

Nachklausuraufgabe 1

Bestimmen Sie zwei modulo 210 inkongruente Lösungen des folgenden Kongruenzsystems:

$$2x \equiv 3 \pmod{5} \quad 4x \equiv 2 \pmod{6} \quad 3x \equiv 2 \pmod{7}$$

Lösung:

Für alle $x \in \mathbb{Z}$ mit $4x \equiv 2 \pmod{6}$ gibt es ein $y \in \mathbb{Z}$ mit $4x = 2 + 6y$.

Für alle $x \in \mathbb{Z}$ mit $4x \equiv 2 \pmod{6}$ ist also $2x \equiv 1 \pmod{3}$.

Wegen $(2, 3) = (2, 5) = (3, 7) = 1$, $2 \cdot 2 \equiv 1 \pmod{3}$, $3 \cdot 2 \equiv 1 \pmod{5}$ und $5 \cdot 3 \equiv 1 \pmod{7}$ ist das Kongruenzsystem

$$2x \equiv 1 \pmod{3} \quad 2x \equiv 3 \pmod{5} \quad 3x \equiv 2 \pmod{7}$$

äquivalent zu dem Kongruenzsystem

$$x \equiv 2 \pmod{3} \quad x \equiv 9 \pmod{5} \quad x \equiv 10 \pmod{7}.$$

Gesucht werden also alle $x \in \mathbb{Z}$ mit

$$x \equiv -1 \pmod{3}, \quad x \equiv -1 \pmod{5} \quad \text{und} \quad x \equiv 3 \pmod{7}.$$

Definiert man

$$m_1 := 3, \quad m_2 := 5, \quad m_3 := 7,$$

$$M_1 := m_2 \cdot m_3 = 5 \cdot 7 = 35, \quad M_2 := m_3 \cdot m_1 = 7 \cdot 3 = 21 \quad \text{und} \quad M_3 := m_1 \cdot m_2 = 3 \cdot 5 = 15,$$

so gilt für alle $(M_1^*, M_2^*, M_3^*)^T \in \mathbb{Z}^3$

$$M_1 \cdot M_1^* \equiv 1 \pmod{m_1} \iff 35M_1^* \equiv 1 \pmod{3} \iff -M_1^* \equiv 1 \pmod{3} \iff M_1^* \equiv -1 \pmod{3}$$

$$M_2 \cdot M_2^* \equiv 1 \pmod{m_2} \iff 21M_2^* \equiv 1 \pmod{5} \iff 1 \cdot M_2^* \equiv 1 \pmod{5} \iff M_2^* \equiv 1 \pmod{5}$$

$$M_3 \cdot M_3^* \equiv 1 \pmod{m_3} \iff 15M_3^* \equiv 1 \pmod{7} \iff 1 \cdot M_3^* \equiv 1 \pmod{7} \iff M_3^* \equiv 1 \pmod{7}$$

Mit dem Chinesischen Restsatz folgt

$$\begin{aligned} x &\equiv -1 \pmod{3}, \quad x \equiv -1 \pmod{5} \quad \text{und} \quad x \equiv 3 \pmod{7} \\ &\iff x \equiv ((-1) \cdot (-1) \cdot 35 + 1 \cdot (-1) \cdot 21 + 1 \cdot 3 \cdot 15) \pmod{3 \cdot 5 \cdot 7} \\ &\iff x \equiv (35 - 21 + 45) \pmod{15 \cdot 7} \\ &\iff x \equiv 59 \pmod{105}. \end{aligned}$$

Es gilt

$$\begin{aligned} 2 \cdot 59 &= 118 \equiv 3 \pmod{5}, & 2 \cdot 164 &= 328 \equiv 3 \pmod{5}, \\ 4 \cdot 59 &= 236 \equiv 2 \pmod{6}, & 4 \cdot 164 &= 656 \equiv 2 \pmod{6}, \\ 3 \cdot 59 &= 177 \equiv 2 \pmod{7} \quad \text{und} & 3 \cdot 164 &= 492 \equiv 2 \pmod{7}. \end{aligned}$$

Mit $59 \not\equiv 164 \pmod{210}$ sind also in 59 und 164 zwei modulo 210 inkongruente Lösungen des Kongruenzsystems $2x \equiv 3 \pmod{5} \quad 4x \equiv 2 \pmod{6} \quad 3x \equiv 2 \pmod{7}$ gefunden.

Nachklausuraufgabe 2

Zeigen Sie, dass $\tau(n)$ genau dann ungerade ist, wenn $n \in \mathbb{N}$ eine Quadratzahl ist.

Lösung:

1. Möglichkeit

Sei $n \in \mathbb{N}$. Sei $g : \left\{ \begin{array}{l} \mathbb{N} \rightarrow \mathbb{Q} \\ d \mapsto g_d := \frac{n}{d} \end{array} \right\}$. Für alle $d \in \mathbb{N}$ gilt

$$\left(d < \sqrt{n} \iff \frac{n}{d} = g_d > \sqrt{n} \right) \quad \text{und} \quad \left(d > \sqrt{n} \iff \frac{n}{d} = g_d < \sqrt{n} \right).$$

Für alle $d \in \mathbb{N}$ und alle $k \in \mathbb{N}$ gilt

$$g_d = g_k \iff \frac{n}{d} = \frac{n}{k} \iff d = k.$$

Damit ist g injektiv. Für alle $d \in \mathbb{N}$ gilt $d|n \iff g_d|n$ wegen $n = d \cdot \frac{n}{d} = d \cdot g_d$. Wegen $\#\{d \in \mathbb{N} ; d|n\} \leq n < \infty$ ist g also bijektiv auf $\{d \in \mathbb{N} ; d|n\}$.

Nun ist

$$\begin{aligned} \tau(n) &= \#\{d \in \mathbb{N} ; d|n\} = \#\{d \in \mathbb{N} ; d|n \text{ und } d < \sqrt{n}\} + \#\{d \in \mathbb{N} ; d|n \text{ und } d > \sqrt{n}\} \\ &\quad + \#\{d \in \mathbb{N} ; d|n \text{ und } d = \sqrt{n}\} \\ &= \#\{d \in \mathbb{N} ; d|n \text{ und } d < \sqrt{n}\} + \#\{d \in \mathbb{N} ; g_d|n \text{ und } g_d < \sqrt{n}\} \\ &\quad + \#\{d \in \mathbb{N} ; d|n \text{ und } d = \sqrt{n}\} \\ &= \#\{d \in \mathbb{N} ; d|n \text{ und } d < \sqrt{n}\} + \#\{d \in \mathbb{N} ; d|n \text{ und } d < \sqrt{n}\} \\ &\quad + \#\{d \in \mathbb{N} ; d|n \text{ und } d = \sqrt{n}\} \\ &= 2 \cdot \#\{d \in \mathbb{N} ; d|n \text{ und } d < \sqrt{n}\} + \#\{d \in \mathbb{N} ; d|n \text{ und } d = \sqrt{n}\}. \end{aligned}$$

Wegen $\{d \in \mathbb{N} ; d|n \text{ und } d = \sqrt{n}\} \subseteq \{\sqrt{n}\}$ ist also $\tau(n)$ genau dann ungerade, wenn $\#\{d \in \mathbb{N} ; d|n \text{ und } d = \sqrt{n}\} = 1$ ist.

Das ist genau dann der Fall, wenn $\{d \in \mathbb{N} ; d|n \text{ und } d = \sqrt{n}\} = \{\sqrt{n}\}$ ist, also genau dann, wenn $\sqrt{n} \in \mathbb{N}$ ist. Das ist genau dann der Fall, wenn n eine Quadratzahl ist.

2. Möglichkeit

τ ist nach Folgerung 5.3 multiplikativ.

Für alle $p \in \mathbb{P}$ und alle $a \in \mathbb{N}_0$ gilt $\tau(p^a) = \sum_{d|p^a} 1 = \sum_{b=0}^a 1 = a + 1$ wegen $\{d \in \mathbb{N} ; d|p^a\} = \{p^b \in \mathbb{N} ; b \in \mathbb{N}_0 \text{ und } b \leq a\}$ nach Bemerkung 1.18.

Sei $n \in \mathbb{N}$ mit der Primfaktorzerlegung $n = \prod_{j=1}^r p_j^{a_j}$.

$$\text{Dann gilt } \tau(n) = \tau\left(\prod_{j=1}^r p_j^{a_j}\right) = \prod_{j=1}^r \tau(p_j^{a_j}) = \prod_{j=1}^r (a_j + 1).$$

Also ist $\tau(n)$ genau dann ungerade, wenn $(a_j + 1)$ für alle $j \in \mathbb{N}$ mit $j \leq r$ ungerade ist. Das ist genau dann der Fall, wenn a_j für alle $j \in \mathbb{N}$ mit $j \leq r$ gerade ist, also wenn für alle $j \in \mathbb{N}$ mit $j \leq r$ ein b_j mit $a_j = 2b_j$ existiert.

Damit ist $\tau(n)$ genau dann ungerade, wenn $n = \prod_{j=1}^r p_j^{a_j} = \prod_{j=1}^r p_j^{2b_j} = \left(\prod_{j=1}^r p_j^{b_j}\right)^2$ ist, also wenn n eine Quadratzahl ist.

3. Möglichkeit

Sei $n \in \mathbb{N}$ mit der Primfaktorzerlegung $n = \prod_{j=1}^r p_j^{a_j}$.

Nach Bemerkung 1.18 ist $d|n$ äquivalent zu $d = \prod_{j=1}^r p_j^{d_j}$ mit $d_j \in \mathbb{N}_0$ und $d_j \leq a_j$ für alle $j \in \mathbb{N}$ mit $j \leq r$.

Für jedes $j \in \mathbb{N}$ mit $j \leq r$ stehen $(a_j + 1)$ solcher $d_j \in \mathbb{N}_0$ mit $d_j \leq a_j$ zur Verfügung. Da diese beliebig miteinander kombiniert werden können, folgt $\tau(n) = \prod_{j=1}^r (a_j + 1)$.

Also ist $\tau(n)$ genau dann ungerade, wenn $(a_j + 1)$ für alle $j \in \mathbb{N}$ mit $j \leq r$ ungerade ist. Das ist genau dann der Fall, wenn a_j für alle $j \in \mathbb{N}$ mit $j \leq r$ gerade ist, also wenn für alle $j \in \mathbb{N}$ mit $j \leq r$ ein b_j mit $a_j = 2b_j$ existiert.

Damit ist $\tau(n)$ genau dann ungerade, wenn $n = \prod_{j=1}^r p_j^{a_j} = \prod_{j=1}^r p_j^{2b_j} = \left(\prod_{j=1}^r p_j^{b_j} \right)^2$ ist, also wenn n eine Quadratzahl ist.

Nachklausuraufgabe 3

Bestimmen Sie alle Lösungen der Kongruenz $16x^2 - 2x - 10 \equiv 0 \pmod{245}$.

Lösung:

Es ist $245 = 5 \cdot 49 = 5 \cdot 7^2$ die Primfaktorzerlegung von 245.

Für alle $x \in \mathbb{Z}$ ist $16x^2 - 2x - 10 \equiv 0 \pmod{5}$ genau dann, wenn $x^2 - 2x \equiv 0 \pmod{5}$ ist.

Wegen $0^2 - 2 \cdot 0 = 0$, $2^2 - 2 \cdot 2 = 0$ und des Satzes von LAGRANGE 3.5 ist also für alle $x \in \mathbb{Z}$

$$16x^2 - 2x - 10 \equiv 0 \pmod{5} \iff x \in (0 + 5\mathbb{Z}) \cup (2 + 5\mathbb{Z}).$$

Für alle $x \in \mathbb{Z}$ ist $16x^2 - 2x - 10 \equiv 2 \cdot x^2 - 2x - 3 \pmod{7}$.

Es gilt

$$2 \cdot (-3)^2 - 2 \cdot (-3) - 3 = 18 + 6 - 3 = 21 \equiv 0 \pmod{7},$$

$$2 \cdot (-2)^2 - 2 \cdot (-2) - 3 = 8 + 4 - 3 = 11 \not\equiv 0 \pmod{7},$$

$$2 \cdot (-1)^2 - 2 \cdot (-1) - 3 = 2 + 2 - 3 = 1 \not\equiv 0 \pmod{7},$$

$$2 \cdot 0^2 - 2 \cdot 0 - 3 = 0 - 0 - 3 = -3 \not\equiv 0 \pmod{7},$$

$$2 \cdot 1^2 - 2 \cdot 1 - 3 = 2 - 2 - 3 = -3 \not\equiv 0 \pmod{7},$$

$$2 \cdot 2^2 - 2 \cdot 2 - 3 = 8 - 4 - 3 = 1 \not\equiv 0 \pmod{7}$$

und

$$2 \cdot 3^2 - 2 \cdot 3 - 3 = 18 - 6 - 3 = 9 \not\equiv 0 \pmod{7}.$$

Für alle $x \in \mathbb{Z}$ gilt also

$$16x^2 - 2x - 10 \equiv 0 \pmod{7} \iff x \equiv -3 \pmod{7}.$$

Es gelten $32 \cdot (-3) - 2 = -96 - 2 = -98 = (-14) \cdot 7 \equiv 0 \pmod{7}$ und

$$16 \cdot (-3)^2 - 2 \cdot (-3) - 10 = 48 \cdot 3 + 6 - 10 \equiv (-1) \cdot 3 - 4 \pmod{49} \equiv -7 \pmod{49} \not\equiv 0 \pmod{49}$$

Mit dem Aufsteigesatz 3.7 folgt, dass es kein $x \in \mathbb{Z}$ mit $16x^2 - 2x - 10 \equiv 0 \pmod{49}$ gibt.

Damit ergibt sich

$$\{x \in \mathbb{Z}; 16x^2 - 2x - 10 \equiv 0 \pmod{245}\} = \emptyset.$$

Nachklausuraufgabe 4

Seien $p \in \mathbb{P} \setminus \{2\}$ und $a \in \mathbb{Z}$ mit $(a, p) = 1$ und $\text{ord}_p(a) = 3$. Zeigen Sie $\left(\frac{a}{p}\right) = 1$.

Hinweis: Es gilt $a^3 - 1 = (a - 1) \cdot (a^2 + a + 1)$. Betrachten Sie den Rest von $(a + 1)^2 \pmod p$.

Lösung:

Wegen $\text{ord}_p(a) = 3$ ist $a^3 - 1 \equiv 1 - 1 \pmod p$ und deshalb wird $a^3 - 1$ von p geteilt.

Nun ist (man lese von rechts nach links)

$$a^3 - 1 = (a^3 + a^2 + a) - (a^2 + a + 1) = (a - 1) \cdot (a^2 + a + 1).$$

Wegen $p \in \mathbb{P}$ gilt also $p \mid (a - 1)$ oder $p \mid (a^2 + a + 1)$.

Die Annahme $p \mid (a - 1)$ führt zu $a = a - 1 + 1 \equiv 1 \pmod p$ im Widerspruch zu $\text{ord}_p(a) = 3$.

Also teilt p die Zahl $(a^2 + a + 1)$ und es folgt

$$a \equiv a + (a^2 + a + 1) \pmod p \equiv a^2 + 2a + 1 \pmod p \equiv (a + 1)^2 \pmod p.$$

Insbesondere ist a ein quadratischer Rest modulo p und es gilt also $\left(\frac{a}{p}\right) = 1$.

Nachklausuraufgabe 5

Seien $k \in \mathbb{N} \setminus \{1\}$, $a := 2^k + 1$, $m \in \mathbb{N}$ und $n \in \mathbb{N}$ mit $(n, m) = 1$, $n \equiv 1 \pmod 2$ und $m \equiv a \pmod{4n}$. Zeigen Sie $\left(\frac{n}{m}\right) = \left(\frac{a}{n}\right)$.

Lösung:

Es gilt $m \equiv a \pmod n$ und es gilt

$$m \equiv a \pmod 4 \equiv 2^k + 1 \pmod 4 \equiv 4 \cdot 2^{k-2} + 1 \pmod 4 \equiv 1 \pmod 4.$$

Also gibt es ein $\ell \in \mathbb{N}$ mit $m = 1 + 4\ell$. Außerdem gibt es ein $k \in \mathbb{N}$ mit $n = 1 + 2k$.

Mit der Rechenregel zum JACOBI-Symbol 3.17 (7) folgt

$$\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right) \cdot (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}} = \left(\frac{m}{n}\right) \cdot (-1)^{2\ell k} = \left(\frac{m}{n}\right).$$

Mit der Rechenregel zum JACOBI-Symbol 3.17 (1) folgt

$$\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right) = \left(\frac{a}{n}\right).$$

Nachklausuraufgabe 6

Seien $f : \mathbb{N} \rightarrow \mathbb{C}$ und $g : \mathbb{N} \rightarrow \mathbb{C}$ zwei zahlentheoretische Funktionen.

Beweisen Sie die Identität $\ln \cdot (f * g) = (\ln \cdot f) * g + f * (\ln \cdot g)$.

Lösung:

Für alle $n \in \mathbb{N}$ gilt

$$\begin{aligned} ((\ln \cdot f) * g + f * (\ln \cdot g))(n) &= \sum_{d|n} (\ln \cdot f)(d) \cdot g\left(\frac{n}{d}\right) + \sum_{d|n} f(d) \cdot (\ln \cdot g)\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \ln(d) \cdot f(d) \cdot g\left(\frac{n}{d}\right) + \sum_{d|n} f(d) \cdot \ln\left(\frac{n}{d}\right) \cdot g\left(\frac{n}{d}\right) \\ &= \sum_{d|n} f(d) \cdot g\left(\frac{n}{d}\right) \cdot \left(\ln(d) + \ln\left(\frac{n}{d}\right)\right) \\ &= \sum_{d|n} f(d) \cdot g\left(\frac{n}{d}\right) \cdot \ln\left(d \cdot \frac{n}{d}\right) = \ln(n) \cdot \sum_{d|n} f(d) \cdot g\left(\frac{n}{d}\right) = (\ln \cdot (f * g))(n). \end{aligned}$$

Nachklausuraufgabe 7

Eine Zahl $n \in \mathbb{N}$ heißt mehrfach multiplikativ vollkommen, falls $\prod_{d|n} d$ eine Potenz von n darstellt. Zeigen Sie, dass jede gerade vollkommene Zahl mehrfach multiplikativ vollkommen ist.

Lösung:

Sei $n \in \mathbb{N}$ mit $2|n$ vollkommen.

Nach Satz 5.5 (1) gibt es ein $k \in \mathbb{N}$ mit $p := 2^{k+1} - 1 \in \mathbb{P}$ und $n = 2^k p$. Also ist

$$\{d \in \mathbb{N} ; d|n\} = \{2^j \in \mathbb{N} ; j \in \mathbb{N}_0 \text{ mit } j \leq k\} \cup \{2^j p \in \mathbb{N} ; j \in \mathbb{N}_0 \text{ mit } j \leq k\}.$$

eine disjunkte Zerlegung der Menge der Teiler von n . Damit folgt

$$\prod_{d|n} d = \prod_{j=0}^k 2^j \cdot \prod_{j=0}^k (2^j p) = \prod_{j=0}^k (2^{2j} \cdot p) = p^{k+1} \cdot (2^2)^{\sum_{j=0}^k j} = p^{k+1} \cdot (2^2)^{\frac{k \cdot (k+1)}{2}} = (2^k p)^{k+1} = n^{k+1}.$$

Nachklausuraufgabe 8

Geben Sie alle $k \in \mathbb{N}$ mit $\varphi(k) = 44$ an.

Lösung:

Seien $n \in \mathbb{N}$ mit $\varphi(n) = 44$ und $n = \prod_{j=1}^r p_j^{a_j}$ die eindeutige Primfaktorzerlegung von n .

Dann ist $44 = 2^2 \cdot 11$ die eindeutige Primfaktorzerlegung von $\varphi(n) = \prod_{j=1}^r (p_j - 1) \cdot p_j^{a_j - 1}$.

Insbesondere folgt $(p_j - 1) | 44$ für alle $j \in \mathbb{N}$ mit $j \leq r$.

Damit folgt $p_j - 1 \in \{1, 2, 4, 11, 22, 44\}$ für alle $j \in \mathbb{N}$ mit $j \leq r$.

Also kommen nur Primfaktoren aus der Menge $\mathbb{P} \cap \{2, 3, 5, 12, 23, 45\} = \{2, 3, 5, 23\}$ in Betracht ($12 = 3 \cdot 4$ und $45 = 5 \cdot 9$).

Es gibt also ein $(a, b, c, d)^T \in \mathbb{N}_0^4$ mit $n = 2^a \cdot 3^b \cdot 5^c \cdot 23^d$.

Annahme: $d \geq 2$

Dann wird $\varphi(n)$ von $22 \cdot 23^{d-1}$ geteilt.

Das ist ein Widerspruch zu $\varphi(n) = 44 < 22 \cdot 23 = 506 \leq 22 \cdot 23^{d-1}$.

Annahme: $d = 0$

Dann gilt $p_j \leq 5$ für alle $j \in \mathbb{N}$ mit $j \leq r$. Insbesondere wäre $p \leq 5$ für alle $p \in \mathbb{P}$ mit $p | \varphi(n)$ mit Widerspruch zu $11 \in \mathbb{P}$ und $11 | \varphi(n)$.

Also gilt $d = 1$ und damit $44 = \varphi(n) = \varphi(2^a \cdot 3^b \cdot 5^c) \cdot \varphi(23) = \varphi(2^a \cdot 3^b \cdot 5^c) \cdot 22$.

Das führt zu $2 = \varphi(2^a \cdot 3^b \cdot 5^c)$.

Annahme: $c \neq 0$

Dann wäre $2 = \varphi(2^a \cdot 3^b \cdot 5^c) = \varphi(2^a \cdot 3^b) \cdot \varphi(5^c) = \varphi(2^a \cdot 3^b) \cdot 4 \cdot 5^{c-1}$.

Das ergibt den Widerspruch $4|2$.

Also ist $c = 0$.

Annahme: $b \geq 2$

Dann wäre $2 = \varphi(2^a \cdot 3^b) = \varphi(2^a) \cdot 2 \cdot 3^{b-1}$. Das ergibt den Widerspruch $3|2$.

Fall 1: $b = 1$

Dann ist $2 = \varphi(2^a) \cdot \varphi(3) = \varphi(2^a) \cdot 2$ und es folgt $\varphi(2^a) = 1$.

Es sind $\varphi(2^0) = 1 = \varphi(2^1)$. Für alle $\tilde{a} \in \mathbb{N} \setminus \{1\}$ ist $\varphi(2^{\tilde{a}}) = 1 \cdot 2^{\tilde{a}-1} \geq 2 > 1 = \varphi(2^a)$.

Also ergeben sich die Fälle $(a, b, c, d)^T = (0, 1, 0, 1)^T$ und $(a, b, c, d)^T = (1, 1, 0, 1)^T$.

Fall 1: $b = 0$

Dann ist $2 = \varphi(2^a)$. Wegen $\varphi(2^0) = 1 \neq 2$ ist also $a \geq 1$.

Damit folgt $2 = \varphi(2^a) = 1 \cdot 2^{a-1} = 2^{a-1}$, was $a = 2$ zur Folge hat.

Damit ergibt sich also der Fall $(a, b, c, d)^T = (2, 0, 0, 1)^T$.

Also ist $(a, b, c, d)^T \in \{(0, 1, 0, 1)^T, (1, 1, 0, 1)^T, (2, 0, 0, 1)^T\}$. Dies ergibt

$$\{k \in \mathbb{N} ; \varphi(k) = 44\} = \{3 \cdot 23, 2 \cdot 3 \cdot 23, 2^2 \cdot 23\} = \{69, 92, 138\}.$$