overline{2} &= \{-6, -2, 2, 6, \ldots, 162, 166, \ldots\}\\ \overline{3} &= \{-5, -1, 3, 7, \ldots, 163, 167, \ldots\}\end{aligned}$$

Aufgabe 8: In welche Restlassen gehören die Zahlen 69, 2468, 99451, –567 und –11111 bezüglich der Module 7, 12, 112?

Aufgabe 9: Wahr oder falsch, falls falsch korrigiere:

a) $456 \equiv 78 \pmod{32}$

b) $8793 \equiv 61 \pmod{123}$

Aufgabe 10: Bestimme jeweils die kleinste natürliche Zahl n für die gilt:

a) $39 \equiv n \pmod{5}$

b) $n \equiv 456 \pmod{11}$

c) $1111 \equiv 45 \pmod{n}$

Rechnen mit Restklassen

Bekanntlich kann man mit ganzen Zahlen Rechnungen durchführen: addieren, subtrahieren, multiplizieren. Dividieren ist in den ganzen Zahlen jedoch nicht (immer) möglich!

Wie ist das im Falle von Restklassen modulo m?

Addition

$\overline{3}+\overline{2} = \qquad \pmod{4}$ $\qquad\qquad$ $\overline{7}+\overline{12} = \qquad \pmod{6}$

Allgemein:

Multiplikation

$\overline{3}\cdot\overline{2} = \qquad \pmod{4}$ $\qquad\qquad$ $\overline{7}\cdot\overline{12} = \qquad \pmod{6}$

Allgemein:

Rechenregeln für Restklassen

Mit Hilfe der *Rechenregeln für Restklassen* lassen sich die folgenden Aufgaben lösen.

$$\overline{a}\pm\overline{b}=\overline{a\pm b} \quad \Leftrightarrow \quad a+b \equiv a \bmod m \pm b \bmod m \pmod{m}$$

$$\overline{a}\cdot\overline{b}=\overline{a\cdot b} \quad \Leftrightarrow \quad a\cdot b \equiv a \bmod m \cdot b \bmod m \pmod{m}$$

$$\overline{a}^n=\overline{a^n} \quad \Leftrightarrow \quad a^n \equiv (a \bmod m)^n \pmod{m}$$

Aufgabe 11: Beweise die ersten beiden Rechenregeln für Restklassen!

Da es nun bei jedem beliebigen Modul nur endlich viele Klassen gibt, können wir diese in einer Tabelle aufschreiben, d.h. wir können *Additions- und Multiplikationstafeln* aufstellen. (Einfachheitshalber lasse ich hier die Striche unten weg).

$m = 3$:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$m = 5$:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Beispiel zum Lesen der Tabellen: m = 3, addiert man 1 und 1 (mod 3), sprich zwei ganze Zahlen, die durch 3 den Rest 1 ergeben, so ergibt die Summen dividiert durch 3 den Rest 2.

Aufgabe 12: Erstelle eine Multiplikationstafel für m = 6.

Aufgabe 13: Erstelle eine Multiplikationstabelle für m = 9 mit Excel!

Aufgabe 14: Rechne mit den Restklassen modulo 5!

a) $\overline{3}+\overline{3}$ b) $\overline{2}-\overline{4}$ c) $\overline{2}\cdot\overline{3}$ d) $\overline{4}\cdot\overline{4}$

Aufgabe 15: Berechne!

a) $207\cdot 556 \mod 3$ b) $699\cdot 7001 \mod 7$ c) $9199\cdot 12405 \mod 8$

Aufgabe 16: Berechne

a) $2^{654} \mod 7$ b) $2^{569} \mod 7$ c) $2^{81} \mod 5$

d) $42^{108} \mod 4$ e) $41^{1028} \mod 4$

Aufgabe 17: Berechne

a) $29^{60} \bmod 99$ b) $73^{10} \bmod 78$ c) $123^{345} \bmod 678$

Aufgabe 18: Untersuche die Terme $23^{45} - 15^{147}$ und $67^{54} - 32^{12}$ auf ihre Reste bezüglich 3, 6, 7.

Aufgabe 19: Auf welche Ziffer enden die Zahlen 3^{160}, 7^{111}, 7^{126}, 7^{127} und 8^{111}?

Aufgabe 20: Zeige: $43^7 - 87^{13}$ ist ohne Rest durch 44 teilbar.