

Übungen zu Zahlentheorie, SS 2008

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 $a, b \in \mathbb{Z}$ 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) Es sei $\mathbb{Z}[i] = \{x + iy \mid x, y \in \mathbb{Z}\}$. Zeige, daß $(\mathbb{Z}[i], +, \cdot)$ ein kommutativer Ring mit 1 ist (mit Addition und Multiplikation der komplexen Zahlen).

Man nennt $(\mathbb{Z}[i], +, \cdot)$ den Ring der Gaußschen ganzen Zahlen. Für $\alpha, \beta \in \mathbb{Z}[i]$ sagt man, β teilt α (in $\mathbb{Z}[i]$) wenn es ein $\gamma \in \mathbb{Z}[i]$ gibt mit $\alpha = \beta\gamma$ (und schreibt dafür kurz $\beta \mid \alpha$).

Ist $x + iy \in \mathbb{Z}[i]$ (mit $x, y \in \mathbb{Z}$), so wird die Norm $N(x + iy)$ von $x + iy$ durch

$$N(x + iy) = x^2 + y^2 (= (x + iy)(x - iy) = |x + iy|^2)$$

definiert. (Beachte, daß es sich dabei um eine Abbildung $N : \mathbb{Z}[i] \rightarrow \mathbb{Z}$ handelt.)

42) a) Zeige $N(\alpha\beta) = N(\alpha)N(\beta)$ für alle $\alpha, \beta \in \mathbb{Z}[i]$

b) Zeige: Wenn $\beta \mid \alpha$ (in $\mathbb{Z}[i]$) dann $N(\beta) \mid N(\alpha)$ (in \mathbb{Z}).

c) Verwende a) um zu zeigen, daß $\mathbb{Z}[i]$ nullteilerfrei ist

(d.h. es ist unmöglich, daß $\alpha\beta = 0$ wenn $\alpha, \beta \neq 0$).

43) Ein $\alpha \in \mathbb{Z}[i]$ wird Einheit von $\mathbb{Z}[i]$ genannt, wenn es ein multiplikatives Inverses in $\mathbb{Z}[i]$ besitzt, d.h. wenn ein $\beta \in \mathbb{Z}[i]$ mit der Eigenschaft $\alpha\beta = 1$ existiert. Die Menge der Einheiten von $\mathbb{Z}[i]$ wird mit $\mathbb{Z}[i]^*$ bezeichnet. Zeige

$$\mathbb{Z}[i]^* = \{\alpha \in \mathbb{Z}[i] \mid N(\alpha) = 1\} = \{1, -1, i, -i\}.$$

44) Zeige: Für alle $\alpha, \beta \in \mathbb{Z}[i]$ mit $\beta \neq 0$ gibt es $\gamma, \rho \in \mathbb{Z}[i]$, die $\alpha = \gamma\beta + \rho$ und $N(\rho) < N(\beta)$ erfüllen. Anleitung: Wenn $\alpha/\beta = r + is$ (mit $r, s \in \mathbb{Q}$), wähle $x, y \in \mathbb{Z}$, die $|r - x| \leq 1/2$ und $|s - y| \leq 1/2$ erfüllen und setze $\gamma = x + iy$.

45) Zeige: Führt man für $\alpha, \beta \in \mathbb{Z}[i] \setminus \{0\}$ fortwährend die im vorangegangenen Beispiel beschriebene Division mit Rest durch, d.h.

$$\alpha = \gamma_0\beta + \rho_1, \beta = \gamma_1\rho_1 + \rho_2, \rho_1 = \gamma_2\rho_2 + \rho_3, \dots$$

mit $N(\beta) > N(\rho_1) > N(\rho_2) > N(\rho_3) > \dots$, so bricht dieses Verfahren ab. Ist dabei ρ_n der letzte Rest $\neq 0$ (d.h. $\rho_{n-2} = \gamma_{n-1}\rho_{n-1} + \rho_n$, $\rho_{n-1} = \gamma_n\rho_n$), so ist ρ_n ein größter gemeinsamer Teiler von α und β im folgenden Sinn: $\rho_n \mid \alpha$, $\rho_n \mid \beta$ und wenn $\delta \mid \alpha$ und $\delta \mid \beta$ (für ein $\delta \in \mathbb{Z}[i]$) dann $\delta \mid \rho_n$.

46) Zeige die Implikationen (i) \Rightarrow (ii) \Rightarrow (iii) für $\alpha, \beta, \pi \in \mathbb{Z}[i]$ mit $\pi \notin \{0, 1, -1, i, -i\}$:

(i) Wenn $\pi \mid (\alpha\beta)$ dann $\pi \mid \alpha$ oder $\pi \mid \beta$ (d.h. π ist prim).

(ii) Wenn $\pi = \alpha\beta$ dann $\alpha \in \mathbb{Z}[i]^*$ oder $\beta \in \mathbb{Z}[i]^*$ (d.h. π ist irreduzibel).

(iii) Die Menge der Teiler von π ist $\{1, -1, i, -i, \pi, -\pi, i\pi, -i\pi\}$.

47) Zeige, daß die drei Aussagen (i), (ii) und (iii) aus dem vorangegangenen Beispiel äquivalent sind, d.h. zeige die Implikation (iii) \Rightarrow (i). Anleitung: Angenommen $\pi \mid (\alpha\beta)$. Wenn $\pi \mid \alpha$ fertig. Es gelte darum jetzt $\pi \nmid \alpha$. Führe den euklidischen Algorithmus aus dem vorletzten Beispiel für α und π durch, d.h.

$$\alpha = \gamma_0\pi + \rho_1, \pi = \gamma_1\rho_1 + \rho_2, \dots, \rho_{n-2} = \gamma_{n-1}\rho_{n-1} + \rho_n, \rho_{n-1} = \gamma_n\rho_n \quad (*)$$

wobei $N(\pi) > N(\rho_1) > N(\rho_2) > \dots > N(\rho_n)$. Dann gilt $\rho_n \mid \pi$ und wegen (iii) folgt $\rho_n \in \{1, -1, i, -i, \pi, -\pi, i\pi, -i\pi\}$. Wäre $\rho_n \in \{\pi, -\pi, i\pi, -i\pi\}$, so würde wegen $\rho_n \mid \alpha$ folgen, daß $\pi \mid \alpha$, was der Voraussetzung widerspricht. Also ist ρ_n eine Einheit. Aus (*) folgt

$$\alpha\beta = \gamma_0\pi\beta + \beta\rho_1, \pi\beta = \gamma_1\beta\rho_1 + \beta\rho_2, \dots, \beta\rho_{n-2} = \gamma_{n-1}\beta\rho_{n-1} + \beta\rho_n, \beta\rho_{n-1} = \gamma_n\beta\rho_n.$$

Wegen $N(\pi\beta) > N(\beta\rho_1) > N(\beta\rho_2) > \dots > N(\beta\rho_n)$ handelt es sich dabei um den euklidischen Algorithmus für $\alpha\beta$ und $\beta\pi$. Also ist $\beta\rho_n$ ein größter gemeinsamer Teiler von $\alpha\beta$ und $\beta\pi$. Da $\pi \mid (\alpha\beta)$ und $\pi \mid (\beta\pi)$ folgt $\pi \mid (\beta\rho_n)$ und daher $\pi \mid \beta$.

48) Zeige die folgenden Aussagen:

a) Wenn $N(\pi)$ eine Primzahl ist (mit $\pi \in \mathbb{Z}[i]$) dann ist π irreduzibel (und daher nach dem vorletzten Beispiel prim) in $\mathbb{Z}[i]$.

b) Es sei p eine Primzahl. Wenn es $x, y \in \mathbb{Z}$ mit der Eigenschaft $x^2 + y^2 = p$ gibt, sind $x + iy$ und $x - iy$ prim in $\mathbb{Z}[i]$ (wobei man o.B.d.A. $x > y > 0$ verlangen kann).

49) Zeige die folgenden Aussagen:

- a) $1 + i$ ist prim in $\mathbb{Z}[i]$.
- b) Es sei p eine Primzahl. Wenn es $x, y \in \mathbb{Z}$ mit der Eigenschaft $x^2 + y^2 = p$ gibt, ist $p = 2$ oder $p \equiv 1 \pmod{4}$.
- c) Es sei p eine Primzahl mit der Eigenschaft $p \equiv 3 \pmod{4}$. Dann ist p prim als Element von $\mathbb{Z}[i]$.

Bemerkung: Man kann zeigen, daß sich jede Primzahl $p \equiv 1 \pmod{4}$ als Summe zweier Quadrate darstellen läßt. Ein besonders eleganter Beweis dieser Tatsache stammt von Heath-Brown. Man findet ihn z.B. in *Das BUCH der Beweise* von Aigner und Ziegler.

50) Es sei $\mathbb{Z}[i\sqrt{5}] = \{x + i\sqrt{5}y \mid x, y \in \mathbb{Z}\}$. Zeige, daß $(\mathbb{Z}[i\sqrt{5}], +, \cdot)$ ein kommutativer, nullteilerfreier Ring mit 1 ist (mit Addition und Multiplikation der komplexen Zahlen).

Für $\alpha, \beta \in \mathbb{Z}[i\sqrt{5}]$ sagt man, β teilt α (in $\mathbb{Z}[i\sqrt{5}]$) wenn es ein $\gamma \in \mathbb{Z}[i\sqrt{5}]$ gibt mit $\alpha = \beta\gamma$ (und schreibt dafür kurz $\beta \mid \alpha$).

Ist $x + i\sqrt{5}y \in \mathbb{Z}[i\sqrt{5}]$ (mit $x, y \in \mathbb{Z}$), so wird die Norm $N(x + i\sqrt{5}y)$ von $x + i\sqrt{5}y$ durch $N(x + i\sqrt{5}y) = x^2 + 5y^2 (= (x + i\sqrt{5}y)(x - i\sqrt{5}y) = |x + i\sqrt{5}y|^2)$ definiert.

- 51)** a) Zeige $N(\alpha\beta) = N(\alpha)N(\beta)$ für alle $\alpha, \beta \in \mathbb{Z}[i\sqrt{5}]$
b) Zeige: Wenn $\beta \mid \alpha$ (in $\mathbb{Z}[i\sqrt{5}]$) dann $N(\beta) \mid N(\alpha)$ (in \mathbb{Z}).

52) Ein $\alpha \in \mathbb{Z}[i\sqrt{5}]$ wird Einheit von $\mathbb{Z}[i\sqrt{5}]$ genannt, wenn es ein multiplikatives Inverses in $\mathbb{Z}[i\sqrt{5}]$ besitzt, d.h. wenn ein $\beta \in \mathbb{Z}[i\sqrt{5}]$ mit der Eigenschaft $\alpha\beta = 1$ existiert. Die Menge der Einheiten von $\mathbb{Z}[i\sqrt{5}]$ wird mit $\mathbb{Z}[i\sqrt{5}]^*$ bezeichnet. Zeige

$$\mathbb{Z}[i\sqrt{5}]^* = \{\alpha \in \mathbb{Z}[i\sqrt{5}] \mid N(\alpha) = 1\} = \{1, -1\}.$$

53) Zeige die Implikation (i) \Rightarrow (ii) für $\alpha, \beta, \pi \in \mathbb{Z}[i\sqrt{5}]$ mit $\pi \notin \{0, 1, -1\}$:

- (i) Wenn $\pi \mid (\alpha\beta)$ dann $\pi \mid \alpha$ oder $\pi \mid \beta$ (d.h. π ist prim).
- (ii) Wenn $\pi = \alpha\beta$ dann $\alpha \in \mathbb{Z}[i\sqrt{5}]^*$ oder $\beta \in \mathbb{Z}[i\sqrt{5}]^*$ (d.h. π ist irreduzibel).

54) Zeige, daß 2 in $\mathbb{Z}[i\sqrt{5}]$ irreduzibel aber nicht prim ist (d.h. die Implikation (ii) \Rightarrow (i) ist in $\mathbb{Z}[i\sqrt{5}]$ falsch). Hinweis: Man kann $2 \mid ((1 + i\sqrt{5})(1 - i\sqrt{5}))$ als Ausgangspunkt verwenden, um zu zeigen, daß 2 nicht prim ist.

55) 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).

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

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

57) Zeige für alle $a, b \in \mathbb{Z}$ und alle Primzahlen p : Wenn $a^2 \equiv b^2 \pmod{p}$ gilt, dann gilt $p \mid (a - b)$ oder $p \mid (a + b)$.

58) 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 $1 \leq i \leq p - 1$.

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

60) 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 folgende 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.

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

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

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

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

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

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

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

64) Es seien $a_1, \dots, a_n, b \in \mathbb{Z}$. Eine Gleichung der Gestalt $a_1x_1 + \dots + a_nx_n = b$ bei der nach Lösungen $x_1, \dots, x_n \in \mathbb{Z}$ gesucht wird, wird lineare diophantische Gleichung genannt. Zeige: Die lineare diophantische Gleichung $a_1x_1 + \dots + a_nx_n = b$ ist genau dann lösbar wenn $\text{ggT}(a_1, \dots, a_n) \mid b$.

65) Es seien $a, b, c \in \mathbb{Z}$. Zeige: Wenn die lineare diophantische Gleichung $ax + by = c$ lösbar ist, ist ihre Lösungsmenge durch $\{(x_0 - \frac{b}{d}t, y_0 + \frac{a}{d}t) \mid t \in \mathbb{Z}\}$ 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 $d = \text{ggT}(a, b)$.

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

67) Löse die folgenden simultanen Kongruenzen:

a) $x \equiv 1 \pmod{7}, \quad x \equiv 4 \pmod{9}, \quad x \equiv 3 \pmod{5},$

b) $x \equiv 1 \pmod{20}, \quad x \equiv 9 \pmod{21}, \quad x \equiv 20 \pmod{23}.$

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

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

69) 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?)

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

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

72) 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 .

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

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

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

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

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

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

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

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

80) 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 $1 + \left(\frac{a}{p}\right)$ Lösungen (mit $a \in \mathbb{Z}$ beliebig).

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

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

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

84) 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.

85) Welche der folgenden Kongruenzen sind lösbar?

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

86) 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.

87) 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

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

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

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

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