

Übungen zu Zahlentheorie, SS 2017

Christoph Baxa

- 1) Finde alle positiven Teiler von a) 1799 b) 997.
- 2) Zeige $(a - b) \mid (a^n - b^n)$ für alle $a, b \in \mathbb{Z}$ und alle $n \in \mathbb{N}$.
- 3) Zeige: Wenn $m \mid n$ dann $(a^m - b^m) \mid (a^n - b^n)$ (mit $a, b \in \mathbb{Z}, m, n \in \mathbb{N}$).
- 4) Zeige: Wenn $2 \nmid n$ für ein $n \in \mathbb{N}$ dann $8 \mid (n^2 + 23)$.
- 5) Zeige: Wenn $3 \nmid n$ für ein $n \in \mathbb{N}$ dann $3 \mid (n^2 + 23)$.
- 6) Zeige: Wenn $2 \nmid a$ und $2 \nmid b$ (mit $a, b \in \mathbb{Z}$) dann $2 \mid (a^2 + b^2)$ aber $4 \nmid (a^2 + b^2)$.
- 7) Zeige: Wenn $7 \mid (a^2 + b^2)$ (mit $a, b \in \mathbb{Z}$) dann $7 \mid a$ und $7 \mid b$.
- 8) Finde alle $n \in \mathbb{N}$, die $(n + 1) \mid (n^2 + 1)$ erfüllen.
- 9) Zeige $6 \mid (n^3 - n)$ für alle $n \in \mathbb{N}$.
- 10) Zeige $13 \mid (4^{2n+1} + 3^{n+2})$ für alle $n \in \mathbb{N} \cup \{0\}$. Hinweis: Verwende Induktion.
- 11) Zeige $169 \mid (3^{3n+3} - 26n - 27)$ für alle $n \in \mathbb{N} \cup \{0\}$.
- 12) Zeige $n^2 \mid ((n + 1)^n - 1)$ für alle $n \in \mathbb{N}$.
- 13) Zeige $(1^3 + 2^3 + \dots + n^3) \mid (3(1^5 + 2^5 + \dots + n^5))$ für alle $n \in \mathbb{N}$.
- 14) Zeige $[x + k] = [x] + k$ für alle $x \in \mathbb{R}$ und alle $k \in \mathbb{Z}$.
- 15) Finde und beweise eine Formel, die $[-x]$ durch $[x]$ ausdrückt (für $x \in \mathbb{R}$).
- 16) Zeige $[x_1] + \dots + [x_k] \leq [x_1 + \dots + x_k]$ für alle $x_1, \dots, x_k \in \mathbb{R}$.
- 17) Bestimme den ggT mit Hilfe des euklidischen Algorithmus für:
a) ggT(7469, 2464) b) ggT(2689, 4001) c) ggT(2947, 3997) d) ggT(1109, 4999)
- 18) Finde mit Hilfe des euklidischen Algorithmus $x, y \in \mathbb{Z}$, derart dass
a) $243x + 198y = 9$ b) $71x - 50y = 1$ c) $43x + 64y = 1$ d) $93x - 81y = 3$

- 19)** Zeige: Die Relation $m \mid n$ ist auf \mathbb{N} eine Ordnungsrelation. Ist sie eine Totalordnung? In welcher Beziehung steht sie zur üblichen Ordnungsrelation \leq auf \mathbb{N} ?
- 20)** Zeige: Wenn $\text{ggT}(a, 4) = \text{ggT}(b, 4) = 2$ (mit $a, b \in \mathbb{Z}$) dann $\text{ggT}(a + b, 4) = 4$.
- 21)** Zeige: Wenn $a, b \in \mathbb{Z}$ und $\text{ggT}(a, b) = 1$ dann $\text{ggT}(a + b, a - b) \in \{1, 2\}$.
- 22)** Zeige: Für alle $k \in \mathbb{Z}$ sind $2k + 1$ und $9k + 4$ relativ prim.
- 23)** Bestimme $\text{ggT}(4k + 1, 5k + 2)$ in Abhängigkeit von $k \in \mathbb{Z}$.
- 24)** Bestimme $\text{ggT}(2k - 1, 9k + 4)$ in Abhängigkeit von $k \in \mathbb{Z}$.
- 25)** Zeige: Sind $a, b \in \mathbb{Z}$ (nicht beide $= 0$) mit $\text{ggT}(a, b) = d$, so gilt $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ (wobei $n\mathbb{Z} := \{kn \mid k \in \mathbb{Z}\}$).
- 26)** Bestimme $\text{ggT}(56049, 14601, 43803)$.
- 27)** Finde $x, y, z \in \mathbb{Z}$, derart dass a) $6x + 10y + 15z = 1$, b) $21x + 15y + 35z = 1$.
- 28)** Gegeben seien $a, b, c, d \in \mathbb{Z}$ mit $b, d \neq 0$ und $\text{ggT}(a, b) = \text{ggT}(c, d) = 1$.
Zeige: Wenn $\frac{a}{b} + \frac{c}{d} \in \mathbb{Z}$ dann gilt $b \in \{d, -d\}$.
- 29)** Zeige für $a, b_1, \dots, b_k \in \mathbb{Z}$, dass
- $$\text{ggT}(a, b_1 \cdots b_k) = 1 \iff \text{ggT}(a, b_i) = 1 \text{ für } 1 \leq i \leq k$$
- 30)** Zeige: Ist $p, p + 2$ ein Primzahlzwilling und $p > 3$ so gilt $12 \mid (p + (p + 2))$.
- 31)** Finde sämtliche Primzahltrillinge, d.h. alle Tripel $p, p + 2, p + 4$ von Primzahlen.
- 32)** Zeige: Bezeichnet p_n die n -te Primzahl, so ist $p_n \leq 2^{2^{n-1}}$. Hinweis: Verwende den Beweis von Satz 11 und Induktion.
- 33)** Zeige: Sind $a, k \in \mathbb{N}$, $k > 1$ und ist $a^k - 1$ Primzahl, so muss $a = 2$ sein.
- 34)** Zeige: Sind $a, k \in \mathbb{N} \setminus \{1\}$ und ist $a^k + 1$ Primzahl, so muss a gerade und k eine Potenz von 2 sein.
- 35)** Zeige: Es gibt unendlich viele Primzahlen der Gestalt $3k + 2$ (mit $k \in \mathbb{Z}$).
- 36)** Zeige: Es gibt unendlich viele Primzahlen der Gestalt $6k + 5$ (mit $k \in \mathbb{Z}$).

37) Es sei p eine Primzahl mit der Eigenschaft, dass $2^p - 1$ ebenfalls Primzahl ist und $n := 2^{p-1}(2^p - 1)$. Zeige, dass $\sum_{d|n} d = 2n$, d.h. die Summe der positiven Teiler von n (ohne n selbst) ist genau n . (Zahlen mit dieser Eigenschaft werden vollkommen genannt. Man kann zeigen, dass alle geraden vollkommenen Zahlen von dieser Gestalt sind.)

38) Zeige: Wenn $ab = c^n$ (mit $a, b, c, n \in \mathbb{N}$ und $\text{ggT}(a, b) = 1$) dann sind a und b ebenfalls n -te Potenzen natürlicher Zahlen.

39) Zeige: Sind $n_1, \dots, n_k \in \mathbb{Z} \setminus \{0\}$ so gilt $\text{kgV}(\ell n_1, \dots, \ell n_k) = |\ell| \cdot \text{kgV}(n_1, \dots, n_k)$ für alle $\ell \in \mathbb{Z} \setminus \{0\}$.

40) Zeige: Ist $k \geq 2$ und $n_1, \dots, n_k \in \mathbb{Z} \setminus \{0\}$ so gilt

$$\text{kgV}(\text{kgV}(n_1, \dots, n_{k-1}), n_k) = \text{kgV}(n_1, \dots, n_k)$$

41) Begründe: Wenn jemand heuer an einem Montag (Dienstag, ..., Samstag, Sonntag) Geburtstag hat, wird er oder sie nächstes Jahr an einem Dienstag (Mittwoch, ..., Sonntag, Montag) Geburtstag haben (vorausgesetzt keines der beiden Jahre ist ein Schaltjahr).

42) Löse nochmals mit Hilfe von Kongruenzen: a) Bsp. 4) b) Bsp. 5) c) Bsp. 10)

43) Bestimme den Rest der folgenden Divisionen mit Rest mittels Kongruenzen:

$$\text{a) } 2^3 \cdot 3^6 \cdot 7^3 \cdot 13 \cdot 17 : 11 \qquad \text{b) } 9^2 \cdot 11 \cdot 37 \cdot 41 : 7$$

44) Zeige für alle $a, b \in \mathbb{Z}$ und alle Primzahlen p , dass $(a + b)^p \equiv a^p + b^p \pmod{p}$.
Hinweis: Zeige zunächst $p \mid \binom{p}{i}$ für $1 \leq i \leq p - 1$.

45) a) Bestimme die letzten beiden Ziffern der Dezimaldarstellung von 7^n für $n \in \mathbb{N}$ bel.
b) Bestimme die letzte Ziffer der Dezimaldarstellung von 2^n für $n \in \mathbb{N}$ beliebig.

46) Die Zahl $n \in \mathbb{N}$ habe die Dezimaldarstellung $n = a_0 + 10a_1 + 10^2a_2 + \dots + 10^k a_k$ mit $a_0, a_1, a_2, \dots, a_k \in \{0, 1, 2, \dots, 9\}$.

a) Beweise die folgenden Teilbarkeitsregel für 7: Die Zahl n ist genau dann durch 7 teilbar, wenn der folgende Ausdruck durch 7 teilbar ist:

$$(a_0 + 10a_1 + 100a_2) - (a_3 + 10a_4 + 100a_5) + (a_6 + 10a_7 + 100a_8) - + \dots$$

b) Zeige, dass eine völlig analoge Teilbarkeitsregel für die Teilbarkeit durch 13 gilt. Verwende Teil a), um $7 \mid 194618851$ zu überprüfen.

47) Die Zahl $n \in \mathbb{N}$ habe die Dezimaldarstellung $n = a_0 + 10a_1 + 10^2a_2 + \cdots + 10^k a_k$ mit $a_0, a_1, a_2, \dots, a_k \in \{0, 1, 2, \dots, 9\}$. Beweise die folgenden Teilbarkeitsregeln:

- a) $13 \mid n \iff 13 \mid (4a_0 + (a_1 + 10a_2 + 10^2a_3 + \cdots + 10^{k-1}a_k))$
 b) $17 \mid n \iff 17 \mid (-5a_0 + (a_1 + 10a_2 + 10^2a_3 + \cdots + 10^{k-1}a_k))$
 c) $19 \mid n \iff 19 \mid (2a_0 + (a_1 + 10a_2 + 10^2a_3 + \cdots + 10^{k-1}a_k))$

Verwende Teil a), um $13 \mid 112697$ (nur mit Hilfe von Bleistift und Papier) zu überprüfen.

48) Für welche $a \in \mathbb{Z}$ sind die folgenden linearen Kongruenzen lösbar?

- a) $11x \equiv a \pmod{80}$ b) $12x \equiv a \pmod{16}$ c) $3x \equiv 5 \pmod{a}$ d) $ax \equiv 11 \pmod{17}$

49) Löse die folgenden linearen Kongruenzen (sofern sie lösbar sind):

- a) $8x \equiv 12 \pmod{19}$ b) $8x \equiv 12 \pmod{160}$ c) $8x \equiv 12 \pmod{28}$

50) Es seien $a_1, \dots, a_n, b \in \mathbb{Z}$, wobei a_1, \dots, a_n nicht alle $= 0$ sein sollen. Zeige: Die lineare diophantische Gleichung

$$a_1x_1 + \cdots + a_nx_n = b$$

ist genau dann lösbar, wenn $\text{ggT}(a_1, \dots, a_n) \mid b$.

51) Es seien $a, b, c \in \mathbb{Z}$, wobei a, b nicht beide $= 0$ sein sollen. Zeige: Wenn die lineare diophantische Gleichung $ax + by = c$ lösbar ist, ist ihre Lösungsmenge durch

$$\left\{ \left(x_0 - \frac{b}{d}t, y_0 + \frac{a}{d}t \right) \mid t \in \mathbb{Z} \right\}$$

gegeben. Dabei ist $(x_0, y_0) \in \mathbb{Z}^2$ eine beliebige Lösung der gegebenen linearen diophantischen Gleichung (d.h. $ax_0 + by_0 = c$) und $d = \text{ggT}(a, b)$.

52) Bestimme die Lösungsmengen der linearen diophantischen Gleichungen aus Bsp. 18.

53) Löse die folgenden simultanen Kongruenzen:

- a) $x \equiv 1 \pmod{7}, \quad x \equiv 4 \pmod{9}, \quad x \equiv 3 \pmod{5},$
 b) $x \equiv 1 \pmod{20}, \quad x \equiv 9 \pmod{21}, \quad x \equiv 20 \pmod{23}.$

54) Finde alle modulo $20 \cdot 21 \cdot 23$ inkongruente Lösungen des folgenden Systems:

$$7x \equiv 8 \pmod{20}, \quad 5x \equiv -6 \pmod{21}, \quad 9x \equiv 13 \pmod{23}.$$

55) Es sei $(R, +, \cdot)$ ein kommutativer Ring mit 1. Ein $p \in R$ (mit $p \neq 0$ und $p \notin R^*$) heißt prim, wenn (für $a, b \in R$) aus $p \mid (ab)$ folgt, dass entweder $p \mid a$ oder $p \mid b$. Ein $p \in R$ (mit $p \neq 0$ und $p \notin R^*$) heißt irreduzibel, wenn aus $p = ab$ (mit $a, b \in R$) folgt, dass entweder $a \in R^*$ oder $b \in R^*$. Zeige: Ist R ein Integritätsbereich (d.h. es gibt außer 0 keine Nullteiler in R) und ist p prim in R , so ist p auch irreduzibel in R . (Welche Elemente von \mathbb{Z} sind prim bzw. irreduzibel?)

56) Zeige: Für jede Primzahl $p (\neq 2)$ gilt $1^2 3^2 5^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$.

57) Sei $n \in \mathbb{N}$. Zeige: Wenn $n > 4$ keine Primzahl ist, dann gilt $(n-1)! \equiv 0 \pmod{n}$.
Was gilt für $n = 4$?

58) Eine unbewiesene Vermutung über die Eulersche φ -Funktion besagt: Zu jedem $m \in \mathbb{N}$ gibt es ein $n \in \mathbb{N}$ mit $n \neq m$ und $\varphi(n) = \varphi(m)$. Zeige diese Vermutung für ungerades m .

59) Zeige: Zu jedem $m \in \mathbb{N}$ gibt es nur endlich viele $n \in \mathbb{N}$ mit der Eigenschaft $\varphi(n) = m$.

60) Zeige für $k, \ell \in \mathbb{N}$: Wenn $k \mid \ell$ dann $\varphi(k) \mid \varphi(\ell)$.

61) Zeige für alle $m, n \in \mathbb{N}$ (wobei $d = \text{ggT}(m, n)$ bezeichnet), dass

$$\varphi(mn) = \varphi(m)\varphi(n) \frac{d}{\varphi(d)}.$$

62) Beweise, dass $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15} \in \mathbb{N}$ für alle $n \in \mathbb{N}$.

63) Zeige, dass $2730 \mid (n^{13} - n)$ für alle $n \in \mathbb{Z}$.

64) Zeige: Jede Primzahl $p \notin \{2, 5\}$ teilt unendlich viele Zahlen der Gestalt $9, 99, 999, \dots$

65) Löse Bsp. 44) nochmals mit Hilfe des kleinen Fermatschen Satzes.

66) Es seien $a, b \in \mathbb{Z}$ und p eine Primzahl. Zeige: Wenn $a^p \equiv b^p \pmod{p}$ dann gilt bereits $a \equiv b \pmod{p^2}$.

Definition. Eine Zahl $n \in \mathbb{N}$, $n \neq 1$ wird Carmichael-Zahl genannt, wenn sie die Bedingung $a^{n-1} \equiv 1 \pmod{n}$ für alle $a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$ erfüllt, aber keine Primzahl (d.h. zusammengesetzt) ist.

67) a) Es seien p_1, \dots, p_k paarweise verschiedene Primzahlen (wobei $k \geq 2$ gelten soll). Zeige: Erfüllt $n := p_1 \cdots p_k$ die Bedingung $(p_i - 1) \mid (n - 1)$ für $1 \leq i \leq k$, so ist n eine Carmichael-Zahl.

b) Zeige, dass 561, 1105 und 41041 Carmichael-Zahlen sind.

68) a) Die Zahl $m \in \mathbb{N}$ besitze die Eigenschaft, dass $6m + 1$, $12m + 1$ und $18m + 1$ Primzahlen sind. Zeige, dass $(6m + 1)(12m + 1)(18m + 1)$ dann eine Carmichael-Zahl ist.

b) Finde die beiden kleinsten $m \in \mathbb{N}$ für die man mit Hilfe der in a) beschriebenen Methode Carmichael-Zahlen erhält.

69) Sei p eine ungerade Primzahl. Das Legendre-Symbol wird oft erweitert, indem man $\left(\frac{a}{p}\right) = 0$ setzt wenn $p \mid a$. Zeige: Verwendet man diese Erweiterung, so besitzt die Kongruenz $x^2 \equiv a \pmod{p}$ genau $1 + \left(\frac{a}{p}\right)$ modulo p inkongruente Lösungen (mit $a \in \mathbb{Z}$ beliebig).

70) Sei p eine ungerade Primzahl. Zeige $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$.

71) Berechne a) $\left(\frac{-1}{31}\right)$ b) $\left(\frac{-1}{17}\right)$ c) $\left(\frac{2}{41}\right)$ d) $\left(\frac{2}{47}\right)$.

72) Leite den ersten Ergänzungssatz aus dem Gaußschen Lemma ab.

73) Zeige: Es gibt unendlich viele Primzahlen $\equiv 7 \pmod{8}$. Hinweis: Angenommen, p_1, \dots, p_s wären alle derartigen Primzahlen. Betrachte $N := (4p_1 \dots p_s)^2 - 2$ und verwende den zweiten Ergänzungssatz.

74) Welche der folgenden Kongruenzen sind lösbar?

$$\text{a) } x^2 \equiv 59 \pmod{79} \quad \text{b) } x^2 \equiv 17 \pmod{41} \quad x^2 \equiv 29 \pmod{101}$$

75) Es sei $p \equiv 1 \pmod{4}$ eine Primzahl. Zeigen, dass die Kongruenz $x^2 \equiv -1 \pmod{p}$ genau die beiden modulo p inkongruenten Lösungen $\left(\frac{p-1}{2}\right)!$ und $-\left(\frac{p-1}{2}\right)!$ besitzt.

76) Es sei $p \notin \{2, 3\}$ eine Primzahl. Zeige, dass die Kongruenz $x^2 \equiv -3 \pmod{p}$ genau dann lösbar ist, wenn $p \equiv 1 \pmod{6}$. Hinweis: Berechne

$$\left(\frac{-3}{6k+1}\right) \quad \text{und} \quad \left(\frac{-3}{6k+5}\right).$$

77) Es seien m_1, \dots, m_k ungerade natürliche Zahlen und $m = m_1 \cdots m_k$. Zeige:

$$\text{a) } \frac{m-1}{2} \equiv \sum_{i=1}^k \frac{m_i-1}{2} \pmod{2} \quad \text{b) } \frac{m^2-1}{8} \equiv \sum_{i=1}^k \frac{m_i^2-1}{8} \pmod{2}$$

Hinweis. Beweise zunächst den Fall $k = 2$ und verwende Induktion nach k .

78) Beweise den ersten Ergänzungssatz für das Jacobi-Symbol: Ist $m \in \mathbb{N}$ ungerade, so gilt $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$.

79) Beweise den zweiten Ergänzungssatz für das Jacobi-Symbol: Ist $m \in \mathbb{N}$ ungerade, so gilt $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$.

80) Beweise das quadratische Reziprozitätsgesetz für das Jacobi-Symbol: Sind $m, n \in \mathbb{N}$ ungerade und relativ prim, so gilt $\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2} \frac{n-1}{2}}$.

81) Entwickle die Zahlen a) $\frac{93}{81}$ und b) $-\frac{71}{50}$ in einen regelmäßigen Kettenbruch.

82) Bestimme den Wert und die Näherungsbrüche der Kettenbrüche

a) $[4; 7, 5, 1, 2]$ und b) $[-2; 1, 3, 2, 2]$.

83) Es bezeichne q_n den Nenner des n -ten Näherungsbruchs einer reellen Zahl. Zeige

$$q_n \geq \left(\frac{1 + \sqrt{5}}{2} \right)^{n-1} \quad \text{für } n \geq 0.$$

Bemerkung. Diese Abschätzung verbessert die in der Vorlesung gegebene ein wenig.

84) Finde für $0 \leq n \leq 4$ die Teilnenner a_n und Näherungsbrüche p_n/q_n der Zahl π .

85) Bestimme den Wert der Kettenbrüche a) $[6; \overline{3, 12}]$ und b) $[4; \overline{2, 8}]$.

86) Zeige, dass $\sqrt{a^2 + 2} = [a; \overline{a, 2a}]$ für alle $a \in \mathbb{N}$.