Lösungshinweise

Dies sind keine Beweise, sondern Lösungsskizzen. Es wird keine Richtigkeit gewährleistet.

Aufgabe 1. Wir sehen, dass $10 \equiv -1 \pmod{11}$ und damit

$$n = a_k \dots a_2 a_1 = \sum_{i=1}^{k} a_i 10^{i-1} \equiv \sum_{i=1}^{k} a_i (-1)^{i-1} = (-1)^{k+1} a_k + \dots - a_2 + a_1 \pmod{11}$$

Aufgabe 2. Wir sehen, dass $7 \mid 1001$ und damit $1000 \equiv -1 \pmod 7$ also

$$\begin{aligned} n = a_{3k} \dots a_2 a_1 &= \sum_{i=1}^{k} a_{3i} a_{3i-1} a_{3i-2} 1000^{i-1} \\ &\equiv \sum_{i=1}^{k} a_{i+2} a_{i+1} a_i (-1)^{i-1} = (-1)^{k+1} a_k a_{k-1} a_{k-2} + \dots - a_6 a_5 a_4 + a_3 a_2 a_1) \pmod 7 \end{aligned}$$

Aufgabe 3. Nach Aufgabe 4 wissen wir, dass für alle $n \in \mathbb{N}$ die Kongruenz $n \equiv n^7 \pmod{42}$ gilt.
Es folgt somit $\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} a_i^7 \pmod{42}$ und per Definition die Behauptung.

Aufgabe 4. Sei $n \in \mathbb{N}$ beliebig. Die Aussage ist äquivalent zu der Aussage: $n \equiv n^7 \pmod{42}$.
Weil $42 = (2)(3)(7)$ gilt und $2, 3, 7$ paarweise teilerfremd sind, ist die Aussage mit dem chinesischen Restsatz äquivalent zur folgenden Aussage:

$$\begin{aligned} n &\equiv n^7 \pmod 2 \\ n &\equiv n^7 \pmod 3 \\ n &\equiv n^7 \pmod 7 \end{aligned}$$

Die erste Gleichung gilt offensichtlich für $\{\overline{0}, \overline{1}\} = \mathbb{Z}/2\mathbb{Z}$.. Wegen des kleinen fermatschen Satzes gilt:

$$\begin{aligned} n &\equiv n^3 \pmod 3 \\ n &\equiv n^7 \pmod 7 \end{aligned}$$

Damit ist die dritte Gleichung gezeigt und die zweite folgt nun aus: $n^7 \equiv (n^3)^2(n) \equiv n^2(n) \equiv n^3 \equiv n \pmod 3$.

Aufgabe 5. Da $x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1})$ müssen wir nur $p \nmid x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1}$ zeigen. Da $p \mid x - y \Leftrightarrow x \equiv y \pmod p$ folgt $x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1} \equiv nx^{n-1} \neq 0 \pmod p$ nach Voraussetzung.

Aufgabe 6. Für $k \in \mathbb{Z}$, $r \in \{0,1,2\}$ gilt $(3k+r)^3 = 9(k^3 + 3k^2r + kr^2) + r^3 \equiv 0, \pm 1 \pmod 9$ je nachdem ob $r = 0,1,2$. Damit hinterlässt jede Kubikzahl die Reste ± 1 oder 0 modulo 9. Gilt $a^3 + b^3 + c^3 \equiv 0 \pmod 9$ muss also eine der Zahlen a, b, c durch 3 teilbar sein.

Aufgabe 7. Wenn die Zahl n^2+n+1 einen Teiler der Form $6k-1$ besitzt, muss sie offensichtlich auch einen Primteiler dieser Form besitzen, da alle anderen Primzahlen außer $2, 3$ die Form $6k+1$ haben. Angenommen $p = 6k-1 \mid n^2+n+1 \Rightarrow p \mid n^3 - 1 \Rightarrow n^3 \equiv 1 \pmod p$. Da $\varphi(p) = 6k-2$ und $(6k-2, 3) = 1$ folgt aus $n^3 \equiv 1 \pmod p$ auch $n \equiv 1 \pmod p$. Dann gilt $n^2 + n + 1 \equiv 3 \pmod p$. Widerspruch.

Aufgabe 8. Man muss hier zusätzlich $(a, b) \neq (\pm 1, \pm 1)$ annehmen. $a^4 + 4b^4 = (a^2+2b^2)^2 - 4a^2b^2 = (a^2+2b^2+2ab)(a^2+2b^2-2ab) = ((a+b)^2+b^2)((a-b)^2+b^2)$

Aufgabe 9. Man hat mindestens zwei aufeinanderfolgende ganze Zahlen ausgewählt. Diese sind teilerfremd. Für den anderen Teil bemerke, dass es n ungerade Zahlen in $\{1, 2, \ldots, 2n\}$ gibt und jede gerade Zahl ein vielfaches einer der Ungeraden Zahlen in $\{1, 2, \ldots, 2n\}$ ist.

Aufgabe 10. Da für $0 \leq k \leq n-1$ keine der n Zahlen $a + kd$ durch n teilbar ist, liegen mindestens zwei in der selben Restklasse, d.h. es gibt $k, k' \in \{0, \ldots, n-1\}$, sodass $a + kd \equiv a + k'd \pmod n \Leftrightarrow (k-k')d \equiv 0 \pmod n$. Damit ist d Nullteiler modulo n also $(d, n) \neq 1$.

Aufgabe 11. Sei $n \in \mathbb{N}$. Angenommen es gibt nur endlich viele Primzahlen $p_1, \ldots, p_n$ der Form $4k+3$, mit $k \in \mathbb{N}$. Wir betrachten die Zahl $x := p_1 \ldots p_n - 1$. Es gilt $x = 4(p_1 \ldots p_n - 1) + 3$. Somit hat x mindestens einen Primteiler q, mit $q = 4l+3$, $l \in \mathbb{N}$. Sonst hätte x Rest 1 bei Division durch 4. Nach Definition von x ist q keine der Primzahlen $p_1, \cdots, p_n$, dies ist ein Widerspruch zur Annahme, dass diese alle Primzahlen der Form $4k+3$ mit $k \in \mathbb{N}$ sind.

Aufgabe 12. Eine gerade volkommene Zahl hat die Form $2^{n-1}(2^n-1)$ für ein $n \in \mathbb{N}$ mit $2^n - 1$ prim, also n ungerade. Wir haben

$$2^{n-1}(2^n-1) \equiv \begin{cases} 1 \cdot 1 = 1, & n \equiv 1 \pmod 4 \\ 4 \cdot 7 \equiv 3, & n \equiv 3 \pmod 4 \end{cases} \pmod 5$$

Da die Zahl gerade ist folgt daraus die Behauptung.

Aufgabe 13. Da die Zahl gerade sein soll, ist a ungerade, also $a = 2^k l + 1$, für $l, k \in \mathbb{N}$, l ungerade, $n > 1$. Desweiteren ist dann $a^a + 1 = a^a - (-1)^a = (a-1)(a^{a-1} - a^{a-2} + \ldots - 1)$. Der rechte Faktor enthalt eine ungerade Anzahl ungerader Summanden, ist also ungerade. Man sieht also, weil $a^a + 1 = 2^{n-1}(2^n-1)$ für ein $n \in \mathbb{N}$ sein muss, dass $k = v_2(a-1) = v_2(a^a+1) = v_2(2^{n-1}(2^n-1)) = n-1$. Für $2 \leq n$ gilt $n \leq 2^{n-1}$ also: $2^{n-1}l^n < (2^{n-1}l+1)^{2^{n-1}l+1} + 1 = a^a + 1 = 2^{n-1}(2^n-1)$, womit $l = 1$ folgen muss. Dann muss $\left(2^{n-1}\right)^{2^{n-1}} + 1 = 2^{n-1}(2^n-1)$ gelten. Wegen $2^{n-1}(2^n-1) < \left(2^{n-1}\right)^{2^{n-1}} + 1$ für $n \geq 2$, reicht es $n = 1$ zu überprüfen. Offenbar ist $3^3 + 1 = 28$ volkommen.

Aufgabe 14. Mit euklidischem Algorithmus folgt:

$$
\begin{aligned}
42 &= 4 * 9 + 6 \\
9 &= 1 * 6 + 3 \\
6 &= 2 * 3 + 0
\end{aligned}
$$

Damit gilt $\mathrm{ggT}(42, 9) = 3$ und $3 = 42 * (-1) + 9 * 5$. Damit ist $(-5, 25) \in \mathbb{Z} \times \mathbb{Z}$ eine Lösung. Und nach Skript ist sieht die Lösungsmenge wie folgt aus: $\{(-5 + \frac{9k}{3}, 25 - \frac{42k}{3}), mit\ k\ \in \mathbb{Z}\}$.

Aufgabe 15. Es gibt keine Lösung, weil 3 die Zahlen 42 und 9 teilt und damit auch $42x + 9y$ für all $x, y \in \mathbb{Z}$, aber $3 \nmid 4$.

Aufgabe 16. Wir müssen das System

$$
\begin{aligned}
X &\equiv 2 \pmod 3 \\
X &\equiv 3 \pmod 5 \\
X &\equiv 2 \pmod 7
\end{aligned}
$$

lösen. Nach dem chinesischen Restsatz ist dieses System modulo $3 \cdot 5 \cdot 7 = 105$ eindeutig lösbar. Mithilfe des euklidischen Algorithmus lösen wir zuerst

$$
\begin{aligned}
X &\equiv 2 \pmod 3 \\
X &\equiv 3 \pmod 5.
\end{aligned}
$$

Da $2 \cdot 5 - 3 \cdot 3 = 1$ sind die Lösungen durch $X = 2 \cdot 2 \cdot 5 + 3 \cdot (-3) \cdot 3 + 15k = -7 + 15k$ mit $k \in \mathbb{Z}$ gegeben. Setzen wir dies in die letzte Zeile des ursprünglichen Systems ein erhalten müssen wir nur noch $k \equiv -7 + 15k \equiv 2 \pmod 7$ so lösen, dass $0 < -7 + 15k < 105$. Wir sehen, dass $k = 2$ klar geht, d.h. $X = 23$.

Aufgabe 17. Seien $m, n \in \mathbb{N}$ beliebige teilerfremde Zahlen. Dann ist die Aussage nach dem chinesischen Restsatz äquivalent zum folgenden Gleichungssystem:

$$
\begin{aligned}
m^{3\varphi(n)} + n^{7\varphi(m)} &\equiv 1 \pmod m \\
m^{3\varphi(n)} + n^{7\varphi(m)} &\equiv 1 \pmod n
\end{aligned}
$$

Es gilt $n^{\varphi(m)} \equiv 1 \pmod m$ und $m^{\varphi(n)} \equiv 1 \pmod n$. Außerdem gilt: $m^{\varphi(m)} \equiv 0 \pmod m$ und $n^{\varphi(n)} \equiv 0 \pmod n$. Einsetzen ergibt die Gleichung.

Aufgabe 18. Von 4 aufeinanderfolgenden ganzen Zahlen hat eine der Form $4k + 3$.

Aufgabe 19. Sei $n = \left(\frac{a}{b}\right)^2 + \left(\frac{c}{d}\right)^2 \Leftrightarrow (bd)^2 n = a^2 + c^2$. Da $(bd)^2 n$ Summe von zwei ganzen Quadraten ist, ist die Anzahl der Primfaktoren der Form $4k + 3$ von $(bd)^2 n$ gerade. Dann ist aber auch die Anzahl der Primfaktoren der Form $4k + 3$ von n gerade.

Aufgabe 20. Falls $(a/b)^n + a_1(a/b)^{n-1} + \cdots + a_0 = p(\frac{a}{b}) = 0$ mit o.B.d.A. $(a, b) = 1$. Gilt nach Multiplikation mit b^n, dass $a^n = -b(a^{n-1}a_1 + a^{n-2}ba_2 + \cdots + a_0 b^{n-1})$. Aus $(a, b) = 1$ folgt nun $b \div 1$ und daraus $\frac{a}{b} \in \mathbb{Z}$.

Aufgabe 21. Die Menge aller rationalen Polynome ist abzählbar.

Aufgabe 22. 42

Aufgabe 23. Es ist für $p \neq 2, 5$:

$$\begin{aligned}\left(\frac{10}{p}\right) &= \left(\frac{5}{p}\right)\left(\frac{2}{p}\right) = \left(\frac{p}{5}\right)(-1)^{\frac{(p^2-1)}{8}} \\ &= \begin{cases} 1, & p \equiv \pm 1 \pmod 5 \text{ und } p \equiv \pm 1 \pmod 8 \\ & p \equiv \pm 2 \pmod 5 \text{ und } p \equiv \pm 3 \pmod 8 \\ -1, & p \equiv \pm 1 \pmod 5 \text{ und } p \equiv \pm 3 \pmod 8 \\ & p \equiv \pm 2 \pmod 5 \text{ und } p \equiv \pm 1 \pmod 8 \end{cases},\end{aligned}$$

also

$$\left(\frac{10}{p}\right) = \begin{cases} 1, & p \equiv \pm 1, \pm 3, \pm 9 \pm 13 \pmod{40} \\ -1, & p \equiv \pm 7, \pm 11, \pm 17, \pm 19 \pmod{40} \end{cases}$$

Aufgabe 24. Angenommen es gibt nur endlich viele Primzahlen $p_1, \ldots, p_n$ der Form $8k+7$ bzw. $8k-1$. Dann ist jeder Primteiler p von $(p_1 \cdots p_n)^2 - 2$ von der Form $8k+1$, da offensichtlich $(p_1 \cdots p_n)^2 \equiv 2 \pmod p$ also $\left(\frac{2}{p}\right) = 1$. Dann würde aber $-1 \equiv (p_1 \cdots p_n)^2 - 2 \equiv 1 \pmod 8$ folgen. Widerspruch.

Aufgabe 25. Allgemein gilt für ein Polynom $p(X) = AX^2 + BX + C$ vom Grad 2 und eine Primzahl $p \neq 2$ mit $(p, A) = 1$ mittels quadratischer Ergänzung:

$$\begin{aligned} AX^2 + BX + C &\equiv 0 \pmod p \\ \Leftrightarrow (2AX + B)^2 &\equiv B^2 - 4AC \pmod p \end{aligned}$$

Da $X \mapsto 2AX+B$ als Abbildung der Restklassen bijektiv ist, besitzt diese Gleichung genau dann zwei Lösungen, falls $\left(\frac{B^2-4AC}{p}\right) = 1$.

In unserem Fall ist nach Lösungen modulo $391 = 17 \cdot 23$ gefragt. Wegen des chinesischen Restsatzes brauchen wir also Lösbarkeit modulo 17 und modulo 23. Allerdings ist $B^2 - 4AC = -127$ und $\left(\frac{-127}{23}\right) = \left(\frac{11}{23}\right) = -\left(\frac{23}{11}\right) = -1$

Aufgabe 26. Angenommen $\{1, 2, \ldots, \lfloor\sqrt{p}\rfloor + 1\}$ enthält nur quadratische Reste. Sei nun $r \in \{1, \ldots, p-1\}$ der kleinste quadratische Nichtrest. Da $(\lfloor\sqrt{p}\rfloor + 1)^2 > p$, gibt es ein $s \in \{2, \ldots, \lfloor\sqrt{p}\rfloor + 1\}$, sodass $rs > p > r(s-1) \Rightarrow r > rs - p > 0$. Da rs ein quadratischer Nichtrest ist, ist dies auch $rs - p$, Widerspruch zur Minimalität von r.

Aufgabe 27.

$$\begin{aligned}\tau^2 &= \left(\sum_{a \in (\mathbb{Z}/l\mathbb{Z})^*} \left(\frac{a}{l}\right) e^{\frac{2\pi i a}{l}}\right)^2 = \sum_{a \in (\mathbb{Z}/l\mathbb{Z})^*} \sum_{b \in (\mathbb{Z}/l\mathbb{Z})^*} \left(\frac{ab}{l}\right) e^{\frac{2\pi i (a+b)}{l}} \\ &= \sum_{a \in (\mathbb{Z}/l\mathbb{Z})^*} \sum_{b' \in (\mathbb{Z}/l\mathbb{Z})^*} \left(\frac{b'}{l}\right) e^{\frac{2\pi i a(1+b')}{l}} = \sum_{b' \in (\mathbb{Z}/l\mathbb{Z})^*} \left(\frac{b'}{l}\right) \sum_{a \in (\mathbb{Z}/l\mathbb{Z})^*} e^{\frac{2\pi i a(1+b')}{l}} \\ &= \sum_{b' \in (\mathbb{Z}/l\mathbb{Z})^*} \left(\frac{b'}{l}\right) \begin{cases} (l-1), & b' = -1 \\ -1, & \text{sonst} \end{cases} = \left(\frac{-1}{l}\right) l\end{aligned}$$

Für die mittlere Zeile wurde $b = ab'$ substituiert. Die erste Gleichheit der letzten Zeile folgt aus der geometrischen Summenformel

$$\sum_{i=1}^{l-1} e^{\frac{2\pi i a(1+b')}{l}} = \frac{e^{\frac{2\pi i l(1+b')}{l}} - 1}{e^{\frac{2\pi i(1+b')}{l}} - 1} = 0$$

für $1 + b' \neq 0$. Dei zweite Gleichheit aus der Formel $\sum_{b' \in (\mathbb{Z}/l\mathbb{Z})^*, b' \neq -1} \left(\frac{b'}{l}\right) = -\left(\frac{-1}{l}\right)$, welche gilt, weil es gleich viele quadratische Nichtreste wie Reste modulo l ungleich 0 gibt.

Aufgabe 28. Da $p \equiv 2 \pmod 3$, definiert $x \mapsto x^3$ einen Gruppenisomorphismus von $(\mathbb{Z}/p\mathbb{Z})^*$.

Aufgabe 29. Wir definieren $A := [2, \overline{1, 2, 1}]$ und $B : [\overline{1, 2, 1}]$. Dann gilt $A = 2 + \frac{1}{B}$ und $B = [1, 2, 1, B]$. Wir lösen die Gleichungssysteme

$$\begin{aligned} A &= [2, B], \\ B &= 1 + \cfrac{1}{2 + \cfrac{1}{1 + \frac{1}{B}}} \end{aligned}$$

und erhalten $B = \frac{1+\sqrt{10}}{3}$ und $A = \frac{\sqrt{10}+1}{3}$.

Aufgabe 30. Wir liefern nur das Ergebnis: $\sqrt{2} = [1, \overline{2}]$ und $\frac{1+\sqrt{5}}{2} = [\overline{1}]$

Aufgabe 31. Wir definieren $A := [D, \overline{2D}]$ und $B = [\overline{2D}]$. Dann gilt $B = 2D + \frac{1}{B}$. Lösen des Gleichungssystems ergibt $B = D + \sqrt{1 + D^2}$. Einsetzen in $A = D + \frac{1}{B}$ und Auflösen ergibt $A = \sqrt{1 + D^2}$.