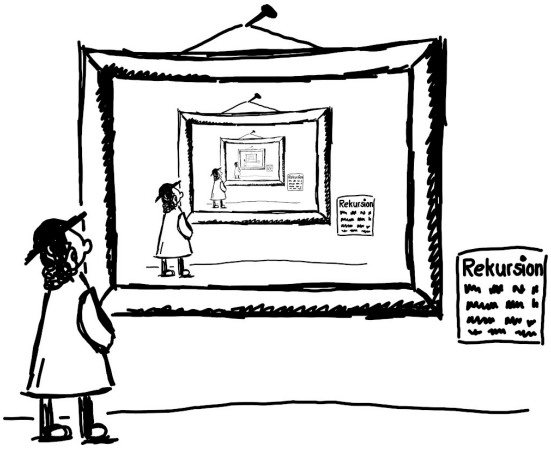
Universität Stuttgart

Beispielaufgabe zur Studienwahl

Rekursion und Prüfziffer: Rechnen mit Resten



Wir definieren die Folge $f_0, f_2, f_2, \ldots$ ganzer Zahlen durch ihre Startwerte $f_0 = 0$ und $f_1 = 2$ sowie die rekursive Vorschrift $f_n = 3f_{n-1} - f_{n-2}$ für alle $n \geq 2$.

Berechnen Sie die ersten sechs Folgenterme:

$f_0 =$ ☐ $f_1 =$ ☐ $f_2 =$ ☐

$f_3 =$ ☐ $f_4 =$ ☐ $f_5 =$ ☐

Berechnen Sie die letzte Dezimalziffer z_n von f_n:

$z_0 =$ ☐ $z_1 =$ ☐ $z_2 =$ ☐ $z_3 =$ ☐ $z_4 =$ ☐ $z_5 =$ ☐

$z_6 =$ ☐ $z_7 =$ ☐ $z_8 =$ ☐ $z_9 =$ ☐ $z_{10} =$ ☐ $z_{11} =$ ☐

Das Programm `rechneronline.de/summe/rekursion.php` behauptet $f_{39} = 17888788647582926$. Ist das korrekt?

- ☐ Ja, weil ich es nachgerechnet habe.
- ☐ Ja, weil die erste Ziffer richtig ist.
- ☐ Ja, weil die letzte Ziffer richtig ist.
- ☐ Nein, weil die erste Ziffer falsch ist.
- ☐ Nein, weil die letzte Ziffer falsch ist.
- ☐ Nein, weil diese Zahl keine Primzahl ist.

Bestimmen Sie die letzte Ziffer von f_p für $p = 12345678$: $z_p =$ ☐

Bestimmen Sie die letzte Ziffer von f_q für $q = 3^{3^{3^3}}$: $z_q =$ ☐

Weitere Aufgaben und Informationen unter:
Studienwahl-Kompass Mathematik
Universität Stuttgart

mathematik
fakultät8

Stufe 0 / Kurzantwort: Die gesuchten Folgenterme sind $f_0 = 0$, $f_1 = 2$, $f_2 = 6$, $f_3 = 16$, $f_4 = 42$, $f_5 = 110$ und deren letzte Ziffern $z_0 = 0$, $z_1 = 2$, $z_2 = 6$, $z_3 = 6$, $z_4 = 2$, $z_5 = 0$, $z_6 = 8$, $z_7 = 4$, $z_8 = 4$, $z_9 = 8$, $z_{10} = 0$ und $z_{11} = 2$. Danach wiederholen sich die letzten Ziffern alle zehn Folgenterme. Um z_n zu bestimmen, genügt es daher, die letzte Ziffer von n zu kennen.

Demnach endet f_{39} genauso wie f_9 mit der Ziffer $z_{39} = z_9 = 8$. Der vom Programm berechnete Wert kann nicht richtig sein, da er auf die letzte Ziffer 6 endet. Für $p = 12345678$ finden wir ebenso $z_p = z_8 = 4$. Die Zahl q endet auf 7, also gilt $z_q = z_7 = 4$.

Stufe 1 / Ausführung: Sie können die letzte Ziffer z_n auf verschiedenen Wegen berechnen; einige Rechenwege sind spürbar länger und mühsamer, andere sind geschickter und effizienter. Auch das ist Mathematik: Wir wollen nicht nur das korrekte Ergebnis, sondern auch einen effizienten Rechenweg! Der hier verwendete Trick heißt „Rechnen mit Restklassen“ oder „Modulo-Rechnung“. Im Folgenden erfahren Sie, wie das funktioniert und welche mathematischen Überlegungen dahinter stehen.

Berechnung von $f_0, \dots, f_5$: Die Folgenterme werden durch Einsetzen nacheinander berechnet:

$$f_0 = 0,\ f_1 = 2,\ f_2 = 3f_1 - f_0 = 6 - 0 = 6,\ f_3 = 16,\ f_4 = 42,\ f_5 = 110$$

Um die letzten Ziffern der Folgenterme zu berechnen, haben wir mehrere Möglichkeiten:

Mit brutaler Gewalt: Wir berechnen auch noch $f_6, \dots, f_{11}$ und nehmen dann die letzten Ziffern. Das ist mühsam, aber für die ersten Folgenterme von Hand noch machbar. Für z_{39} ist dies gerade noch möglich, aber schon lästig, für z_p mit $p = 12345678$ ist es menschlich unmöglich.

Mit geschlossener Formel: Wir konstruieren eine exakte geschlossene Formel für unsere Folge:

$$f_n = \frac{2}{\sqrt{5}}\left[\left(\frac{3+\sqrt{5}}{2}\right)^n - \left(\frac{3-\sqrt{5}}{2}\right)^n\right]$$

Steht die Formel erst einmal da, so können Sie sie leicht *überprüfen*. Wie Sie die Formel überhaupt erst *finden*, ist noch etwas raffinierter. Beides erklären wir ausführlich in Stufe 2.

Diese schöne Formel zeigt *näherungsweise* das Wachstumsverhalten für große n, denn die erste Potenz dominiert und beschert uns die Näherung $f_n \approx g_n := 0.894 \cdot 2.618^n$. Die Näherungswerte sind erstaunlich gut: $g_1 = 2.340\ldots$, $g_2 = 6.127\ldots$, $g_3 = 16.041\ldots$, $g_4 = 41.996\ldots$, $g_5 = 109.947\ldots$.

Die *exakte* Auswertung ist leider genauso mühsam wie zuvor und per Hand zudem fehleranfällig. Mit dieser Formel konkrete Folgenterme bis zur letzten Ziffer auszurechnen, ist nicht einfach.

Mit Modulo-Rechnung: Wir bemerken und nutzen, dass nur die letzte Ziffer z_n gesucht ist, und daher ist es gar nicht nötig, den Folgenterm f_n komplett auszurechnen. Um die letzte Ziffer z_n zu bestimmen, genügt es bereits, die vorigen letzten Ziffern z_{n-1} und z_{n-2} zu kennen.

Überlegung 1: Positivität aller Folgenterme. Nach den ersten Werten $f_0 = 0$, $f_1 = 2$, $f_2 = 6$, $f_3 = 16$, $f_4 = 42$, $f_5 = 110$ vermuten wir: $0 = f_0 < f_1 < f_2 < f_3 < \dots$, insbesondere ist f_n positiv für alle $n \geq 1$. Das können wir leicht nachrechnen: Zunächst gilt $f_0 = 0 < 2 = f_1$. Angenommen, wir haben bereits $0 = f_0 < f_1 < \dots < f_{n-1} < f_n$. Dann folgt

$$f_{n+1} = 3f_n - f_{n-1} = 2f_n + \underbrace{f_n - f_{n-1}}_{>0} > 2f_n > f_n,$$

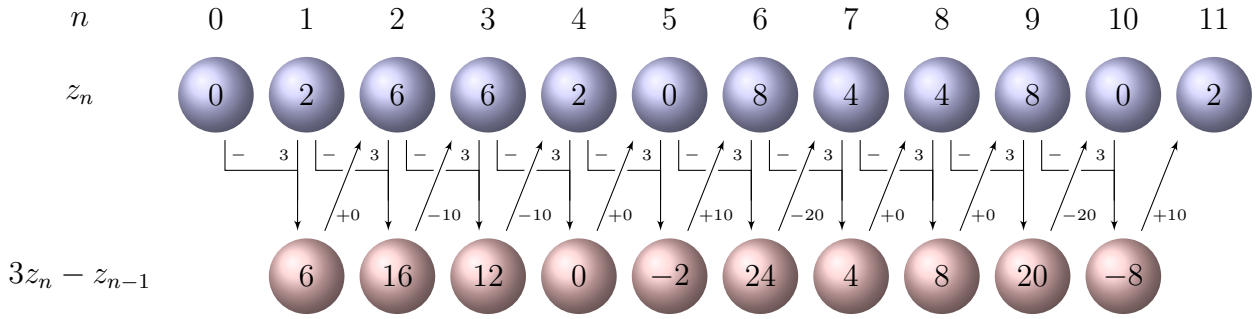
also gilt $0 = f_0 < f_1 < \dots < f_{n-1} < f_n < f_{n+1}$. So fortfahrend erhalten wir Schritt für Schritt die vermuteten Ungleichungen $0 = f_0 < f_1 < f_2 < f_3 < \dots$, also $f_n < f_{n+1}$ für alle $n \in \mathbb{N}$.

Überlegung 2: Berechnung der letzten Ziffern. Für jede natürliche Zahl $f \in \mathbb{N}$ ist die letzte Ziffer z der Rest der Division von f durch 10. Ausgeschrieben gilt also $f = 10s + z$ mit $s, z \in \mathbb{N}$ und $0 \leq z < 10$. Allgemein dividieren wir $a \in \mathbb{Z}$ durch $b \in \mathbb{Z}$ mit $b > 0$ und erhalten $a = bs + r$ mit Quotient $s \in \mathbb{Z}$ und Rest $0 \leq r < b$. Wir schreiben kurz $r = a \operatorname{rem} b$ (engl. *remainder*).

Aus $f_{n-1} = 10s_{n-1} + z_{n-1}$ und $f_{n-2} = 10s_{n-2} + z_{n-2}$ berechnen wir

$$\begin{aligned} f_n = 3f_{n-1} - f_{n-2} &= 3 \cdot (10s_{n-1} + z_{n-1}) - (10s_{n-2} + z_{n-2}) \\ &= 10 \cdot (3s_{n-1} - s_{n-2}) + (3z_{n-1} - z_{n-2}). \end{aligned}$$

Das bedeutet $z_n = f_n \operatorname{rem} 10 = 3z_{n-1} - z_{n-2} \operatorname{rem} 10$. Anders gesagt: Wir berechnen $3z_{n-1} - z_{n-2}$ und addieren bzw. subtrahieren so oft 10, bis wir die ersehnte Ziffer $z_n \in \{0, 1, \ldots, 9\}$ erhalten.



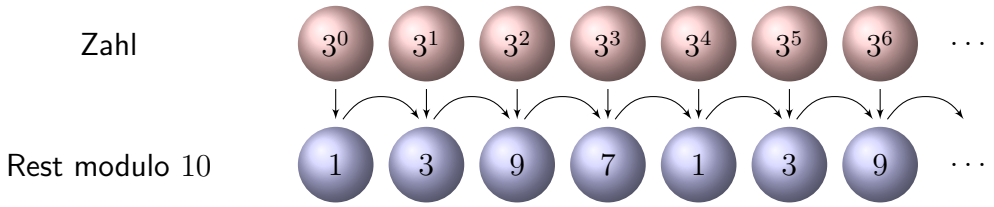
Mit diesem Trick können wir die Ziffern z_n einfacher und schneller bestimmen, sogar im Kopf!

Déjà Vu: Die letzten beiden Werte sind eine 0 gefolgt von einer 2. Das hatten wir schon ganz am Anfang! Damit beginnt alles wieder von vorne und wiederholt sich immer in Zehnerschritten: Für alle natürlichen Zahlen $n, k \in \mathbb{N}$ gilt $z_{n+10k} = z_n$. Wollen Sie also z_n ausrechnen, so genügt es, die letzte Ziffer $i = n \operatorname{rem} 10$ zu kennen, denn dann gilt $z_n = z_i$. Mit diesem Trick müssen Sie nun überhaupt nicht mehr rechnen, sondern können den Wert z_i einfach in obiger Tabelle nachschlagen!

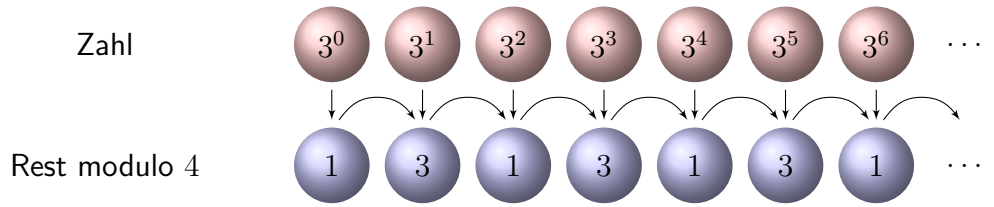
Prüfziffer: Die letzte Ziffer $z_{39} = f_{39} \operatorname{rem} 10$ lesen wir ebenso leicht ab: $z_{39} = z_9 = 8$. Dies widerspricht dem Ergebnis, das das Programm `rechneronline.de/summe/rekursion.php` liefert. So enttarnen Sie diesen (Rundungs-)Fehler: mit wenig Aufwand, aber mathematischer Finesse!

Große Zahlen: Ebenso leicht können wir $z_p = f_p \operatorname{rem} 10$ für $p = 12345678$ bestimmen: $z_p = z_8 = 4$.

Astronomisch große Zahlen: Mit demselben Trick berechnen wir $z_q = f_q \operatorname{rem} 10$ für $q = 3^{3^{3^3}}$. Dazu berechnen wir $i = q \operatorname{rem} 10$ und nutzen $z_q = z_i$. Für $n = 0, 1, 2, \ldots, 3^3, \ldots$ berechnen wir $3^n \operatorname{rem} 10$:



Diese Potenzfolge $a_n = 3^n$ entsteht durch die Rekursion $a_0 = 1$ und $a_n = 3a_{n-1}$ für $n = 1, 2, 3, \ldots$ und unsere obigen Überlegungen übertragen sich. Die letzte Ziffer $3^n \operatorname{rem} 10$ wiederholt sich alle vier Schritte. Für $n = 4k + r$ haben 3^n und 3^r dieselbe letzte Ziffer. Speziell für $n = 3^{3^3}$ wollen wir also $r = n \operatorname{rem} 4$ berechnen. Wie zuvor untersuchen wir dazu $3^m \operatorname{rem} 4$ für $m = 0, 1, 2, \ldots, 3^3, \ldots$:



Demnach gilt $3^m \operatorname{rem} 4 = 1$, falls m gerade ist, und $3^m \operatorname{rem} 4 = 3$, falls m ungerade ist. In den drei Grafiken lesen wir nun von unten nach oben ab: Da $m = 3^3$ ungerade ist, bleibt für $n = 3^m = 3^{3^3}$ der Rest $n \operatorname{rem} 4 = 3$. Also ist $q \operatorname{rem} 10 = 3^n \operatorname{rem} 10 = 7$ und daher $z_q = z_7 = 4$.

Stufe 2 / Was will und soll diese Aufgabe?

Nach der Lösung dieser Aufgabe erläutern wir als Rück- und Ausblick, warum wir diese Problemstellung mathematisch interessant finden und inwiefern sie repräsentativ ist für das Mathematikstudium.

Zunächst lernen Sie an dieser Aufgabe: Vertrauen Sie nicht blind einem Computerprogramm! Seien Sie achtsam und prüfen Sie, ob numerische Ergebnisse stimmig und sinnvoll sind. Programme machen nicht immer das, was man denkt oder wünscht. Daher ist es wichtig, Hintergründe zu kennen, Ergebnisse zu hinterfragen und auf Plausibilität zu prüfen. Im Studium lernen Sie die mathematischen Grundlagen und Methoden, um diese selbstständig, sicher, kritisch, korrekt und kreativ anzuwenden!

Hier illustrieren wir Rekursion und Induktion. **Rekursion** ist eine grundlegende Konstruktionsmethode in Mathematik und Informatik und vielen Anwendungen. Die berühmte Fibonacci-Folge zum Beispiel beschreibt die Größe a_n einer Kaninchenpopulation zur Zeit $n = 0, 1, 2, \ldots$; sie entsteht durch die Startwerte $a_0 = a_1 = 1$ und die Rekursionsvorschrift $a_n = a_{n-1} + a_{n-2}$ für alle $n \geq 2$.

Eng verbunden mit der Rekursion ist die **Induktion** als grundlegende Beweismethode. Beides sind Universalwerkzeuge, die Sie daher gleich zu Beginn des Studiums erlernen. Die Rekursion dient zur Konstruktion einer Folge, die Induktion dient zum Nachweis einer Aussage. Zu zeigen ist eine

- Behauptung: Für alle natürlichen Zahlen $n \in \mathbb{N}$ mit $n \geq m$ gilt die Aussage $A(n)$.

Diese zeigen wir mittels vollständiger Induktion durch Nachweis der beiden folgenden Aussagen:

- Induktionsanfang: Es gilt die erste Aussage $A(m)$ für den vorgegebenen Startwert m.
- Induktionsschritt: Für jede natürliche Zahl $n \geq m$ gilt: Aus $A(n)$ folgt $A(n+1)$.

Die Idee ist sehr anschaulich: Es gilt $A(m)$. Daraus folgt $A(m+1)$. Daraus folgt $A(m+2)$. Daraus folgt $A(m+3)$. Und so weiter. Die sorgfältige Ausformulierung sind genau die beiden obigen Punkte: Induktionsanfang und Induktionsschritt. Zwei einfache Beispiele aus Stufe 1 sollen dies illustrieren.

Behauptung 1: Für alle $n \geq 1$ gilt die Aussage $A(n)$: $f_n > f_{n-1} \geq 0$.

Beweis: Wir nutzen das Prinzip der vollständigen Induktion.

- Induktionsanfang: Die Aussage $A(1)$ gilt, denn $f_1 = 2$ und $f_0 = 0$, also $f_1 > f_0 \geq 0$.
- Induktionsschritt: Gegeben sei $n \geq 1$ und die gültige Aussage $A(n)$, also $f_n > f_{n-1} \geq 0$. Daraus folgt $f_{n+1} = 2f_n + f_n - f_{n-1} > 2f_n > f_n > 0$. Somit gilt die Aussage $A(n+1)$. □

Bemerkung: Wichtig sind sowohl Induktionsschritt als auch Induktionsanfang. Für die Startwerte $f_0 = 3$ und $f_1 = 1$ zeigt die Folge $f_2 = 0$, $f_3 = -1$, $f_4 = -3$, usw. ein ganz anderes Verhalten!

Bemerkung: Oft wird das Prinzip der vollständigen Induktion in einer **starken Formulierung** verwendet: Eigentlich wollen wir die Aussagen $A(n)$ für alle $n \geq m$ zeigen. Dazu zeigen wir für alle $n \geq m$ die scheinbar stärkere Aussage $B(n)$: Für alle $k \in \mathbb{N}$ mit $m \leq k \leq n$ gilt $A(k)$. Das bedeutet konkret: Im Induktionsschritt folgern wir aus $A(k)$ für alle k mit $m \leq k \leq n$ die Aussage $A(n+1)$. Beide Formulierungen sind logisch äquivalent, die schwache ist sparsamer, die starke ist bequemer.

In Stufe 1 haben wir angekündigt, die geschlossene Formel zu überprüfen. Mit dem richtigen Werkzeug gelingt dies nun leicht und wir können sie für alle $n \in \mathbb{N}$ beweisen, sehr elegant und effizient.

Behauptung 2: Für alle $n \geq 0$ gilt die Aussage $A(n)$: $f_n = g_n := \frac{2}{\sqrt{5}}\left[\left(\frac{3+\sqrt{5}}{2}\right)^n - \left(\frac{3-\sqrt{5}}{2}\right)^n\right]$.

Beweis: Wir nutzen das Prinzip der vollständigen Induktion (in der starken Formulierung).

- Induktionsanfang: Die ersten beiden Aussagen $A(0)$ und $A(1)$ sind wahr, denn wir berechnen $g_0 = \frac{2}{\sqrt{5}}\left[\left(\frac{3+\sqrt{5}}{2}\right)^0 - \left(\frac{3-\sqrt{5}}{2}\right)^0\right] = \frac{2}{\sqrt{5}}(1-1) = 0$ und $g_1 = \frac{2}{\sqrt{5}}\left[\left(\frac{3+\sqrt{5}}{2}\right)^1 - \left(\frac{3-\sqrt{5}}{2}\right)^1\right] = 2$.
- Induktionsschritt: Es gelte $f_k = g_k$ für $k \leq n$. Geduldig rechnet man zuerst $g_{n+1} = 3g_n - g_{n-1}$ nach. (Versuchen Sie dies als Übung!) Nach Voraussetzung gilt $g_n = f_n$ und $g_{n-1} = f_{n-1}$, also folgt $g_{n+1} = 3g_n - g_{n-1} = 3f_n - f_{n-1} = f_{n+1}$. Somit gilt die Aussage $A(n+1)$. □

Auf der Suche nach einer geschlossenen Formel. Mit Induktion können wir die geschlossene Formel für f_n leicht nachprüfen, aber wie kommen wir auf eine solche Formel? Zufällig erraten wird man diese Formel wohl kaum. Wir suchen daher eine möglichst allgemeine Lösungsmethode!

Für die einfachere Folge $a_0 = 5$ und $a_n = 3a_{n-1}$ ist die Formel leicht zu finden: Es gilt $a_n = 5 \cdot 3^n$. Das bringt uns auf die Idee, eine Formel $f_n = \lambda \cdot b^n$ zu versuchen. Das nennt man die **Ansatzmethode**: Wir machen einen (geschickt geratenen) Ansatz und bestimmen die noch freien Parameter λ und b. Wir setzen zunächst $f_n = b^n$ in die Rekursionsgleichung $f_n = 3f_{n-1} - f_{n-2}$ ein und erhalten

$$b^n = 3b^{n-1} - b^{n-2}.$$

Es genügt, für $n = 2$ die Gleichung $b^2 = 3b - 1$ zu erfüllen, alle höheren Gleichungen folgen daraus. Für die quadratische Gleichung $b^2 = 3b - 1$ berechnen wir dank Mitternachtsformel die beiden Lösungen $b_{1/2} = \frac{3 \pm \sqrt{5}}{2}$. Wir erhalten daher zwei Lösungen der Rekursionsgleichung $g_n = \left(\frac{3+\sqrt{5}}{2}\right)^n$ und $h_n = \left(\frac{3-\sqrt{5}}{2}\right)^n$. Leider erfüllt keine der beiden unsere Anfangsbedingungen $f_0 = 0$ und $f_1 = 2$.

Sind wir gescheitert? Hier rettet uns **Linearität**: Auch jede Linearkombination $f_n = \lambda g_n + \mu h_n$ mit $\lambda, \mu \in \mathbb{R}$ erfüllt die Rekursionsgleichung. Können wir λ und μ so wählen, dass unsere Anfangsbedingungen erfüllt sind? Für $n = 0$ muss $f_0 = 0$ gelten, also $\lambda + \mu = 0$. Für $n = 1$ muss $f_1 = 2$ gelten, also $\lambda b_1 + \mu b_2 = 2$. Dieses lineare Gleichungssystem hat die eindeutige Lösung $\lambda = \frac{2}{\sqrt{5}}$, $\mu = -\frac{2}{\sqrt{5}}$. (Übung!) Wir erhalten so die ersehnte geschlossene Formel:

$$f_n = \tfrac{2}{\sqrt{5}}\left[\left(\tfrac{3+\sqrt{5}}{2}\right)^n - \left(\tfrac{3-\sqrt{5}}{2}\right)^n\right]$$

Alternativ erhalten Sie die geschlossene Formel mit Matrizenrechnung und Diagonalisierung. Wie das genau funktioniert, lernen Sie im ersten Studienjahr in der Vorlesung **Lineare Algebra**.

Stufe 3 / Mathematische Grundlage: Modulo-Rechnung.

Das Rechnen mit Resten, kurz Modulo-Rechnung, ist überall nützlich. In unserem Beispiel haben wir mit der „Prüfziffer“ leicht nachgewiesen, dass das Computerprogramm falsch gerechnet hat. Modulo-Rechnung spielt ebenso in der **Kryptographie** eine zentrale Rolle. Das klassische RSA-Verfahren und viele nachfolgende asymmetrische Verschlüsselungsverfahren, basieren auf Modulo-Rechnung: Mit dem öffentlichen Schlüssel (*public key*) kann jeder seine Daten verschlüsseln. Aber nur wer den privaten Schlüssel (*private key*) kennt, kann die Daten wieder entschlüsseln.

Beim Lösen der Aufgabe haben wir beobachtet, dass es reicht, nur auf die letzten Ziffern zu achten, also auf die Reste bei Division durch 10. Später wurden Reste bei Division durch 4 bzw. durch 2 betrachtet. Dies kann man mathematisch genauer beschreiben, formalisieren und verallgemeinern:

Wir fixieren eine natürliche Zahl $m \in \mathbb{N}_{\geq 1}$. Wir nennen zwei ganze Zahlen a und b *kongruent modulo* m, geschrieben $a \equiv b \pmod{m}$, falls ihre Differenz $a - b$ durch m teilbar ist, und zwar ganzzahlig ohne Rest. Die Bedingung $a \equiv b \mod m$ ist äquivalent zu $a \operatorname{rem} m = b \operatorname{rem} m$.

Beispiel: Modulo $m = 7$ gilt $1 \equiv 8$, $2 \equiv 23$ und $-11 \equiv 3$. Die Präzisierung $\mod 7$ lassen wir weg.

Alle Zahlen, die zu $a \in \mathbb{Z}$ kongruent modulo m sind, wollen wir zusammenfassen und wie ein einziges Element behandeln: Die Kongruenzklasse $[a] := \{\, b \in \mathbb{Z} \mid a \equiv b \pmod{m} \,\}$ ist die Menge aller ganzen Zahlen b, die zu a kongruent sind. Genau dann gilt $[a] = [b]$, wenn $a \equiv b \pmod{m}$ ist.

Beispiel: Modulo $m = 10$ erhalten wir genau zehn verschiedene Kongruenzklassen:

$$\begin{aligned}
[0] &= \{\ldots, -20, -10, 0, 10, 20, \ldots\}, \\
[1] &= \{\ldots, -19, -9, 1, 11, 21, \ldots\}, \\
&\ldots, \\
[9] &= \{\ldots, -11, -1, 9, 19, 29, \ldots\}.
\end{aligned}$$

Jede ganze Zahl a gehört zu genau einer dieser Kongruenzklassen, nämlich zu $[a \operatorname{rem} 10]$.

Allgemein erhalten wir die Menge $\mathbb{Z}/m = \{\,[0],[1],\ldots,[m-1]\,\}$ aller Kongruenzklassen von $\mathbb{Z}$ modulo m. Kongruenzklassen können wir addieren durch $[a]+[b] := [a+b]$ und multiplizieren durch $[a]\cdot[b] := [a\cdot b]$. In Worten: Um zwei Kongruenzklassen zu verknüpfen, wählen wir daraus je ein Element a und b, verknüpfen diese, und bilden dazu die Kongruenzklasse. Hierbei ist Vorsicht geboten, denn wir müssen willkürlich Elemente wählen, und es ist keineswegs klar, ob das Ergebnis von unseren Wahlen abhängt. Das tut es wundersamerweise nicht! Hier einige Beispiele:

In $\mathbb{Z}$ gilt	$67+34=101,$	$67\cdot 34=2278,$
	$(-3)+24=21,$	$(-3)\cdot 24=-72,$
	$17+(-6)=11,$	$17\cdot(-6)=-102.$
In $\mathbb{Z}/10$ gilt	$[7]+[4]=[1],$	$[7]\cdot[4]=[8].$

Allgemein müssen wir folgendes nachrechnen: Aus $[a]=[a']$ und $[b]=[b']$ folgt $[a+b]=[a'+b']$ und $[a\cdot b]=[a'\cdot b']$. Versuchen Sie dies als Übung! Oder freuen Sie sich auf das Mathematikstudium!

Die folgenden Tabellen zeigen Addition und Multiplikation in der Menge $\mathbb{Z}/10$:

$+$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[7]	[8]	[9]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[7]	[8]	[9]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[7]	[8]	[9]	[0]	[1]	[2]	[3]	[4]	[5]
[7]	[7]	[8]	[9]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[8]	[8]	[9]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[9]	[9]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]

$\cdot$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
[2]	[0]	[2]	[4]	[6]	[8]	[0]	[2]	[4]	[6]	[8]
[3]	[0]	[3]	[6]	[9]	[2]	[5]	[8]	[1]	[4]	[7]
[4]	[0]	[4]	[8]	[2]	[6]	[0]	[4]	[8]	[2]	[6]
[5]	[0]	[5]	[0]	[5]	[0]	[5]	[0]	[5]	[0]	[5]
[6]	[0]	[6]	[2]	[8]	[4]	[0]	[6]	[2]	[8]	[4]
[7]	[0]	[7]	[4]	[1]	[8]	[5]	[2]	[9]	[6]	[3]
[8]	[0]	[8]	[6]	[4]	[2]	[0]	[8]	[6]	[4]	[2]
[9]	[0]	[9]	[8]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

Übung: Schreiben Sie für $\mathbb{Z}/m$ mit $m=2,3,4,5$ die Additions- und Multiplikationstabelle aus.

Die Konstruktion von $\mathbb{Z}/m$ ist raffiniert und grundlegend. Was ist der Nutzen? Die neue Schreibweise für Addition und Multiplikation ist kurz und präzise und daher für Rechnungen sehr effizient. Wir illustrieren dies, indem wir unsere obigen Rechnungen kurz, präzise und elegant formulieren:

Behauptung 3: Für alle $n\geq 10$ gilt die Aussage $A(n)$: $[f_n]=[f_{n-10}]$.

Beweis: Wir nutzen das Prinzip der vollständigen Induktion (in der starken Formulierung).

- Induktionsanfang: Für $n=10$ und $n=11$ rechnet man $A(n)$ einfach nach, wie oben gezeigt.
- Induktionsschritt: Sei $n\geq 11$ und für alle k mit $10\leq k\leq n$ gelte $A(k)$. Somit gelten die Aussagen $A(n-1)$: $[f_{n-1}]=[f_{n-11}]$ und $A(n)$: $[f_n]=[f_{n-10}]$. Damit folgt $A(n+1)$, denn $[f_{n+1}]=[3f_n-f_{n-1}]=[3][f_n]-[f_{n-1}]=[3][f_{n-10}]-[f_{n-11}]=[3f_{n-10}-f_{n-11}]=[f_{n-9}]$. □

Behauptung 4: Für alle $n\geq 0$ gilt $A(n)$: $[f_n]=[f_{n\,\mathrm{rem}\,10}]$, für die letzten Ziffern also $z_n=z_{n\,\mathrm{rem}\,10}$.

Beweis: Wir nutzen das Prinzip der vollständigen Induktion (in der starken Formulierung).

- Induktionsanfang: Die Aussage $A(n)$ gilt für $n=0,1,\ldots,9$, denn hier ist $n=n\,\mathrm{rem}\,10$.
- Induktionsschritt: Sei $n\geq 10$ und für alle k mit $0\leq k<n$ gelte die Aussage $A(k)$. Wir nutzen $n'=n-10\geq 0$ und $n'\,\mathrm{rem}\,10=n\,\mathrm{rem}\,10$. Dank Behauptung 3 und Induktionsvoraussetzung $A(n')$ gilt $[f_n]=[f_{n'}]=[f_{n'\mathrm{rem}10}]=[f_{n\mathrm{rem}10}]$. □

Die weiteren Rechnungen modulo 4 bzw. 2 lassen sich ebenso elegant formulieren. Versuchen Sie dies als Übung! Auch dies ist eine Stärke der Mathematik: Dank guter und präziser Notation werden unsere Rechnungen übersichtlicher und leichter. Abstraktion hilft ganz konkret!