53. Österreichische Mathematik-Olympiade

Junior*innen -Kurs 11. Jänner 2022

Modulo - Rechnen mit Restklassen

Beim Modulo-Rechnen müssen wir zuallererst eine natürliche Zahl m auswählen, die wir Modul nennen. Wenn wir nun *modulo* m rechnen, interessiert uns nicht mehr, wie groß eine Zahl eigentlich ist, sondern nur, welcher Rest übrig bleibt, wenn wir sie durch den Modul m dividieren.

> *Beispiel:* Der einfachste Modul, den wir wählen können, ist $m = 2$. Bei Division durch 2 gibt es nur zwei mögliche Reste: Wenn die Zahl gerade ist, bleibt Rest 0, wenn die Zahl ungerade ist, bleibt Rest 1. Wir kümmern uns also nicht mehr um die eigentlichen Zahlen, sondern nur darum, ob sie gerade oder ungerade sind.

Wenn wir modulo m rechnen, sind also zwei Zahlen a und b, die dividiert durch m denselben Rest ergeben, für uns gleich. Wir sagen dann, dass a und b in derselben *Restklasse modulo* m liegen oder *moldulo* m *kongruent* sind. Mathematisch schreiben wir das folgendermaßen auf:

$$a \equiv b \mod m$$

Beispiele:

$$1 \equiv 3 \mod 2$$
$$2 \equiv 100 \mod 2$$
$$4 \equiv 7 \mod 3$$
$$6 \equiv 14 \mod 4$$
$$3 \equiv 18 \mod 5$$

Mit Restklassen kann man genauso rechnen wie mit normalen Zahlen. Zusätzlich kann man jederzeit eine Zahl durch eine andere Zahl derselben Restklasse ersetzen. Natürlich gibt das Ergebnis am Ende auch nur an, in welcher Restklasse das eigentliche Ergebnis ist.

> *Beispiel:* Wir wollen wissen, ob die Zahl $545 \cdot 652 + 937 \cdot 213 + 791 \cdot 135$ gerade oder ungerade ist. Anstatt die Zahl zur Gänze auszurechnen, rechnen wir also modulo 2. Wir ersetzen jede Zahl in der Rechnung durch 0 oder 1, je nachdem welchen Rest sie bei Division durch 2 ergibt:
>
> $$545 \cdot 652 + 937 \cdot 213 + 791 \cdot 135 \equiv 1 \cdot 0 + 1 \cdot 1 + 1 \cdot 1 \mod 2$$

Nun haben wir etwas viel einfacheres auszurechnen:

$$1 \cdot 0 + 1 \cdot 1 + 1 \cdot 1 = 2$$

Das Ergebnis können wir wieder durch 0 oder 1 ersetzen, je nachdem in welcher Restklasse es ist:

$$2 \equiv 0 \mod 2$$

Insgesamt wissen wir jetzt also:

$$545 \cdot 652 + 937 \cdot 213 + 791 \cdot 135 \equiv 0 \mod 2$$

Das bedeutet, diese Zahl ist gerade.

Was wir hier gemacht haben, ist eigentlich genau dasselbe wie wenn wir gesagt hätten: $545 \cdot 652$ ist gerade, weil 652 gerade ist. $937 \cdot 213$ ist ungerade, weil 937 und 213 ungerade sind. $791 \cdot 135$ ist ungerade, weil 791 und 135 ungerade sind. Wir haben also die Summe von einer geraden und zwei ungeraden Zahlen, also ist das Ergebnis gerade. Der Vorteil vom Modulo-Rechnen gegenüber dieser Methode ist aber, dass es leichter aufzuschreiben ist und dass es auch für größere Module funktioniert, nicht nur für den Modul 2.

Achtung: Beim Addieren, Subtrahieren und Multiplizieren können wir, wie gerade im Beispiel, jederzeit eine Zahl durch eine andere Zahl derselben Restklasse ersetzen. Bei anderen Rechenoperationen sollten wir aber aufpassen:

- Divisionen vertragen sich gar nicht mit dem Modulo-Rechnen: Wenn etwa die Zahl, durch die wir dividieren, in der Restklasse 0 liegt, müssten wir plötzlich durch 0 dividieren! Bei Divisionen darf man daher im Allgemeinen nicht mit Modulo rechnen, Ausnahmen gibts nur für Modulo-Profis.

- Bei Potenzen muss man ganz genau aufpassen. Betrachten wir die Potenz a^b. Die Basis a dürfen wir durch eine andere Zahl derselben Restklasse ersetzen. Schließlich wird a nur immer wieder mit sich selber multipliziert, und bei Multiplikationen wissen wir schon, dass das Ersetzen erlaubt ist. Den Exponenten b dürfen wir aber NICHT ersetzen, weil mit ihm nicht direkt gerechnet wird, sondern er nur angibt, wie oft a mit sich selbst multipliziert wird.

Aufgaben

1. Berechne, in welcher Restklasse bezüglich dem angegebenen Modul die folgenden Zahlen liegen:

   a) $412 \mod 4$ b) $9638 \mod 9$ c) $271485 \mod 25$ d) $2641 \mod 11$

2. Zeige: Zwei Zahlen sind genau dann kongruent modulo m, wenn ihre Differenz durch m teilbar ist. Anders ausgedrückt:

   $$a \equiv b \mod m \quad \Leftrightarrow \quad m|(a-b)$$

3. Bestimme die Einerstelle der folgenden Zahlen:

   a) $345 \cdot 13284 - 24767 \cdot 2983 + 57221$

   b) $135 + 32135 - 342 \cdot 7198 - 341 \cdot 9819$

   c) $85941^6 - 5473^3 \cdot 5249$

   d) $\frac{5550}{25} \cdot 91384$

4. Beweise, dass man beim Addieren und Subtrahieren modulo m tatsächlich Zahlen durch andere Zahlen derselben Restklasse ersetzen darf. Das heißt:

   Wenn $a \equiv a' \mod m$ und $b \equiv b' \mod m$, dann gilt auch $a + b \equiv a' + b' \mod m$ und $a - b \equiv a' - b' \mod m$.

5. Zeige, dass die folgenden Gleichungen keine Lösungen in den ganzen Zahlen haben:

   a) $18a - 33b + 5(c + 1) = 2c$

   b) $98x + 84y + 91z = 215$

   c) $x^2 + 1 = 3y$

   d) $a^2 + b^2 = 1234567$

6. Beweise, dass man beim Multiplizieren modulo m tatsächlich Zahlen durch andere Zahlen derselben Restklasse ersetzen darf.

7. Beweise die folgenden Teilbarkeiten:

   a) $35 \mid 7220 \cdot 832 - 713 \cdot 49831 - 982$

   b) $60 \mid 2543 \cdot 913 + 105 \cdot (-9381) + 8329 \cdot 238 + 1044$

   c) $3 \mid 2^{5182} - 1$

   d) $13 \mid 2021^{53} + 2022^{53}$

Lösungen

1. a) $412 = 103 \cdot 4 + 0 \;\Rightarrow\; 412 \equiv 0 \mod 4$
   b) $9638 = 9630 + 8$, 9 teilt 9630 $\Rightarrow\; 9638 \equiv 8 \mod 9$
   c) $271485 = 271475 + 10$, 25 teilt 271475 $\Rightarrow\; 271485 \equiv 10 \mod 25$
   d) $2641 = 2640 + 1$, 11 teilt 2640 $\Rightarrow\; 2641 \equiv 1 \mod 11$

2. Sei $a = k \cdot m + x$ und $b = l \cdot m + y$ das Ergebnis der Division mit Rest durch m. Die beiden Zahlen a und b sind also genau dann kongruent modulo m, wenn $x = y$. Die Differenz der Zahlen ist $a - b = (k \cdot m + x) - (l \cdot m + y) = (k - l) \cdot m + (x - y)$. Also ist die Differenz genau dann durch m teilbar, wenn $x - y$ durch m teilbar ist. Als Reste von Divisionen durch m sind x und y aber Zahlen aus der Menge $\{0, 1, 2, ..., m-2, m-1\}$. Der Betrag der Differenz $x - y$ ist also kleinergleich $m - 1$ und damit ist $x - y$ nur durch m teilbar, wenn $x - y = 0$, also wenn $x = y$. Also ist $a - b$ genau dann durch m teilbar, wenn $x = y$, was genau dann der Fall ist, wenn a und b kongruent modulo m sind.

3. Um die Einerstelle einer Zahl zu bestimmen, müssen wir die Zahl modulo 10 berechnen. Um dann die Einerstelle zu berechnen, müssen wir nur noch wissen, ob die Zahl positiv oder negativ ist. Denn wenn wir etwa berechnen, dass die Zahl kongruent 7 $\mod 10$ ist, bedeutet das, dass es eine der folgenden Zahlen ist: $\{..., -23, -13, -3, 7, 17, 27, ...\}$.

   a) $345 \cdot 13284 - 24767 \cdot 2983 + 57221 \equiv 5 \cdot 4 - 7 \cdot 3 + 1 \equiv 20 - 21 + 1 \equiv 0 \mod 10$. Also ist die Einerstelle 0. (Man sieht leicht, dass in dem Fall egal ist, ob die Zahl positiv oder negativ ist, denn die Zahlen der Restklasse 0 sind: $\{..., -20, -10, 0, 10, 20, ...\}$.)

   b) $135 + 32135 - 342 \cdot 7198 - 341 \cdot 9819 \equiv 5 + 5 - 2 \cdot 8 - 1 \cdot 9 \equiv -15 \equiv -5 \equiv 5 \mod 10$. Wir haben Glück, auch bei 5 ist egal, ob die Zahl positiv oder negativ ist, die Einerstelle ist sicher 5.

   c) Die Exponenten 6 und 3 dürfen wir nicht ersetzen, aber die sind eh kleine Zahlen. $85941^6 - 5473^3 \cdot 5249 \equiv 1^6 - 3^3 \cdot 9 \equiv 1 - 27 \cdot 9 \equiv 1 - 7 \cdot 9 \equiv -62 \equiv -2 \equiv 8 \mod 10$. Größenabschätzung zeigt, dass die Zahl positiv ist, also ist die Einerstelle 8.

   d) Wir müssen zuerst den Bruch ausrechnen, bevor wir mit dem Modulo-Rechnen anfangen. $\frac{5550}{25} \cdot 91384 = \frac{555 \cdot 10}{25} \cdot 91384 = \frac{5 \cdot 111 \cdot 5 \cdot 2}{25} \cdot 91384 = 222 \cdot 91384 \equiv 2 \cdot 4 \equiv 8 \mod 10$. Die Zahl ist sicher positiv, hat also Einerstelle 8.

4. Wir benutzen, was wir aus Aufgabe 2. wissen:
   $a \equiv a' \mod m \;\Rightarrow\; m|(a - a')$
   $b \equiv b' \mod m \;\Rightarrow\; m|(b - b')$
   Also $m \mid (a - a') + (b - b') = (a + b) - (a' + b') \;\Rightarrow\; a + b \equiv a' + b' \mod m$
   $m \mid (a - a') - (b - b') = (a - b) - (a' - b') \;\Rightarrow\; a - b \equiv a' - b' \mod m$

5. Wir müssen die Gleichung immer modulo einem passenden Modul betrachten, wo sich dann ein Widerspruch ergibt. Manchmal kann man erkennen, welche Modul man nehmen könnte, manchmal muss man einfach kleine Zahlen der Reihe nach ausprobieren.

a) $18a - 33b + 5(c+1) = 2c$
$\Rightarrow 0a - 0b + 2(c+1) \equiv 2c \mod 3$
$\Rightarrow 2 \equiv 0 \mod 3$, Widerspruch, also gibt es keine Lösung.

b) $98x + 84y + 91z = 215$
$\Rightarrow 0x + 0y + 0z \equiv 5 \mod 7$
$\Rightarrow 0 \equiv 5 \mod 7$, Widerspruch.

c) $x^2 + 1 = 3y$
$\Rightarrow x^2 + 1 \equiv 0y \mod 3$
$\Rightarrow x^2 \equiv -1 \mod 3$
$\Rightarrow x^2 \equiv 2 \mod 3$
Um zu erkennen, dass das nicht möglich ist, setzen wir einfach für x alle möglichen Restklassen ein: $0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 4 \equiv 1 \mod 3$. Als Ergebnis kam da nie 2 vor, ein Quadrat kann daher nie in der Restklasse $2 \mod 3$ liegen. Man sagt, dass 2 kein *quadratischer Rest* modulo 3 ist, während 0 und 1 sehr wohl *quadratische Reste* modulo 3 sind.

d) $a^2 + b^2 = 1234567$
$\Rightarrow a^2 + b^2 \equiv 3 \mod 4$
Durch Ausprobieren wie in c) sieht man, dass die quadratischen Reste modulo 4 genau 0 und 1 sind. Wenn man jetzt aber für a^2 und b^2 jede Kombination aus 0 und 1 einsetzt, kommt man nie auf 3, also hat die Gleichung keine Lösung.

6. Wir zeigen zuerst $a \equiv a' \mod m \Rightarrow ax \equiv a'x \mod m$, also dass man in einer Multiplikation eine der beiden Zahlen ersetzen darf:
$a \equiv a' \mod m \Rightarrow m|(a - a') \Rightarrow m|(a - a') \cdot x = ax - a'x \Rightarrow ax \equiv a'x \mod m$
Jetzt wenden wir das einfach zweimal an: Sei also $a \equiv a' \mod m$ und $b \equiv b' \mod m$, dann gilt $ab \equiv a'b \equiv a'b' \mod m$.

7. a) Wir rechnen nach, dass die Zahl modulo 5 und modulo 7 in der Restklasse 0 liegt, also durch 5 und 7 und damit auch durch 35 teilbar ist:
$7220 \cdot 832 - 713 \cdot 49831 - 982 \equiv 0 \cdot 2 - 3 \cdot 1 - 2 \equiv -5 \equiv 0 \mod 5$
$7220 \cdot 832 - 713 \cdot 49831 - 982 \equiv 3 \cdot 6 - 6 \cdot 5 - 2 \equiv -14 \equiv 0 \mod 7$

b) Genauso wie a), diesmal zerlegen wir $60 = 3 \cdot 4 \cdot 5$:
$2543 \cdot 913 + 105 \cdot (-9381) + 8329 \cdot 238 + 1044 \equiv 2 \cdot 1 + 0 \cdot (0) + 1 \cdot 1 + 0 \equiv 3 \equiv 0 \mod 3$
$2543 \cdot 913 + 105 \cdot (-9381) + 8329 \cdot 238 + 1044 \equiv 3 \cdot 1 + 1 \cdot (-1) + 1 \cdot 2 + 0 \equiv 4 \equiv 0 \mod 4$
$2543 \cdot 913 + 105 \cdot (-9381) + 8329 \cdot 238 + 1044 \equiv 3 \cdot 3 + 5 \cdot (-1) + 4 \cdot 3 + 4 \equiv 20 \equiv 0 \mod 5$

c) $2^{5182} - 1 \equiv (-1)^{5182} - 1 \equiv 1 - 1 \equiv 0 \mod 3$

d) $2021^{53} + 2022^{53} \equiv 6^{53} + 7^{53} \equiv 6^{53} + (-6)^{53} \equiv 6^{53} - 6^{53} \equiv 0 \mod 13$