Teilbarkeiten und Rechnen mit Resten

Korrespondenzzirkel Mathematik – 1. Brief

Klassenstufe 7/8

Was dich erwartet:

In diesem Kurs tauchen wir tiefer in die Welt der **Teilbarkeit und dem Rechnen mit Resten** ein. Zahlentheoretische Aufgaben sind ein wesentlicher Bestandteil mathematischer Wettbewerbsaufgaben, zum Beispiel in der Mathematik-Olympiade. Zahlentheoretische Betrachtungen beziehen sich in der Regel auf den Zahlenbereich der ganzen Zahlen. Oft genügt es aber auch, sich auf den Bereich der natürlichen Zahlen zu beschränken.

Hier gilt: Es wird in keiner Weise erwartet, dass du alle Aufgaben löst! Wenn du die Zeit dazu hast – super! Aber wenn nicht, kannst du auch nur die Aufgaben einschicken, die du geschafft hast; selbst wenn das nur eine Aufgabe ist. Wir freuen uns über jede Rücksendung!

Was du bereits kennen solltest:

Für die bevorstehenden Aufgaben solltest du diese Inhalte schon beherrschen:

- Grundlegende Kenntnisse zu **Primzahlen, Teilern und Vielfachen**
- Einfache **Mengen** verstehen können wie z.B. $M = \{1, 2, 3, 4, 6, 12\}$
- Sicheres Rechnen mit **Potenzen** und Anwenden der **Potenzgesetze**, insbesondere $a^{m+n} = a^m \cdot a^n$ und $(a^n)^m = a^{n \cdot m}$

Falls dir einer dieser Punkte noch unbekannt ist, schau am besten vorher nochmal in deine Unterlagen. Das macht dir den Einstieg in diesen Brief leichter.

1 Teilbarkeit und Teiler

Sind a und b zwei ganze Zahlen ($a, b \in \mathbb{Z}$), so heißt a *Teiler* von b, wenn es ein $k \in \mathbb{Z}$ gibt mit $b = a \cdot k$. In diesem Fall schreibt man $a \mid b$ und sagt: „a teilt b“. Dann gilt auch: $\frac{b}{a} = k$ mit $k \in \mathbb{Z}$.
Gibt es hingegen kein $k \in \mathbb{Z}$ mit $b = a \cdot k$, so schreibt man $a \nmid b$ und sagt: „a teilt b nicht“.

Eigenschaften der Teilbarkeit

Seien a, b und c natürliche Zahlen, dann gilt:

1. $a \mid b \implies a \mid b \cdot c$
2. $a \mid b$ und $a \mid c \implies a \mid b + c$
3. $a \mid b$ und $b \mid c \implies a \mid c$
4. $a \mid b \implies a \leq b$
5. $a \cdot b \mid c \implies a \mid c$ und $b \mid c$

Satz 1.1 (Division mit Rest): Zu je zwei natürlichen Zahlen a und b (mit $a \neq 0$) gibt es stets eindeutig bestimmte nichtnegative ganze Zahlen q und r mit der Eigenschaft:

$$b = q \cdot a + r, \quad 0 \leq r < a.$$

Beispiel: Es sei $a = 7$ und $b = 23$. Dann gilt *eindeutig* $23 = 3 \cdot 7 + 2$. Also ist $q = 3$ und $r = 2$. Die Eindeutigkeit beruht darauf, dass $r < a$ sein muss, was zum Beispiel mit $23 = 2 \cdot 7 + 9$ nicht erfüllt ist, da 9 nicht kleiner als 7 ist. Man sagt: „23 lässt bei Division durch 7 den Rest 2.“ Damit r der kleinste Rest mit $r < a$ ist, muss $q = \lfloor \frac{b}{a} \rfloor$ gelten. Die Klammer wird dabei als ”(untere) Gaußklammer”bezeichnet. Für eine reelle Zahl x ist $\lfloor x \rfloor$ die größte ganze Zahl, die kleiner oder gleich x ist. In unserem Beispiel also: $q = \lfloor \frac{b}{a} \rfloor = \lfloor \frac{23}{7} \rfloor = \lfloor 3,28... \rfloor = 3$.

1.1 Primzahlen

Eine natürliche Zahl heißt *Primzahl*, wenn sie genau zwei verschiedene Teiler hat, nämlich 1 und sich selbst.

Satz 1.2: Jede Primzahl $p > 3$ lässt bei Division durch 6 entweder den Rest 1 oder den Rest 5.
Beweis: Bei Division durch 6 sind die Reste $0, 1, 2, 3, 4, 5$ möglich. Die Zahlen sind darstellbar als: $6k,\ 6k+1,\ 6k+2,\ 6k+3,\ 6k+4,\ 6k+5$. Alle Zahlen der Form $6k$ sind durch 6 teilbar, alle Zahlen der Formen $6k+2 = 2 \cdot (3k+1)$ und $6k+4 = 2 \cdot (3k+2)$ sind durch 2 teilbar und alle Zahlen der Form $6k+3 = 3 \cdot (2k+1)$ sind durch 3 teilbar und können deshalb keine Primzahlen $p > 3$ sein. Als Primzahlen sind folglich nur Zahlen der Form $6k+1$ und $6k+5$ möglich. w.z.b.w.

Satz 1.3 (Hauptsatz der elementaren Zahlentheorie): Jede natürliche Zahl größer als 1 ist entweder eine Primzahl oder lässt sich als Produkt aus Primzahlen schreiben. Diese Produktdarstellung ist abgesehen von der Reihenfolge der Primzahlen *eindeutig*.
Beispiel: Die Primfaktorzerlegung (PFZ) von 72 ist: $72 = 2^3 \cdot 3^2$.

1.2 Anzahl der Teiler einer Zahl

Auf der Grundlage der Primfaktorzerlegung kann man die Anzahl der Teiler einer Zahl ermitteln.
Satz 1.4: Hat eine Zahl z die Primfaktorzerlegung

$$z = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n},$$

dann hat sie genau $(a_1+1)(a_2+1)\cdots(a_n+1)$ verschiedene Teiler.

Dieses Ergebnis resultiert aus einer kombinatorischen Überlegung. Zum Beispiel kommt der Primfaktor p_1 in jedem Teiler mit einem der Exponenten von 0 bis a_1 vor. Das sind (a_1+1) verschiedene Möglichkeiten. Da dies auch für die anderen Primfaktoren gilt, erhält man für die Anzahl der Teiler das oben genannte Produkt.

Beispiel: $72 = 2^3 \cdot 3^2$ hat $(3+1)\cdot(2+1) = 12$ Teiler. Es sind $1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36$ und 72. Diese Teiler sind paarweise zueinander Komplimentärteiler, d.h. ihr Produkt ist 72. Es gilt $1 \cdot 72 = 2 \cdot 36 = 3 \cdot 24 = 4 \cdot 18 = 6 \cdot 12 = 8 \cdot 9 = 72$

Folgerung: Alle Quadratzahlen größer als 0 und nur diese haben eine ungerade Anzahl von Teilern. Nur für die Quadratzahlen größer als 1 gilt, dass alle Exponenten ihrer Primfaktoren α_i gerade sind, sodass das Produkt $(\alpha_1+1)\cdot(\alpha_2+1)\cdot\ldots\cdot(\alpha_n+1)$ ungerade ist.

1.3 Der größte gemeinsame Teiler (ggT)

Zwei oder mehrere natürliche Zahlen haben stets einen größten gemeinsamen Teiler, der größer oder gleich 1 ist, weil 1 gemeinsamer Teiler von allen natürlichen Zahlen ist. Für den größten gemeinsamen Teiler zweier natürlicher Zahlen a und b schreiben wir $\mathrm{ggT}(a, b)$. Gilt $\mathrm{ggT}(a, b) = 1$, so heißen a und b *teilerfremd* oder *relativ prim*. Insbesondere gilt für jede natürliche Zahl $n \geq 1$: $\mathrm{ggT}(n, 1) = 1$ und $\mathrm{ggT}(n, 0) = n$, denn n ist immer ein Teiler von 0.

Wichtig: Zwei Zahlen a und b müssen teilerfremd sein, damit aus $a \mid c$ und $b \mid c$ auch $a \cdot b \mid c$ gefolgert werden kann.

Verfahren zur Ermittlung des größten gemeinsamen Teilers:

(a) **Teilermengenverfahren**
Wir bilden für beide natürliche Zahlen a und b die Teilermengen (Menge aller Teiler einer Zahl) $T(x)$ und ermitteln aus der Menge der gemeinsamen Teiler den größten.
Beispiel: Für $\mathrm{ggT}(24; 66)$ bekommen wir die Teilermengen $T(24) = \{\mathbf{1}, \mathbf{2}, \mathbf{3}, 4, \mathbf{6}, 8, 12, 24\}$ und $T(66) = \{\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{6}, 11, 22, 33, 66\}$. Die gemeinsamen Teiler von 24 und 66 sind demnach $gT(24, 66) = \{1, 2, 3, 6\}$, wobei 6 ihr größter ist.

(b) **Primfaktorverfahren**
Wir bilden die Primfaktorzerlegung beider Zahlen und übernehmen in den größten gemeinsamen Teiler die jeweils kleinsten Potenzen der gemeinsamen Primfaktoren:

$$\begin{array}{rcll} 24 & = & 2^3 \cdot 3^1 & \\ 66 & = & 2^1 \cdot 3^1 \cdot 11^1 & \\ \hline \text{ggT}(24, 66) & = & 2^1 \cdot 3^1 & = 6 \end{array}$$

(c) **Euklidischer Algorithmus**
Das Teilermengenverfahren und das Primfaktorverfahren sind für große Zahlen nicht mehr praktikabel. Dafür eignet sich aber der Euklidische Algorithmus. Grundlage für diesen Algorithmus ist folgender Zusammenhang.

Satz 1.5: Sind a und b zwei natürliche Zahlen mit $a > b$, dann gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(a - b, b)$.

Beweis: Wenn t ein beliebiger gemeinsamer Teiler von a und b ist, dann folgt aus $t \mid a$ und $t \mid b$ wegen $a = m \cdot t$ und $b = n \cdot t$ direkt $a - b = (m - n) \cdot t$ und deshalb auch $t \mid (a - b)$. Das muss folglich auch für den größten gemeinsamen Teiler gelten. w.z.b.w.

Wenn $a - b$ größer als b ist, dann können wir die Subtraktion wiederholen und erhalten

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(a - b, b) = \mathrm{ggT}(a - 2b, b).$$

Da nach Satz 1.1 $a = q \cdot b + r$ mit $0 \leq r < b$ gilt, kann schließlich

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(a - qb, b) = \mathrm{ggT}(r, b) \quad \text{mit } r < b$$

gefolgert werden. Dieser Zusammenhang bildet die Grundlage des Euklidischen Algorithmus.

Für unser Beispiel gilt:

Gesucht ist: $\mathbf{ggT(66, 24)} : 66 - 2 \cdot 24 = 18\ (q = 2, r = 18) \Rightarrow \mathrm{ggT}(66, 24) = \mathrm{ggT}(18, 24)$

danach gilt für $\mathrm{ggT}(24, 18) : 24 - 1 \cdot 18 = 6\ (q = 1, r = 6) \Rightarrow \mathrm{ggT}(24, 18) = \mathrm{ggT}(6, 18)$

danach gilt für $\mathrm{ggT}(18, 6) : 18 - 3 \cdot 6 = 0\ (q = 3, r = 0) \Rightarrow \mathrm{ggT}(18, 6) = \mathrm{ggT}(0, 6)$

Da $6 - 0 = 6$ gilt, würde eine Weiterführung immer wieder zu $\mathrm{ggT}(6, 0)$ führen. Folglich ist der Euklidische Algorithmus beendet, wenn $r = 0$ entstanden ist. Schließlich gilt $\mathrm{ggT}(6, 0) = 6$. Der größte gemeinsame Teiler ist folglich 6.

Für zwei natürliche Zahlen a und b und ihren größten gemeinsamen Teiler $\mathrm{ggT}(a, b)$ gibt es immer zwei ganze Zahlen x und y, so dass $\mathrm{ggT}(a, b) = x \cdot a + y \cdot b$ gilt. Dazu kann man den Euklidischen Algorithmus rückwärts verfolgen. Zunächst nehmen wir die vorletzte Zeile: $6 = 1 \cdot 24 - 1 \cdot 18$. Danach müssen wir aus der ersten Zeile $18 = 1 \cdot 66 - 2 \cdot 24$ benutzen und in die erste Gleichung einsetzen:
$6 = 1 \cdot 24 - 1 \cdot (1 \cdot 66 - 2 \cdot 24) = -1 \cdot 66 + 3 \cdot 24$. Man erhält folglich $\mathbf{6} = -1 \cdot \mathbf{66} + 3 \cdot \mathbf{24}$.

Für das **kleinste gemeinsame Vielfache** (kgV) gilt stets:

$$\mathrm{kgV}(a,b) = \frac{a \cdot b}{\mathrm{ggT}(a,b)}$$

Daher ist von 66 und 24 das kleinste gemeinsame Vielfache: $\mathrm{kgV}(66;24) = \frac{1584}{6} = 264$.

2 Rechnen mit Kongruenzen

Wenn zwei ganze Zahlen a und b bei der Division durch die natürliche Zahl m den gleichen Rest r lassen, dann sind „a und b kongruent modulo m“. Man schreibt

$$a \equiv b \pmod{m}.$$

Die Division mit Rest aus 1.1 kann also auch als *Kongruenz* geschrieben werden, für unser Beispiel von oben gilt: $23 \equiv 2 \pmod 7$. Gesprochen wird das als: „23 ist kongruent 2 modulo 7 “ und bedeutet 23 und 2 lassen den gleichen Rest bei Division durch 7 (nämlich 2).

Mit Kongruenzen kann man in vielen Fällen genauso rechnen wie mit Gleichungen. Für $a, b, c, d \in \mathbb{Z}$, $m, n \in \mathbb{N}$ sowie $a \equiv b \pmod m$ und $c \equiv d \pmod m$ folgt:

Eigenschaften der Teilbarkeit

Seien a, b und c natürliche Zahlen, dann gilt:

(a) $a \pm c \equiv b \pm d \pmod m$

(b) $a \cdot c \equiv b \cdot d \pmod m$

(c) $a^n \equiv b^n \pmod m$

(d) $a \cdot n \equiv b \cdot n \pmod{m \cdot n}$

Für die Division einer Kongruenz durch eine natürliche Zahl n gelten allerdings besondere Regeln.

Insbesondere die Folgerung (c) ist für viele Aufgaben sehr praktikabel.

Beispiel: Ermittle den Rest, den die Zahl 2025^{2025} bei der Division durch 7 lässt.
Lösung: Da 2023 durch 7 teilbar ist, gilt $2025 \equiv 2 \pmod 7$. Daraus folgt $2025^2 \equiv 2^2 \pmod 7$ und $2025^3 \equiv 2^3 \equiv 1 \pmod 7$. Mit dem Rest 1 können wir schnell auf hohe Potenzen schließen: $2025^{2025} = 2025^{3 \cdot 675} = (2025^3)^{675} \equiv 1^{675} \equiv 1 \pmod 7$. Folglich lässt die Zahl 2025^{2025} bei der Division durch 7 den Rest 1, d.h. $2025^{2025} - 1$ ist durch 7 teilbar.

Aufgaben: Teilbarkeiten und Rechnen mit Resten

Aufgabe 1

a) Berechne $\operatorname{ggT}(455, 247)$.

b) Ermittle zwei ganze Zahlen x und y so, dass $\operatorname{ggT}(455, 247) = 455x + 247y$ gilt.

Aufgabe 2

Auf welche Ziffer endet 13^{2025}.

Aufgabe 3

a) Beweise $44 \mid 87^{13} + 43^{7}$.

b) Beweise $51 \mid 33^{2n} + 171^{n}$ für alle natürlichen Zahlen n.

Aufgabe 4

Die natürliche Zahl n hat genau zwei Teiler. $n+1$ hat genau drei Teiler. Wie viele Teiler hat dann $n+2$?

Aufgabe 5

Beweise: Für jede Primzahl $p > 3$ gilt $24 \mid p^2 - 1$.
Hinweis: Nutze die binomische Formel.

Aufgabe 6

Ein Zahlenpaar (p, q) heißt Primzahlzwillingspaar, wenn p und q Primzahlen mit $q = p + 2$ sind. Wir betrachten im Folgenden nur Primzahlzwillingspaare (p, q) mit $p > 3$.

a) Untersuche, ob es ein solches Primzahlzwillingspaar (p, q) gibt, für das $p+6$ eine Primzahl ist.

b) Untersuche, ob es ein solcher Primzahlzwillingspaar (p, q) gibt, für das $p+4$ eine Primzahl ist.

c) Beweise, dass für jedes solche Primzahlzwillingspaar das um 1 vergrößerte Produkt beider Primzahlen durch 36 teilbar ist.

Aufgabe zu einem anderen Thema

Aufgabe 7

Löse die Ungleichung: $\frac{5-x}{2+x} > 3$

Etwas zum freien Denken...

Aufgabe 8

In einem Raum von 2,40 m × 6,00 m Grundfläche und mit 2,40 m hohen Wänden hockt auf der Mittellinie einer der beiden quadratischen Wände, 20 cm über dem Boden, eine Spinne. Auf der Mittellinie der gegenüberliegenden Wand, 20 cm unter der Decke, sitzt eine Fliege. Die Spinne möchte die Fliege fressen und krabbelt auf einem möglichst kurzen Weg zu ihr hin. Da die Spinne nicht fliegen kann, darf ihr Weg natürlich nur über die Wände, die Decke und den Fußboden gehen. Wie lang ist der Weg der Spinne?

