Verständnisfragen

1. Der größte gemeinsame Teiler zweier Zahlen a, b ist eine Primzahl. Besitzen die Zahlen a, b weitere gemeinsame Teiler?
Lösung: Sei $d = ggT(a, b)$. Dann ist $a = k_1 d$ und $b = k_2 d$. Sei d' ein weiterer Teiler von a und b, dann gilt, dass $d' \mid k_1$, $d' \mid k_2$ oder $d' \mid d$. Wenn $d' \mid d$, dann ist entweder $d = d'$ oder $d = 1$, denn d ist eine Primzahl. Wenn $d' \mid k_1$ und $d' \mid k_2$, dann teilt auch $d \cdot d'$ a und b. Da aber d der größte gemeinsame Teiler ist, muss $d' = 1$ sein. Entsprechend folgt, dass a, b keine weiteren gemeinsamen Teiler bis auf die 1 besitzen.

2. Wieviele gerade Primzahlen gibt es? *Lösung:* Nur 2.

3. Zeigen Sie:
   (a) $\forall a, b \in \mathbb{Z}$: Ist $a \mid b$ und $b \mid a \Rightarrow a = b$ oder $a = -b$.
   Lösung: Es gibt $k_1, k_2 \in \mathbb{Z}$: $b = k_1 a$ und $a = k_2 b$, dann folgt $b = k_1 k_2 b$, also $k_1 k_2 = 1$. Da $k_1, k_2 \in \mathbb{Z}$, folgt $k_1 = k_2 = 1$ oder $k_1 = k_2 = -1$. Dies zeigt die Ausage.
   (b) $\forall a_1, a_2, b_1, b_2 \in \mathbb{Z}$: $a_1 \mid b_1$ und $a_2 \mid b_2 \Rightarrow a_1 a_2 \mid b_1 b_2$
   Lösung: Es gibt $k_1, k_2 \in \mathbb{Z}$: $b_1 = k_1 a_1$ und $b_2 = k_2 a_2$, dann folgt $b_1 b_2 = k_1 k_2 a_1 a_2$, also teilt $a_1 a_2$ das Produkt $b_1 b_2$.

4. Sei $n \in \mathbb{N}$. Ist $n! = 0$ in $\mathbb{Z}_n$? *Lösung:* Es ist $n! = 1 \cdot 2 \cdot \dots \cdot n$, also $n \mid n!$ und damit $n! = 0 \mod n$.

5. Erklären Sie, warum der Euklidische Algorithmus immer zu einer Lösung führt. *Lösung:* s. Vorlesung.

6. Welche der folgenden Aussagen ist richtig? Beweisen Sie richtige Aussagen bzw. geben Sie für falsche Aussagen ein Gegenbeispiel an.
   - ☐ $a \in \mathbb{Q}, b \in \mathbb{R} \setminus \mathbb{Q} \quad \Rightarrow \quad a + b \in \mathbb{R} \setminus \mathbb{Q}$: Ja, richtig, denn Annahme: Es sei $a + b \in \mathbb{Q}$, dann existieren $p, q \in \mathbb{Z}$: $a + b = \frac{p}{q}$, also $b = \frac{p}{q} - a$. Da $a \in \mathbb{Q}$, folgt daraus $b \in \mathbb{Q}$, was einen Widerspruch zur Voraussetzung wäre. Also ist $a + b \in \mathbb{R} \setminus \mathbb{Q}$.
   - ☐ $a, b \in \mathbb{R} \setminus \mathbb{Q} \quad \Rightarrow \quad a + b \in \mathbb{R} \setminus \mathbb{Q}$: falsch, denn $\sqrt{2} - \sqrt{2} = 0 \notin \mathbb{R} \setminus \mathbb{Q}$.
   - ☐ $a \in \mathbb{Q}, b \in \mathbb{R} \setminus \mathbb{Q} \quad \Rightarrow \quad a \cdot b \in \mathbb{R} \setminus \mathbb{Q}$: richtig, denn Annahme: es sei $a \cdot b \in \mathbb{Q}$, dann gibt es $p, p', q, q' \in \mathbb{Z}$, so dass $a \cdot b = \frac{p}{q}$, $a = \frac{p'}{q'}$ und $b = \frac{pq'}{qp'} \in \mathbb{Q}$, Widerspruch zur Voraussetzung.
   - ☐ $\exists a \in \mathbb{R} : a^2 \notin \mathbb{Q}, a^4 \in \mathbb{Q}$: Ja, $\sqrt[4]{2}$, denn $\sqrt{2} \notin \mathbb{Q}$, aber $2 \in \mathbb{Q}$.
   - ☐ $\exists a, b \in \mathbb{R} \setminus \mathbb{Q} : a + b \in \mathbb{Q}, a \cdot b \in \mathbb{Q}$. Ja: $a = \sqrt{2}, b = -\sqrt{2}$.

Vollständige Induktion

1. Zeigen Sie die folgenden Aussagen mit Hilfe der vollständigen Induktion:

(a) n Menschen schütteln sich genau einmal untereinander die Hände. Dann wird genau $\frac{n(n-1)}{2}$-mal die Hände geschüttelt: Induktionsanfang: Zwei Menschen: es gibt ein Händeschütteln.
Induktionsannahme: Die Aussage sei für $n \geq 2$ wahr.
Induktionsschluß: Es schütteln sich $n+1$ Menschen die Hände. n Menschen haben sich bereits alle untereinander die Hände geschüttelt. Dann muss noch der $n+1$-te Mensch allen n anderen Menschen die Hand schütteln. Mit der Induktionsannahme erhalten wir also $\frac{n(n-1)}{2} + n$ Händeschütteln. Umformen ergibt $\frac{(n+1)n}{2}$. Also ist die Aussage bewiesen.

(b) Die Summe der ersten n ungeraden Zahlen ist n^2.
Induktionsanfang: $1 = 1^2$.
Induktionsannahme: $\sum_{k=1}^{n} 2k - 1 = n^2$
Induktionsschluß:

$$\sum_{k=1}^{n+1} 2k - 1 = \sum_{k=1}^{n} 2k - 1 + 2(n+1) - 1 = n^2 + 2n + 1 = (n+1)^2.$$

(c) $\forall n \in \mathbb{N} : \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$
Induktionsanfang: $1 = \frac{1 \cdot 2 \cdot 3}{6}$.
Induktionsannahme: $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$
Induktionsschluß:

$$\sum_{k=1}^{n+1} k^2 = \sum_{k=1}^{n} k^2 + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6}.$$

(d) $\forall n \in \mathbb{N} : \sum_{k=0}^{n} 2^k = 2^{n+1} - 1$. Induktionsanfang: $2^0 = 2^1 - 1$.
Induktionsannahme: $\sum_{k=1}^{n} 2^k = 2^{n+1} - 1$
Induktionsschluß:

$$\sum_{k=1}^{n+1} 2^k = \sum_{k=1}^{n} 2^k + 2^{n+1} = 2^{n+1} - 1 + 2^{n+1} = 2^{n+2} - 1.$$

Standardaufgaben

1. Berechnen Sie mit Hilfe des Euklidischen Algorithmus $d = \mathrm{ggT}(104, 47)$ und Zahlen $r, s \in \mathbb{Z}$, so dass $d = 104r + 47b$.
   Lösung: Es ist $d = 1$ und $1 = (-14)104 + 31 \cdot 47$.

2. Berechnen Sie mit Hilfe des Euklidischen Algorithmus $d = \mathrm{ggT}(12345, 54321)$.*Lösung:* Es ist $d = 3$.

3. Berechnen Sie
   (a) $12 \mod 5 = 2$
   (b) $237 \mod 10 = 7$
   (c) $222 \mod 11 = 2$

(d) $1001 \mod 11 = 0$

4. Berechnen Sie für $n \geq 4$
   (a) $(n+1) \mod n = 1$
   (b) $n(n+1) \mod n = 0$
   (c) $(n+1)(n-1) \mod n = n-1$
   (d) $(n-1) \mod (n+1) = n-1$
   (e) $(n+2)^2 \mod (n+1) = 1$

5. Zeigen Sie, dass eine Zahl $a = a_n \ldots a_0$ genau dann durch 11 teilbar ist, wenn die alternierende Summe $\sum_{i=0}^{n}(-1)^i a_i$ ihrer Ziffern a_i durch 11 teilbar ist.
   Lösung: Es ist $a = \sum_{k=0}^{n} a_k 10^k$. Es soll $a \mod 11 = 0$ sein. Unter Anwendung der Rechenregeln für Modulorechnung erhalten wir:

$$\begin{aligned} a \mod 11 &= 0 \\ \sum_{k=0}^{n}\left(a_k 10^k\right) \mod 11 &= 0 \\ \sum_{k=0}^{n}\left(a_k \mod 11 (10 \mod 11)^k\right) &= 0 \\ \sum_{k=0}^{n} a_k(-1)^k \mod 11 &= 0 \end{aligned}$$

   Damit ist die Aussage gezeigt.
   Ist die Zahl 317206375 durch 11 teilbar? Wir rechnen $3-1+7-2+0-6+3-7+5 = 2$. Damit ist die Zahl nicht durch 11 teilbar.

6. Zeigen Sie, dass $2^{10} = 1 \mod 11$.
   Lösung: Es ist $2^{10} = 2^5 \cdot 2^5$. Weiter ist $2^5 \mod 11 = 32 \mod 11 = 10$. Damit ist

$$2^{10} \mod 11 = (2^5 \mod 11) \cdot (2^5 \mod 11) = 100 \mod 11 = 1.$$

7. Zeigen Sie, dass $9518^{42} = 4 \mod 5$.
   Lösung: Es ist $9518 \mod 5 = 3$. Weiter ist $42 = 2 \cdot 3 \cdot 7$:

$$9518^{42} \mod 5 = \left((3^2 \mod 5)\right)^{21} = \left(4^3 \mod 5\right)^7 = \left(4^7 \mod 5\right) = 4 \mod 5.$$

8. (*) Was sind die letzten drei Ziffern von 7^{9999}? Starten Sie zunächst mit $7^4 = 2401$ und betrachten Sie dann $7^{4k} = (2400+1)^k$ mittels des Binomischen Lehrsatzes.
   Der Binomische Lehrsatz lautet

$$(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}, \quad \binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

   Lösung: Mit Hilfe des Tipps schreiben wir

$$\begin{aligned} 7^{4k} \mod 1000 &= (2400+1)^k \mod 1000 \\ &= \sum_{j=0}^{k}\binom{k}{j}2400^j \mod 1000 \end{aligned}$$

Da alle Potenzen $2400^j \mod 1000 = 0$ für $j \geq 2$, folgt:

$$\sum_{j=0}^{k} \binom{k}{j} 2400^j \mod 1000 = (1 + k \cdot 2400) \mod 1000.$$

Es ist $9999 = 2499 \cdot 4 + 3$. Also ist $k = (2500 - 1)$. Damit erhalten wir:

$(1 + (2500 - 1) \cdot 2400) \mod 1000 = (1 - 2400) \mod 1000 = (1 - 400) \mod 1000.$

Insgesamt erhalten wir

$$\begin{aligned}
7^{9999} \mod 1000 &= 7^3 \cdot 7^{2499 \cdot 4} \mod 1000 \\
&= 7^3 \mod 1000 \cdot 7^{2499 \cdot 4} \mod 1000 \\
&= (343) \mod 1000 \cdot (1 - 400) \mod 1000 \\
&= 343 \mod 1000 - 340 \cdot 400 \mod 1000 - 3 \cdot 400 \mod 1000 \\
&= 343 - 200 \\
&= 143
\end{aligned}$$

Übungsaufgaben: Abgabe

1. Zeigen Sie die folgenden Aussagen mit Hilfe der vollständigen Induktion:
   (a) $\forall n \in \mathbb{N} : 8^n - 3^n$ ist ein Vielfaches von 5.
   Lösung:
   Induktionsanfang: $n = 1$: $8 - 3 = 5$ ist ein Vielfaches von 5.
   Induktionsannahme: Für $n \in \mathbb{N}$ beliebig: $\exists k \in \mathbb{Z} :\ 8^n - 3^n = 5k$
   Induktionsschluß:
$$\begin{aligned} 8^{n+1} - 3^{n+1} &= 8(8^n - 3^n) + 8 \cdot 3^n - 3^{n+1} \\ &= 8(8^n - 3^n) + 5 \cdot 3^n \end{aligned}$$
   Da nach Induktionsannahme $8^n - 3^n$ durch 5 teilbar ist und $5 \cdot 3^n$ durch 5 teilbar, ist auch die Summe durch 5 teilbar und die Aussage bewiesen.

   (b) $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$. Verwenden Sie die Rekursionsformel für $\binom{n}{k}$. *Lösung:* Induktionsanfang: $n = 0$: $(a+b)^0 = 1$ und $\sum_{k=0}^{0} \binom{n}{k} a^{n-k} b^k = \binom{0}{0} a^0 b^0 = 1$. Induktionsannahme: $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$ Induktionsschluß:
$$\begin{aligned} (a+b)^{n+1} &= (a+b)^n\,(a+b) \\ &= (a+b) \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \\ &= \sum_{k=0}^{n} \binom{n}{k} a^{n+1-k} b^k + \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^{k+1}, \quad \text{Indexverschiebung} \\ &= \sum_{k=0}^{n} \binom{n}{k} a^{n+1-k} b^k + \sum_{k=1}^{n} \binom{n}{k-1} a^{n-(k-1)} b^k, \quad \binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k} \\ &= \sum_{k=1}^{n} \binom{n+1}{k} a^{n+1-k} b^k + a^{n+1} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k \end{aligned}$$

   (16 Punkte: pro Teilaufgabe 8 Punkte: 2 Punkte für Induktionsanfang, 1 Punkt für Induktionsannahme, 1 Punkt für richtige Verwendung der Induktionsannahme und 4 Punkte für Rechnung.

2. Berechnen Sie mit Hilfe des Euklidischen Algorithmus $d = \mathrm{ggT}(98701, 345)$.
   Lösung: Es ist $d = 1$. Die Zahlen sind teilerfremd.
   $r_0 = 98701$, $r_1 = 345$, wir rechnen $r_{j+1} = r_{j-1} - kr_j$, $j = j + 1$ bis $r_j = 0$.
$$\begin{aligned} r_2 &= 98701 - 286 \cdot 345 = 31 \\ r_3 &= 345 - 11 \cdot 31 = 4 \\ r_4 &= 31 - 7 \cdot 4 = 3 r_5 \qquad = 4 - 1 \cdot 3 = 1 r_6 = 3 - 3 \cdot 1 = 0 \end{aligned}$$

   (1 Punkt: Ansatz, 2 Punkte Rechnung, 1 Punkt Ergebnis ablesen)

3. (a) Beweisen Sie eine Teilbarkeitsregel für 7 und 13: Bestimmen Sie zunächst die Primfaktorzerlegung von 1001. Zeigen Sie anschließend, dass eine Zahl genau dann durch 7 oder 13 teilbar ist, wenn die alternierende Summe seiner 3-er Päckchen von Ziffern durch 7 oder 13 teilbar ist.
*Lösung:*Vorüberlegung: Es ist $1001 = 7\cdot 11\cdot 13$. $a+b10^3 \mod 7 = 1001b+(a-b)$ also ist $a+b$ durch 7 teilbar, wenn $a-b$ durch 7 teilbar ist.
Wenn $a10^6 + b10^3 + c = 10^3(10^3a + b) + c = 10^3(1001a + (b-a)) + c = 10^3\cdot 1001\cdot a + 10^3b - 10^3a + c = 1001b - b - 1001a + a + c = a - b + c$.
Allgemein: Sei a eine Zahl mit $3q+r$ Ziffern. Wir beweisen die Aussage mit Hilfe der vollständigen Induktion nach q. Sei $q = 0$, dann ist $a = r$ und natürlich durch 7 teilbar, wenn seine 3 Ziffern durch 7 teilbar ist.
Wir nehmen nun an, dass die Aussage für Zahlen mit $3(q-1)+r$ Ziffern wahr ist.
Induktionsschluß: Es sei a eine Zahl mit $3q+r$ Ziffern. Dann können wir a schreiben als: $a = \sum_{k=1}^{q} a_k 10^{3k} + a_0$. Jede Zahl a_k10^{3k} schreiben wir als $10^{3(k-1)}10^3a_k = 10^{3(k-1)}(1001a_k - a_k)$. Wir rechnen nun die gesamte Zahl modulo 1001:

$$
\begin{aligned}
a \mod 1001 &= \sum_{k=1}^{q} a_k 10^{3k} + a_0 \mod 1001\\
&= \sum_{k=1}^{q} 10^{3(k-1)}(1001a_k - a_k) + a_0 \mod 1001\\
&= \sum_{k=1}^{q} 10^{3(k-1)}(-a_k) + a_0 \mod 1001\\
&= \sum_{k=1}^{q-1} 10^{3k}(-a_k) - a_1 + a_0 \quad \text{Induktionsannahme!} \quad = \sum_{k=0}^{q}(-1)^k a_k \mod 1001
\end{aligned}
$$

Ist 317206375 durch 3 oder 7 teilbar?
$375 - 206 + 317 = 486$ und damit nicht durch 7 teilbar. Es ist $3+1+7+2+6+3+7+5 = 34$. Damit ist 317206375 nicht durch 3 teilbar.

(b) Bestimmen Sie den Rest von 3^{15} und 15^{83} bei Division durch 13.
Lösung: 15 ist $3\cdot 5$. $3^{15} \mod 13 = (3^3 \mod 13)^5 = (1 \mod 13)^5 = 1$.
$(15 \mod 13)^{83} = (2 \mod 13)^{83}$ und $83 = 2^4\cdot 5 + 3$. Es ist $2^4 \mod 13 = 3$ und $3^5 \mod 13 = 9$. Weiter ist $2^3 \mod 13 = 8$. Also zusammengesetzt:

$$15^{83} \mod 13 = 9\cdot 8 \mod 13 = 7.$$

(12 Punkte: 8 Punkte für richtiges Schließen der Teilbarkeitsregel (es muss kein Beweis gegeben werden, eine plausible Erklärung reicht), 4 Punkte für letzte Frage

4. Zeigen Sie, dass $35^{57} - 7$ durch 11 teilbar ist.
Lösung: Es ist $35 \mod 11 = 2$. Damit ist $35^{57} \mod 11 = 2^{57} \mod 11$. Die Potenz können wir berechnen als $57 = 3(18+1)$. Also ist $2^{57} \mod 11 = (2^3 \mod 11)^18(2^3 \mod 11) = 8^{2\cdot 3\cdot 3} \mod 118 \mod 11 = (9 \mod 11)^{3\cdot 3}8 \mod 11 = (3 \mod 11)^3 8 \mod 11 = 5 \mod 11 \cdot 8 \mod 11 = 7 \mod 11$. Also ist $35^{57} - 7 \mod 11 = 7 - 7 \mod 11 = 0$. **(8 Punkte: Zwischenschritte müssen verständlich angegeben sein.**

Abgabe möglich bis zu Beginn der Vorlesung am **04.05.2020**.