3. Kongruenzen

Satz 36 Es sei $m \in \mathbb{N}$, $m \geq 2$ und $a, b \in \mathbb{Z}$. Dann sind äquivalent:

(i) a und b haben bei Division durch m den selben Rest,

(ii) $m \mid (a-b)$,

(iii) $\exists k \in \mathbb{Z} : a = b + km$.

Beweis: (i) $\Rightarrow$ (ii) Es seien $q_1, q_2, r \in \mathbb{Z}$, derart dass $a = q_1 m + r$, $b = q_2 m + r$ und $0 \leq r < m$. Dann ist $a - b = (q_1 m + r) - (q_2 m + r) = (q_1 - q_2) m$ und daher $m \mid (a-b)$.

(ii) $\Rightarrow$ (iii) $m \mid (a-b) \Rightarrow \exists k \in \mathbb{Z} : a - b = km \Rightarrow a = b + km$

(iii) $\Rightarrow$ (i) Wir führen für b und m Division mit Rest durch, also $b = qm + r$ für $q, r \in \mathbb{Z}$ und $0 \leq r < m$. Dann $a = b + km = qm + r + km = (q+k)m + r$ und Division mit Rest führt für a und m ebenfalls auf Rest r.

Definition: Es seien $m \in \mathbb{N}$, $m \geq 2$ und $a, b \in \mathbb{Z}$. Man sagt, a und b seien kongruent modulo m, wenn a, b und m eine (und damit alle) der drei Bedingungen aus Satz 36 erfüllen. Man schreibt dafür $a \equiv b \pmod m$ oder kurz $a \equiv b\ (m)$. Die Zahl m wird dabei Modul genannt. Erfüllen a, b und m die Eigenschaften aus Satz 36 nicht, so schreibt man $a \not\equiv b \pmod m$ oder kurz $a \not\equiv b\ (m)$ und sagt, a und b seien inkongruent modulo m.

S.S. 2025

Beispiele 1) $6 \equiv 24\ (9)$ (denn: 6 und 24 haben beide Rest 6 bei Division durch 9, $9 \mid (6-24) \Leftrightarrow 9 \mid (-18)$, $6 = 24 + (-2)\cdot 9$)

2) $14 \equiv -1\ (15)$ (denn: 14 und -1 haben beide Rest 14 bei Division durch 15, $15 \mid (14-(-1)) \Leftrightarrow 15 \mid 15$, $14 = -1 + 1 \cdot 15$)

3) $365 \equiv 1\ (7)$ (denn: 365 und 1 haben beide Rest 1 bei Division durch 7, $7 \mid (365 - 1) \Leftrightarrow 7 \mid 364$ da $364 = 52 \cdot 7$, $365 = 1 + 52 \cdot 7$)

Satz 37 Es sei $m \in \mathbb{N}$, $m \geq 2$. Kongruent zu sein modulo m ist eine Äquivalenzrelation auf $\mathbb{Z}$. Da es gelten die folgenden drei Eigenschaften (wobei $a, b, c \in \mathbb{Z}$):

(i) $a \equiv a\ (m)$ $\forall a \in \mathbb{Z}$, die Kongruenz modulo m ist reflexiv,

(ii) Aus $a \equiv b\ (m)$ folgt $b \equiv a\ (m)$, die Kongruenz modulo m ist symmetrisch,

(iii) Aus $a \equiv b\ (m)$ und $b \equiv c\ (m)$ folgt $a \equiv c\ (m)$, die Kongruenz modulo m ist transitiv.

Beweis: Für alle drei Punkte ist offensichtlich Bedingung (i) aus Satz 36 erfüllt.

Erinnerung: Jede Äquivalenzrelation $\sim$ zerlegt die Menge M, auf der sie definiert ist, in Äquivalenzklassen. Das sind paarweise disjunkte Teilmengen von M, die folgendermaßen definiert sind: Ist $a \in M$, so ist die Äquivalenzklasse $[a]$ von a die Menge $[a] = \{b \in M \mid b \sim a\}$, die die Menge aller Elemente $b \in M$, die zu a in Relation stehen.

Definition: Es sei $m \in \mathbb{N}$, $m \geq 2$. Die durch die Äquivalenzrelation der Kongruenz modulo m auf $\mathbb{Z}$ definierten Äquivalenzklassen werden Restklassen modulo m genannt.

Satz 38 Es sei $m \in \mathbb{N}$, $m \geq 2$.

(i) Für $a \in \mathbb{Z}$ besteht die Restklasse von a aus allen ganzen Zahlen, die bei Division durch m den selben Rest haben wie a,

(ii) Für $a \in \mathbb{Z}$ ist die Restklasse von a die Menge $a + m\mathbb{Z} = \{a + km \mid k \in \mathbb{Z}\}$,

(iii) $\mathbb{Z}$ zerfällt durch die Äquivalenzrelation der Kongruenz modulo m in die m paarweise verschiedenen Restklassen $m\mathbb{Z}$, $1 + m\mathbb{Z}$, $2 + m\mathbb{Z}$, .., $m-1 + m\mathbb{Z}$.

Beweis: (i) Folgt aus Charakterisierung (i) in Satz 36.

(ii) Folgt aus Charakterisierung (iii) in Satz 36.

(iii) Bei Division mit Rest durch m gibt es genau m mögliche Reste, nämlich $0, 1, 2, .., m-1$. Diese liegen in den Restklassen $0 + m\mathbb{Z} = m\mathbb{Z}$, $1 + m\mathbb{Z}$, $2 + m\mathbb{Z}$, .., $m-1 + m\mathbb{Z}$, die paarweise verschieden sind.

Beispiele: 1) Für $m = 2$ zerfällt $\mathbb{Z}$ durch Kongruenz modulo 2 in die beiden Restklassen $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ und $1 + 2\mathbb{Z} = \{1 + 2k \mid k \in \mathbb{Z}\}$, also in gerade und ungerade Zahlen. (D.h. die Einteilung von $\mathbb{Z}$ in Restklassen modulo m ist eine Verallgemeinerung der Einteilung in gerade und ungerade Zahlen.)

2) Für $m = 3$ zerfällt $\mathbb{Z}$ durch Kongruenz modulo 3 in die drei Restklassen $3\mathbb{Z} = \{3k \mid k \in \mathbb{Z}\}$, $1 + 3\mathbb{Z} = \{3k + 1 \mid k \in \mathbb{Z}\}$ und $2 + 3\mathbb{Z} = \{3k + 2 \mid k \in \mathbb{Z}\} = \{3k - 1 \mid k \in \mathbb{Z}\}$

Satz 39 (Rechenregeln für Kongruenzen) Es seien $m \in \mathbb{N}$, $m \geq 2$ und $a, b, c, d, n \in \mathbb{Z}$.

(i) Aus $a \equiv b\,(m)$ und $c \equiv d\,(m)$ folgt $a + c \equiv b + d\,(m)$,

(ii) Aus $a \equiv b\,(m)$ und $c \equiv d\,(m)$ folgt $a \cdot c \equiv b \cdot d\,(m)$,

(iii) Aus $a \equiv b\,(m)$ und $n \mid m$ (mit $|n| \geq 2$) folgt $a \equiv b\,(|n|)$,

(iv) Aus $a \equiv b\,(m)$ folgt $na \equiv nb\,(|n|m)$ $\forall n \in \mathbb{Z} \setminus \{0\}$,

(v) Wenn $m \neq n$, so gilt $na \equiv nb\,(m) \Leftrightarrow a \equiv b\left(\frac{m}{ggT(m,n)}\right)$.

Beweis: (i) Laut Satz 36 (iii) $\exists k, \ell \in \mathbb{Z}$: $a = b + km$ und $c = d + \ell m$. Daher ist $a + c = (b + km) + (d + \ell m) = b + d + (k + \ell)m$ und $a + c \equiv b + d\,(m)$ nach Satz 36 (iii)

(ii) Haben k und ℓ die selbe Bedeutung wie in (i), so ist

$$ac = (b + km)(d + \ell m) = b\ell + kdm + b\ell m + k\ell m^2 = bd + (kd + b\ell + k\ell m)m$$

und $ac \equiv bd\,(m)$ nach Satz 36 (iii)

(iii) Da $n \mid m$ gilt auch $|n| \mid m$ (wegen Satz 1 (iii)). Aus $|n| \mid m$ und $m \mid (a - b)$ (was wegen Satz 36 (ii) erfüllt ist) folgt $|n| \mid (a - b)$ (wegen Satz 1 (vii)).

Nach Satz 36 (ii) gilt $a \equiv b\,(|n|)$.

(iv) Nach Satz 36 $\exists k \in \mathbb{Z}$: $a-b = km$ und daher $na-nb = knm$. Also gilt $nm \mid (na-nb)$ und daher (wegen Satz 1 (iii)) $|n|m \mid (na-nb)$, also $na \equiv nb \ (|n|m)$.
(Beachte: Aus $n \neq 0$ folgt $|n| \geq 1$ und daher $|n|m \geq m \geq 2$.)

(v) Aus der Äquivalenz $m \mid n \iff ggT(m,n) = m$ folgt

$m \nmid n \iff ggT(m,n) \neq m \iff ggT(m,n) < m \iff \frac{m}{ggT(m,n)} > 1 \iff \frac{m}{ggT(m,n)} \geq 2$

Es bezeichne $d := ggT(m,n)$.

($\Rightarrow$) Nach Satz 36 gilt $m \mid (na-nb)$, d.h. $\exists k \in \mathbb{Z}$: $na-nb = km$ bzw. $n(a-b) = km$.
Daraus folgt $\frac{n}{d}(a-b) = k\frac{m}{d}$, wobei $\frac{n}{d}, \frac{m}{d} \in \mathbb{Z}$. Also gilt $\frac{m}{d} \mid \frac{n}{d}(a-b)$. Nach Korollar 10 ist $ggT(\frac{m}{d}, \frac{n}{d}) = 1$ und mit Hilfe von Satz 12 erhält man $\frac{m}{d} \mid (a-b)$.
Das besagt wegen Satz 36 aber gerade $a \equiv b \left(\frac{m}{ggT(m,n)}\right)$.

($\Leftarrow$) Nach Satz 36 gilt $\frac{m}{d} \mid (a-b)$, d.h. $\exists k \in \mathbb{Z}$: $a-b = k\frac{m}{d}$, woraus $na-nb = (k\frac{n}{d})m$ folgt. Da $k\frac{n}{d} \in \mathbb{Z}$, gilt $m \mid (na-nb)$ und daher $na \equiv nb \ (m)$.

Korollar 40 (Mehr Rechenregeln für Kongruenzen) Es sei $m \in \mathbb{N}$, $m \geq 2$.

(i) Aus $a \equiv b \ (m)$ folgt $a+c \equiv b+c \ (m)$ (für $a, b, c \in \mathbb{Z}$),

(ii) Aus $a \equiv b \ (m)$ folgt $a \cdot c \equiv b \cdot c \ (m)$ (für $a, b, c \in \mathbb{Z}$),

(iii) Aus $a_1 \equiv b_1 \ (m), \dots, a_k \equiv b_k \ (m)$ folgt $a_1 + \dots + a_k \equiv b_1 + \dots + b_k \ (m)$
(für $a_1, \dots, a_k, b_1, \dots, b_k \in \mathbb{Z}$),

(iv) Aus $a_1 \equiv b_1 \ (m), \dots, a_k \equiv b_k \ (m)$ folgt $a_1 \cdots a_k \equiv b_1 \cdots b_k \ (m)$
(für $a_1, \dots, a_k, b_1, \dots, b_k \in \mathbb{Z}$),

(v) Aus $a \equiv b \ (m)$ folgt $a^k \equiv b^k \ (m)$ (für $a, b \in \mathbb{Z}$ und $k \in \mathbb{N}^+$),

(vi) Ist p ein Polynom mit Koeffizienten in $\mathbb{Z}$ und $a \equiv b \ (m)$, so folgt $p(a) \equiv p(b) \ (m)$
(für $a, b \in \mathbb{Z}$),

(vii) Aus $na \equiv nb \ (m)$ und $ggT(m,n) = 1$ folgt $a \equiv b \ (m)$ (für $a, b, n \in \mathbb{Z}$).

Beweis: (i) Das ist der Spezialfall $c = d$ von Satz 39 (i).

(ii) Das ist der Spezialfall $c = d$ von Satz 39 (ii).

(iii) Induktion nach k. $k = 1$ ist trivial und $k = 2$ wurde in Satz 39 (i) bewiesen.
Ist $k \geq 2$ und $a_1 \equiv b_1 \ (m), \dots, a_k \equiv b_k \ (m)$, $a_{k+1} \equiv b_{k+1} \ (m)$, so folgt nach Induktionsvoraussetzung $a_1 + \dots + a_k \equiv b_1 + \dots + b_k \ (m)$. Daraus folgt mit Hilfe von Satz 39 (i)

$a_1 + \dots + a_{k+1} = (a_1 + \dots + a_k) + a_{k+1} \equiv (b_1 + \dots + b_k) + b_{k+1} = b_1 + \dots + b_{k+1} \ (m)$.

(iv) Induktion nach k. $k=1$ ist trivial und $k=2$ wurde in Satz 39 (ii) bewiesen.

Ist $k \geq 2$ und $a_1 \equiv b_1 \,(m), \dots, a_k \equiv b_k \,(m)$, $a_{k+1} \equiv b_{k+1} \,(m)$, so folgt mit Induktionsvoraussetzung $a_1 \cdots a_k \equiv b_1 \cdots b_k \,(m)$. Daraus folgt mit Hilfe von Satz 39 (ii)

$$a_1 \cdots a_{k+1} = (a_1 \cdots a_k)\, a_{k+1} \equiv (b_1 \cdots b_k)\, b_{k+1} = b_1 \cdots b_{k+1} \,(m).$$

(v) Das ist der Spezialfall $a_1 = \dots = a_k = a$ und $b_1 = \dots = b_k = b$ von (iv).

(vi) Es sei $p(x) = c_\ell x^\ell + c_{\ell-1} x^{\ell-1} + \dots + c_1 x + c_0$ mit $c_0, c_1, \dots, c_\ell \in \mathbb{Z}$ und $a \equiv b \,(m)$.

Aus (v) folgt $a^2 \equiv b^2 \,(m)$, $a^3 \equiv b^3 \,(m)$, $\dots$, $a^{\ell-1} \equiv b^{\ell-1} \,(m)$, $a^\ell \equiv b^\ell \,(m)$.

Aus (ii) folgt $c_1 a \equiv c_1 b \,(m)$, $c_2 a^2 \equiv c_2 b^2 \,(m)$, $\dots$, $c_{\ell-1} a^{\ell-1} \equiv c_{\ell-1} b^{\ell-1} \,(m)$, $c_\ell a^\ell \equiv c_\ell b^\ell \,(m)$.

Aus (iii) folgt schließlich

$$p(a) = c_\ell a^\ell + c_{\ell-1} a^{\ell-1} + \dots + c_1 a + c_0 \equiv c_\ell b^\ell + c_{\ell-1} b^{\ell-1} + \dots + c_1 b + c_0 = p(b) \,(m)$$

(vii) Das ist der Spezialfall $\operatorname{ggT}(m,n) = 1$ von Satz 39 (v).

Beispiele: 1) Ein $n \in \mathbb{Z}$ ist genau dann gerade (bzw. ungerade), wenn $n \equiv 0 \,(2)$ (bzw. $n \equiv 1 \,(2)$).

Sind $n, m \in \mathbb{Z}$ gerade, so ist $n \equiv m \equiv 0 \,(2)$ und daher $n + m \equiv 0 + 0 = 0 \,(2)$, d.h. die Summe zweier geraden Zahlen ist gerade.

Ist $n \in \mathbb{Z}$ gerade und $m \in \mathbb{Z}$ ungerade, so ist $n \equiv 0 \,(2)$ und $m \equiv 1 \,(2)$ und daher $n + m \equiv 0 + 1 = 1 \,(2)$, d.h. die Summe einer geraden und einer ungeraden Zahl ist ungerade.

Sind $n, m \in \mathbb{Z}$ ungerade, so ist $n \equiv m \equiv 1 \,(2)$ und daher $n + m \equiv 1 + 1 = 2 \equiv 0 \,(2)$, d.h. die Summe zweier ungeraden Zahlen ist gerade und $n \cdot m \equiv 1 \cdot 1 = 1 \,(2)$, d.h. das Produkt zweier ungeraden Zahlen ist ungerade.

12.5.2025

2) Haben $m, n \in \mathbb{Z}$ die Gestalt $4k+1$, so hat auch ihr Produkt $m \cdot n$ diese Gestalt:

Ist $m = 4k+1$, $n = 4l+1$, so $m \cdot n = (4k+1)(4l+1) = 16kl + 4k + 4l + 1 = 4(4kl + k + l) + 1$

Hat m die Gestalt $4k+1$ und n die Gestalt $4k+3$, so hat $m \cdot n$ die Gestalt $4k+3$:

Ist $m = 4k+1$, $n = 4l+3$, so $m \cdot n = (4k+1)(4l+3) = 16kl + 12k + 4l + 3 = 4(4kl + 3k + l) + 3$

Haben m, n beide Gestalt $4k+3$, so hat $m \cdot n$ die Gestalt $4k+1$:

Ist $m = 4k+3$, $n = 4l+3$, so $m \cdot n = (4k+3)(4l+3) = 16kl + 12k + 12l + 9 = 4(4kl + 3k + 3l + 2) + 1$

Diese Überlegungen kann man mit Hilfe von Kongruenzen stark verkürzen:

Haben m, n beide Gestalt $4k+1$, so $m \equiv n \equiv 1 \,(4) \Rightarrow m \cdot n \equiv 1 \cdot 1 = 1 \,(4)$.

Hat m Gestalt $4k+1$ und n Gestalt $4k+3$, so $m \equiv 1 \,(4)$, $n \equiv 3 \,(4) \Rightarrow m \cdot n \equiv 1 \cdot 3 = 3 \,(4)$

Haben m, n beide Gestalt $4k+3$, so $m \equiv n \equiv 3 \,(4) \Rightarrow m \cdot n \equiv 3 \cdot 3 = 9 \equiv 1 \,(4)$.

Diese Rechnung kann man weiter vereinfachen, indem man $m \equiv n \equiv -1 \,(4)$ verwendet, woraus $m \cdot n \equiv (-1) \cdot (-1) = 1 \,(4)$ folgt.

3) Wir zeigen, dass jede Zehnerpotenz bei Division durch 9 Rest 1 lässt. Elementar kann man das so begründen:

$10 = 9+1$, $100 = 99+1 = 9\cdot 11+1$, $1000 = 999+1 = 9\cdot 111+1$, $10\,000 = 9999+1 = 9\cdot 1111+1$

und allgemein ist $\underbrace{10\ldots0}_{k \text{ Nullen}} = \underbrace{9\ldots9}_{k \text{ Neuner}} + 1 = 9\cdot \underbrace{1\ldots1}_{k \text{ Einser}} + 1$.

Mit Kongruenzen: $10 \equiv 1 \ (9) \Rightarrow 10^k \equiv 1^k = 1 \ (9) \quad \forall k \in \mathbb{N}^+$.

4) Wir bestimmen den Rest der Zahl $2\cdot 3^2\cdot 7^2\cdot 13^2\cdot 113^2$ bei Division durch 11:

Elementar mittels mittels Multiplikation und Division mit Rest:

$$2\cdot 3^2\cdot 7^2\cdot 13^2\cdot 113^2 = 1\,903\,321\,602 = 11\cdot 173\,029\,236 + 6$$

Mit Hilfe von Kongruenzen:

$$2\cdot 3^2\cdot 7^2\cdot 13^2\cdot 113^2 \equiv 2\cdot 9\cdot (-4)^2\cdot 2^2\cdot 3^2 \equiv 2\cdot(-2)\cdot 16\cdot 36 \equiv -4\cdot 5\cdot 3$$
$$= -12\cdot 5 \equiv -1\cdot 5 = -5 \equiv 6 \ (11)$$

Es ist bei solchen Rechnungen oft hilfreich, auch negative Zahlen zu verwenden (wie z. B. hier $7 \equiv -4 \ (11)$), damit die auftretenden Zahlen (absolut) kleiner sind.

Vorbemerkung: Eine wichtige Anwendung von Kongruenzen sind Teilbarkeitsregeln

1) Teilbarkeit durch 2: $2 \mid 7414$ aber $2 \nmid 7415$. Das kann man durch Division mit Rest begründen ($7414 = 2\cdot 3707$ aber $7415 = 2\cdot 3707 + 1$), es reicht aber, die Einerstelle zu betrachten ($2 \mid 4$ aber $2 \nmid 5$). Grundlage dafür sind die Kongruenzen

$$7414 = 7410 + 4 = 10\cdot 741 + 4 = 2\cdot(5\cdot 741) + 4 \equiv 4 \equiv 0 \ (2)$$
$$7415 = 7410 + 5 = 10\cdot 741 + 5 = 2\cdot(5\cdot 741) + 5 \equiv 5 \equiv 1 \ (2)$$

2) Teilbarkeit durch 3: $3 \mid 2547$ aber $3 \nmid 2557$. Das kann man durch Division mit Rest begründen ($2547 = 3\cdot 849$ aber $2557 = 3\cdot 852 + 1$), es reicht aber, die Ziffernsumme zu betrachten ($3 \mid 2547 \Leftrightarrow 3 \mid (2+5+4+7) \Leftrightarrow 3 \mid 18$ aber $3 \nmid 2557 \Leftrightarrow 3 \nmid (2+5+5+7) \Leftrightarrow 3 \nmid 19$)

Grundlage dafür sind die folgenden Kongruenzen

$$2547 = 2\cdot 1000 + 5\cdot 100 + 4\cdot 10 + 7 = 2\cdot(999+1) + 5\cdot(99+1) + 4\cdot(9+1) + 7$$
$$= 2\cdot 999 + 5\cdot 99 + 4\cdot 9 + (2+5+4+7) = 3\cdot(2\cdot 333 + 5\cdot 33 + 4\cdot 3) + (2+5+4+7)$$
$$\equiv 2+5+4+7 = 18 \equiv 0 \ (3)$$

$$2557 = 2\cdot 1000 + 5\cdot 100 + 5\cdot 10 + 7 = 2\cdot(999+1) + 5\cdot(99+1) + 5\cdot(9+1) + 7$$
$$= 2\cdot 999 + 5\cdot 99 + 5\cdot 9 + (2+5+5+7) = 3\cdot(2\cdot 333 + 5\cdot 33 + 5\cdot 3) + (2+5+5+7)$$
$$\equiv 2+5+5+7 = 19 \equiv 1 \ (3)$$

Lemma 41 Es seien $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$, $m \geq 2$ und $a \equiv b \,(m)$. Dann gilt $m \mid a \iff m \mid b$.

Beweis Nach Satz 36 $\exists k \in \mathbb{Z}: a = b + km$. Aus $m \mid a$ folgt wegen $b = a - km$ mittels Satz 1 (x), dass $m \mid b$. Gilt $m \mid b$, so folgt aus $a = b + km$ mittels Satz 1 (x), dass $m \mid a$.

Satz 42 Die Zahl $n \in \mathbb{N}^+$ habe dekadische Darstellung $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0$ mit Ziffern $a_k, a_{k-1}, \dots, a_1, a_0 \in \{0, 1, \dots, 9\}$ (wofür man $n = a_k a_{k-1} \dots a_1 a_0$ schreibt).

(i) $n \equiv a_0 \,(2)$,

(ii) $n \equiv a_k + a_{k-1} + \dots + a_1 + a_0 \,(3)$,

(iii) $n \equiv 10 \cdot a_1 + a_0 \,(4)$,

(iv) $n \equiv a_0 \,(5)$,

(v) $n \equiv 10^2 \cdot a_2 + 10 \cdot a_1 + a_0 \,(8)$,

(vi) $n \equiv a_k + a_{k-1} + \dots + a_1 + a_0 \,(9)$,

(vii) $n \equiv a_0 \,(10)$,

(viii) $n \equiv (-1)^k a_k + (-1)^{k-1} a_{k-1} + \dots + a_2 - a_1 + a_0 \,(11)$.

Beweis: (i) Für $i \geq 1$ ist $10^i = 10 \cdot 10^{i-1} \equiv 0 \cdot 10^{i-1} = 0 \,(2)$ und daher

$$n = a_k \underbrace{\cdot 10^k}_{\equiv 0(2)} + a_{k-1} \underbrace{\cdot 10^{k-1}}_{\equiv 0(2)} + \dots + a_1 \underbrace{\cdot 10}_{\equiv 0(2)} + a_0 \equiv a_0 \,(2).$$

(ii) Aus $10 \equiv 1 \,(3)$ folgt $10^i \equiv 1^i = 1 \,(3)$ $\forall i \geq 1$ und daher

$$n = a_k \underbrace{\cdot 10^k}_{\equiv 1(3)} + a_{k-1} \underbrace{\cdot 10^{k-1}}_{\equiv 1(3)} + \dots + a_1 \underbrace{\cdot 10}_{\equiv 1(3)} + a_0 \equiv a_k + a_{k-1} + \dots + a_1 + a_0 \,(3)$$

(iii) Für $i \geq 2$ ist $10^i = 100 \cdot 10^{i-2} \equiv 0 \cdot 10^{i-2} = 0 \,(4)$ ($\because 100 = 4 \cdot 25$) und daher

$$n = a_k \underbrace{\cdot 10^k}_{\equiv 0(4)} + a_{k-1} \underbrace{\cdot 10^{k-1}}_{\equiv 0(4)} + \dots + a_2 \underbrace{\cdot 10^2}_{\equiv 0(4)} + a_1 \cdot 10 + a_0 \equiv a_1 \cdot 10 + a_0 \,(4)$$

(iv) Für $i \geq 1$ ist $10^i = 10 \cdot 10^{i-1} \equiv 0 \cdot 10^{i-1} = 0 \,(5)$ und daher

$$n = a_k \underbrace{\cdot 10^k}_{\equiv 0(5)} + a_{k-1} \underbrace{\cdot 10^{k-1}}_{\equiv 0(5)} + \dots + a_1 \underbrace{\cdot 10}_{\equiv 0(5)} + a_0 \equiv a_0 \,(5)$$

(v) Für $i \geq 3$ ist $10^i = 1000 \cdot 10^{i-3} \equiv 0 \cdot 10^{i-1} = 0 \,(8)$ ($\because 1000 = 8 \cdot 125$) und daher

$$n = a_k \underbrace{\cdot 10^k}_{\equiv 0(8)} + a_{k-1} \underbrace{\cdot 10^{k-1}}_{\equiv 0(8)} + \dots + a_3 \underbrace{\cdot 10^3}_{\equiv 0(8)} + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \,(8)$$

(vi) Aus $10 \equiv 1 \,(9)$ folgt $10^i \equiv 1^i = 1 \,(9)$ $\forall i \geq 1$ und daher

$$n = a_k \underbrace{\cdot 10^k}_{\equiv 1(9)} + a_{k-1} \underbrace{\cdot 10^{k-1}}_{\equiv 1(9)} + \dots + a_1 \underbrace{\cdot 10}_{\equiv 1(9)} + a_0 \equiv a_k + a_{k-1} + \dots + a_1 + a_0 \,(9)$$

(vii) Für $i \geq 1$ ist $10^i = 10 \cdot 10^{i-1} \equiv 0 \cdot 10^{i-1} = 0 \,(10)$ und daher

$$n = a_k \underbrace{\cdot 10^k}_{\equiv 0(10)} + a_{k-1} \underbrace{\cdot 10^{k-1}}_{\equiv 0(10)} + \dots + a_1 \underbrace{\cdot 10}_{\equiv 0(10)} + a_0 \equiv a_0 \,(10)$$

(viii) Aus $10 \equiv -1\ (11)$ folgt $10^i \equiv (-1)^i\ (11)\ \forall i \geq 1$ und daher

$$n = a_k \cdot \underbrace{10^k}_{\equiv (-1)^k (11)} + a_{k-1} \cdot \underbrace{10^{k-1}}_{\equiv (-1)^{k-1} (11)} + \cdots + a_2 \cdot \underbrace{10^2}_{\equiv 1 (11)} + a_1 \cdot \underbrace{10}_{\equiv -1 (11)} + a_0$$

$$\equiv (-1)^k a_k + (-1)^{k-1} a_{k-1} + \cdots + a_2 - a_1 + a_0 \ (11)$$

Korollar 43 (Teilbarkeitsregeln) Die Zahl $n \in \mathbb{N}^+$ habe dekadische Darstellung $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 10 + a_0$ mit Ziffern $a_k, a_{k-1}, \ldots, a_1, a_0 \in \{0, 1, \ldots, 9\}$.

(i) $2 \mid n \iff 2 \mid a_0 \iff a_0 \in \{0, 2, 4, 6, 8\}$,

(ii) $3 \mid n \iff 3 \mid (a_0 + a_1 + \cdots + a_k)$,

(iii) $4 \mid n \iff 4 \mid (10 a_1 + a_0)$,

(iv) $5 \mid n \iff 5 \mid a_0 \iff a_0 \in \{0, 5\}$,

(v) $8 \mid n \iff 8 \mid (100 a_2 + 10 a_1 + a_0)$,

(vi) $9 \mid n \iff 9 \mid (a_0 + a_1 + \cdots + a_k)$,

(vii) $10 \mid n \iff 10 \mid a_0 \iff a_0 = 0$,

(viii) $11 \mid n \iff 11 \mid (a_0 - a_1 + a_2 - + \cdots + (-1)^k a_k)$

Beweis: (i) Die Äquivalenz $2 \mid n \iff 2 \mid a_0$ folgt aus Lemma 41 und Satz 42 (i). Die Äquivalenz $2 \mid a_0 \iff a_0 \in \{0, 2, 4, 6, 8\}$ ist trivial.

(ii) – (viii) Die (ersten) Äquivalenzen folgen aus Lemma 41 und dem jeweiligen Punkt in Satz 42. Die zweiten Äquivalenzen in (iv) und (vii) sind trivial.

Bemerkungen: 1) In der Schule übliche Formulierungen wie z. B. „Eine Zahl ist durch 3 teilbar, wenn ihre Ziffernsumme durch 3 teilbar ist" sind eigentlich um „die halbe Wahrheit", da sie nur die Implikation $3 \mid (a_0 + a_1 + \cdots + a_k) \Rightarrow 3 \mid n$ beschreiben.

2) Die Teilbarkeitsregeln (ii), (vi) und (viii) kann man mehrmals anwenden, z. B.

$3 \mid (296\ 379\ 633) \iff 3 \mid (2+9+6+3+7+9+6+3+3) \iff 3 \mid 48 \iff 3 \mid (4+8) \iff 3 \mid 12$
$\iff 3 \mid (1+2) \iff 3 \mid 3$

19.5.2025

Lemma 44 Es seien $d_1, \ldots, d_\ell \in \mathbb{N}, d_1, \ldots, d_\ell \geq 2$ paarweise relativ prim und $n \in \mathbb{N}^+$. Äquivalent sind:

(i) $(d_1 \cdots d_\ell) \mid n$,

(ii) $d_1 \mid n, d_2 \mid n, \ldots, d_\ell \mid n$.

Beweis: $d_1 \mid n, \ldots, d_\ell \mid n \iff n$ ist gemeinsames Vielfaches von $d_1, \ldots, d_\ell$

$\overset{\text{Satz 27}}{\iff} \operatorname{kgV}(d_1, \ldots, d_\ell) \mid n \overset{\text{Satz 35}}{\iff} (d_1 \cdots d_\ell) \mid n$

Beispiele: Mit Hilfe von Lemma 44 kann man weitere Teilbarkeitsregeln ableiten

1) Korollar 43 (vii) folgt aus Korollar 43 (i) und (iv) denn

$10 \mid n \overset{\text{Lemma 44}}{\Longleftrightarrow} 2 \mid n$ und $5 \mid n \overset{\text{Kor. 43 (i),(iv)}}{\Longleftrightarrow} a_0 \in \{0,2,4,6,8\}$ und $a_0 \in \{0,5\} \Leftrightarrow a_0 = 0$

2) $6 \mid n \overset{\text{Lemma 44}}{\Longleftrightarrow} 2 \mid n$ und $3 \mid n \overset{\text{Kor. 43 (i),(ii)}}{\Longleftrightarrow} a_0 \in \{0,2,4,6,8\}$ und $3 \mid (a_0 + \dots + a_k)$

Satz 45 Es gibt unendlich viele Primzahlen p mit der Eigenschaft $p \equiv 3\ (4)$

Beweis: Angenommen, es gäbe nur endlich viele Primzahlen $\equiv 3\ (4)$, nämlich $p_1, \dots, p_n$.
Wir betrachten die Zahl $N = p_1^2 \cdots p_n^2 + 2$. Es gilt $N \equiv (-1)^2 \cdots (-1)^2 + 2 = 3\ (4)$.
Es sei $N = q_1 \cdots q_m$ die Primfaktorzerlegung von N. Da $2 \nmid N$ ist $2 \notin \{q_1, \dots, q_m\}$.
Also gilt $q_i \equiv 1\ (4)$ oder $q_i \equiv 3\ (4)$ für $1 \le i \le m$. Aus $q_i \equiv 1\ (4)$ für alle $i \in \{1, \dots, m\}$ würde $N \equiv 1\ (4)$ folgen, Widerspruch. Also $\exists j \in \{1, \dots, m\} : q_j \equiv 3\ (4)$. Nun ist aber $q_j \notin \{p_1, \dots, p_n\}$. (Wäre nämlich $q_j \in \{p_1, \dots, p_n\}$, so würde aus $q_j \mid N$ und $q_j \mid p_1^2 \cdots p_n^2$ folgen, dass $q_j \mid (N - p_1^2 \cdots p_n^2)$, d.h. $q_j \mid 2$, ein Widerspruch.) Das ist ein Widerspruch dazu, dass $p_1, \dots, p_n$ bereits alle Primzahlen $\equiv 3\ (4)$ sind.

Bemerkung: Allgemein gilt der DIRICHLETsche Primzahlsatz: Ist $a \in \mathbb{Z}$, $m \in \mathbb{N}$, $m \ge 2$ und $\operatorname{ggT}(a,m) = 1$, so gibt es unendlich viele Primzahlen $p \equiv a\ (m)$. Man beweist ihn mit analytischen Hilfsmitteln. Es gibt aber elementare Beweise für viele spezielle Werte von a und m.