Lösungen zum Thema Zahlentheorie I

Lösung zu Aufgabe 1. Bezeichne die Wochentage Sonntag, Montag, Dienstag, ..., Samstag mit 0, 1, 2, ..., 6. Wenn heute Samstag (6) ist, dann ist der Rest beim Teilen von $6 + 100$ durch 7 unser gesuchter Wochentag. Weil 105 durch 7 teilbar ist, gilt $106 \equiv 1 \pmod 7$, also ist in 100 Tagen Montag.

Lösung zu Aufgabe 2.

1. Es gilt $22 \equiv -2 \pmod{12}$, weil $22 - (-2) = 24 = 2 \cdot 12$ durch 12 teilbar ist. $7 - 4 = 3$ ist nicht durch 11 teilbar, also gilt nicht $7 \equiv 4 \pmod{11}$.
2. $39 \equiv 4 \pmod n$ bedeutet gerade, dass $39 - 4 = 35$ durch n teilbar ist. Daher sind alle möglichen Werte für n die positiven Teiler von $39 - 4 = 35 = 5 \cdot 7$, also $n = 1, 5, 7, 35$.

Lösung zu Aufgabe 3.

1. Wegen $107 \equiv -3 \pmod{10}$ gilt nach Eigenschaft (M) $107 \cdot 107 \equiv (-3) \cdot (-3) \pmod 7$. Wiederholtes Anwenden der Eigenschaft (M) liefert
$$\underbrace{107 \cdot 107 \cdot \ldots \cdot 107}_{107\text{-mal}} = \underbrace{(-3) \cdot (-3) \cdot \ldots \cdot (-3)}_{107\text{-mal}} \pmod{10}.$$
Wir berechnen (es gilt $107 = 4 \cdot 26 + 3$):
$$\begin{aligned}(-3)^{107} &= \underbrace{(-3) \cdot (-3) \cdot \ldots \cdot (-3)}_{107\text{-mal}} \\ &= \underbrace{[(-3) \cdot (-3) \cdot (-3) \cdot (-3)] \cdot \ldots \cdot [(-3) \cdot (-3) \cdot (-3) \cdot (-3)]}_{26\text{-mal}} \cdot (-3) \cdot (-3) \cdot (-3) \\ &= \underbrace{81 \cdot 81 \cdot \ldots \cdot 81}_{26\text{-mal}} \cdot (-27) = 81^{26} \cdot (-27).\end{aligned}$$
Es ist $81 \equiv 1 \pmod{10}$, daher gilt $81^{26} \equiv 1^{26} \equiv 1 \pmod{10}$ nach Eigenschaft (M). Wir setzen zusammen:
$$107^{107} \equiv 81^{26} \cdot (-27) \equiv -27 \equiv 3 \pmod{10}.$$
Also ist $x = 3$.

Schülerzirkel Mathematik, Fakultät für Mathematik, 93040 Regensburg
http://www.mathematik.uni-r.de/schuelerzirkel, schueler.zirkel@mathematik.uni-regensburg.de

2. Schreiben wir E für die letzte Ziffer von 107^{107}, so ist $107^{107} - E$ durch 10 teilbar, das heißt $107^{107} \equiv E \pmod{10}$. Auch für $x = 3$ gilt $107^{107} \equiv x \pmod{10}$. Daher gilt $E \equiv x \pmod{10}$, das heißt $E - x$ ist durch 10 teilbar. Weil x und E beide zwischen 0 und 9 liegen, muss $E - x = 0$ gelten, also $E = x = 3$.

Lösung zu Aufgabe 4. Analog zu Beispiel 6 reicht es zu zeigen, dass die Gleichung modulo 5 keine Lösung besitzt. Dazu zeigen wir $a^5 - 6a + 3 \not\equiv 0 \pmod 5$ für jede Wahl von a zwischen 0 und 4. Wir berechnen:

$a \equiv 0$: $0^5 - 6 \cdot 0 + 3 \equiv 3 \not\equiv 0 \pmod 5$.

$a \equiv 1$: $1^5 - 6 \cdot 1 + 3 \equiv -2 \not\equiv 0 \pmod 5$.

$a \equiv 2$: $2^5 - 6 \cdot 2 + 3 \equiv 23 \not\equiv 0 \pmod 5$.

$a \equiv 3$: $3^5 - 6 \cdot 3 + 3 \equiv 228 \not\equiv 0 \pmod 5$.

$a \equiv 4$: $4^5 - 6 \cdot 4 + 3 \equiv 1003 \not\equiv 0 \pmod 5$.

Lösung zu Aufgabe 5. Wir unterteilen die Lösung in drei Schritte.

Schritt 1 Jede natürliche Zahl ist modulo 3 gleich ihrer Quersumme. Wir werden diese Aussage weiter unten allgemein beweisen. Dazu werden wir aber mehrere Variablen gleichzeitig betrachten müssen, weshalb man im Beweis die Übersicht verlieren kann. Da die Beweisstrategie für jede Zahl gleich ist, beweisen wir die Aussage zuerst für die Zahl 100091. Schreibe

$$\begin{aligned} 100091 &= 1 \cdot 100000 + 9 \cdot 10 + 1 \cdot 1 \\ &= 1 \cdot (99999 + 1) + 9 \cdot (9 + 1) + 1 \cdot 1 \\ &= [1 \cdot 99999 + 9 \cdot 9] + [1 \cdot 1 + 9 \cdot 1 + 1 \cdot 1] \\ &= 3 \cdot [1 \cdot 33333 + 9 \cdot 3] + \underbrace{[1 + 9 + 1]}_{\text{Quersumme von 100091}} \end{aligned}$$

Wegen $3 \cdot [1 \cdot 33333 + 9 \cdot 3] \equiv 0 \pmod 3$ folgt

$$100091 \equiv (\text{Quersumme von } 100091) \pmod 3.$$

Allgemeiner Beweis: Wir schreiben eine beliebige natürliche Zahl x in der Form

$$a_d a_{d-1} a_{d-2} \ldots a_2 a_1 a_0,$$

wobei $a_d, a_{d-1}, \ldots a_1, a_0$ die Ziffern dieser Zahl sind. Dann gilt

$$
\begin{aligned}
x &= a_d \cdot 10^d + a_{d-1} \cdot 10^{d-1} + \ldots + a_1 \cdot 10 + a_0 \cdot 1 \\
&= a_d \cdot (\underbrace{9 \ldots 9}_{\text{d-mal}} + 1) + a_{d-1} \cdot (\underbrace{9 \ldots 9}_{\text{(d-1)-mal}} + 1) + \ldots + a_1 \cdot (9+1) + a_0 \cdot 1 \\
&= \left[a_d \cdot \underbrace{9 \ldots 9}_{\text{d-mal}} + a_{d-1} \cdot \underbrace{9 \ldots 9}_{\text{(d-1)-mal}} + \ldots + a_1 \cdot 9 \right] + \left[a_d \cdot 1 + a_{d-1} \cdot 1 + \ldots + a_1 \cdot 1 + a_0 \cdot 1 \right] \\
&= 3 \cdot \left[a_d \cdot \underbrace{3 \ldots 3}_{\text{d-mal}} + a_{d-1} \cdot \underbrace{3 \ldots 3}_{\text{(d-1)-mal}} + \ldots + a_1 \cdot 3 \right] + \underbrace{\left[a_d + a_{d-1} + \ldots + a_1 + a_0 \right]}_{\text{Quersumme von } x}
\end{aligned}
$$

Da der linke Summand $\equiv 0 \pmod 3$ ist, folgt $x \equiv (\text{Quersumme von } x) \pmod 3$.

Schritt 2 Als nächstes zeigen wir, dass eine Quadratzahl n^2 nicht gleich 2 modulo 3 sein kann. Für Modulo 3 gibt es drei Fälle:

$n \equiv 0 \pmod 3$, dann gilt $n^2 \equiv 0^2 \equiv 0 \not\equiv 2 \pmod 3$.

$n \equiv 1 \pmod 3$, dann gilt $n^2 \equiv 1^2 \equiv 1 \not\equiv 2 \pmod 3$.

$n \equiv 2 \pmod 3$, dann gilt $n^2 \equiv 2^2 \equiv 4 \not\equiv 2 \pmod 3$.

Schritt 3 Zusammen bekommen wir für eine Quadratzahl n^2

$$(\text{Quersumme von } n^2) \equiv n^2 \not\equiv 2 \pmod 3.$$

Lösung zu Aufgabe 6.

1. Man berechnet

$$
\begin{aligned}
&1 \cdot 4 + 2 \cdot 7 + 3 \cdot 0 + 4 \cdot 8 + 5 \cdot 0 + 6 \cdot 5 + 7 \cdot 9 + 8 \cdot 7 + 9 \cdot 8 \\
= &4 + 14 + 32 + 30 + 63 + 56 + 72 = 271.
\end{aligned}
$$

Wegen $271 \equiv 7 \not\equiv 1 \pmod{11}$ ist der Ausweis also gefälscht.

2. Berechne

$$
\begin{aligned}
&1 \cdot 7 + 2 \cdot 6 + 3 \cdot 6 + 4 \cdot 9 + 5 \cdot 8 + 6 \cdot 7 + 7 \cdot 9 + 8 \cdot 8 + 9 \cdot 8 \\
= &7 + 12 + 18 + 36 + 40 + 42 + 63 + 64 + 72 = 354, \\
&354 \equiv 2 \pmod{11}.
\end{aligned}
$$

Die Prüfziffer ist also 2.

3. Zum Beispiel hat 100000001 die Prüfziffer X, denn es gilt

$$1 \cdot 1 + 1 \cdot 9 \equiv 10 \pmod{11}.$$

4. Schreibe a_i für die Ziffer an i-ter Stelle (für $1 \leq i \leq 9$) und p für die Prüfziffer, das heißt die anfänglich gültige Ausweisnummer schreibt sich $a_1 a_2 \dots a_8 a_9(p)$. Es gibt zwei Fälle:

   Fall 1: Die Prüfziffer p wird mit einer Ziffer a_j vertauscht:

   $$a_1 a_2 \dots a_{j-1} a_j a_{j+1} \dots a_9(p) \quad \longrightarrow \quad a_1 a_2 \dots a_{j-1} p a_{j+1} \dots a_9(a_j)$$

   Wir müssen zeigen, dass in der Nummer

   $$a_1 a_2 \dots a_{j-1} p a_{j+1} \dots a_9(a_j)$$

   die Prüfziffer a_j falsch ist. Dazu ist

   $$1 \cdot a_1 + 2 \cdot a_2 + \dots (j-1) \cdot a_{j-1} + j \cdot p + (j+1) \cdot a_{j+1} + \dots + 9 \cdot a_9 \not\equiv a_j \pmod{11}$$

   zu zeigen. Berechne modulo 11

   $$\begin{aligned} & 1 \cdot a_1 + 2 \cdot a_2 + \dots + (j-1) \cdot a_{j-1} + j \cdot p + (j+1) \cdot a_{j+1} + \dots + 9 \cdot a_9 \\ \equiv\ & 1 \cdot a_1 + 2 \cdot a_2 + \dots + (j-1) \cdot a_{j-1} + j \cdot a_j + (j+1) \cdot a_{j+1} + \dots + 9 \cdot a_9 + (j \cdot p - j \cdot a_j) \\ \equiv\ & p + (j \cdot p - j \cdot a_j) \quad \text{(die anfängliche Ausweisnummer ist gültig)} \end{aligned}$$

   Wir zeigen mit einem indirekten Beweis (siehe Hinweisblatt *Wie beweise ich etwas?*), dass

   $$1 \cdot a_1 + 2 \cdot a_2 + \dots (j-1) \cdot a_{j-1} + j \cdot p + (j+1) \cdot a_{j+1} + \dots + 9 \cdot a_9 \not\equiv a_j \pmod{11}$$

   gilt. Nehmen wir das Gegenteil an, so würde

   $$p + (j \cdot p - j \cdot a_j) \equiv a_j \pmod{11}$$

   gelten. Also wäre

   $$p + (j \cdot p - j \cdot a_j) - a_j = (j+1)(p - a_j)$$

   durch 11 teilbar und damit 11 ein Primfaktor in der Primfaktorzerlegung von $(j+1)(p-a_j)$. Dann wäre $j+1$ oder $p - a_j$ durch 11 teilbar, was nicht sein kann wegen $1 \leq j \leq 9$, $0 \leq a_j \leq 9$, $0 \leq p \leq 10$, $p \neq a_j$. Deshalb ist unsere Annahme falsch. Also hat die neue Nummer die falsche Prüfziffer.

   Fall 2: Zwei verschiedene Ziffern a_i, a_j werden vertauscht:

   $$a_1 a_2 \dots a_{i-1} a_i a_{i+1} \dots a_{j-1} a_j a_{j+1} \dots a_9(p) \quad \longrightarrow \quad a_1 a_2 \dots a_{i-1} a_j a_{i+1} \dots a_{j-1} a_i a_{j+1} \dots a_9(p)$$

   Wir zeigen, dass p nicht die Prüfziffer von der neuen Ausweisnummer sein kann. Berechne modulo 11

   $$\begin{aligned} & 1 \cdot a_1 + 2 \cdot a_2 + \dots + (i-1) \cdot a_{j-1} + i \cdot a_j + \dots + (j-1) \cdot a_{j-1} + j \cdot a_i + \dots + 9 \cdot a_9 \\ \equiv\ & 1 \cdot a_1 + 2 \cdot a_2 + \dots + (i-1) \cdot a_{i-1} + i \cdot a_i + \dots + (j-1) \cdot a_{j-1} + j \cdot a_j + \dots + 9 \cdot a_9 \\ & + (i \cdot a_j - i \cdot a_i + j \cdot a_i - j \cdot a_j) \\ \equiv\ & p + (i \cdot a_j - i \cdot a_i + j \cdot a_i - j \cdot a_j) \end{aligned}$$

Wäre $p+(i\cdot a_j-i\cdot a_i+j\cdot a_i-j\cdot a_j)\equiv p \pmod{11}$, so wäre $(i\cdot a_j-i\cdot a_i+j\cdot a_i-j\cdot a_j) = (i-j)(a_j-a_i)$ durch 11 teilbar. Ähnlich wie im Fall 1 lässt sich begründen, dass das nicht sein kann. Also gehört die neue Nummer nicht zu einem gültigen Ausweis.

5. Unterscheiden sich die Ausweise in ihrer Prüfziffer, so ist klar, dass nicht beide Ausweise gültig sein können. Seien nun die Ausweisnummern von Lisa und Hans von der Form

$$a_1 a_2 \ldots a_{j-1} a_j a_{j+1} \ldots a_9(p), \quad a_1 a_2 \ldots a_{j-1} b_j a_{j+1} \ldots a_9(p)$$

mit $a_j \neq b_j$. Angenommen beide wären gültig, so würde modulo 11 gelten:

$$\begin{aligned} p-p &\equiv 1\cdot a_1 + 2\cdot a_2 + \ldots + (j-1)\cdot a_{j-1} + j\cdot a_j + (j+1)\cdot a_{j+1} + \ldots + 9\cdot a_9 \\ &\quad - (1\cdot a_1 + 2\cdot a_2 + \ldots + (j-1)\cdot a_{j-1} + j\cdot b_j + (j+1)\cdot a_{j+1} + \ldots + 9\cdot a_9) \\ &\equiv j(a_j-b_j) \end{aligned}$$

das heißt, $j(a_j-b_j)$ wäre durch 11 teilbar. Wie in der Lösung der 4. Teilaufgabe überlegt man sich, dass das nicht gelten kann. Daher ist unsere Annahme, dass beide Ausweisnummern gültig sind, falsch. Also muss einer der Ausweise gefälscht sein.