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:*

$$\begin{aligned}
1 &\equiv 3 \mod 2\\
2 &\equiv 100 \mod 2\\
4 &\equiv 7 \mod 3\\
6 &\equiv 14 \mod 4\\
3 &\equiv 18 \mod 5
\end{aligned}$$

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:

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

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