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) Es gibt ein $k \in \mathbb{Z}$, derart dass $a = b + km$.

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 $a - b = (q_1 m + r) - (q_2 m + r) = q_1 m - q_2 m = (q_1 - q_2) m$ und daher $m \mid (a-b)$.

(ii) $\Rightarrow$ (iii) Da $m \mid (a-b)$, gibt es ein $k \in \mathbb{Z}$ mit der Eigenschaft $a - b = km$ und daher $a = b + km$.

(iii) $\Rightarrow$ (i) Wir führen für b und m Division mit Rest durch, dh $b = qm + r$ für $q, r \in \mathbb{Z}$ mit $0 \leq r < m$. Dann ist $a = b + km = qm + r + km = (q+k)m + r$ und die 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 bei Bedingungen aus Satz 36 erfüllen. Man schreibt dafür $a \equiv b \pmod m$ oder kurz $a \equiv b \,(m)$. Die Zahl m heißt dabei Modul. 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.

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

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

23.5.2022

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

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

(i) $a \equiv a \,(m)$ für jedes $a \in \mathbb{Z}$, dh Kongruenz modulo m ist reflexiv,

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

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

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

Erinnerung: Jede Äquivalenzrelation zerlegt die Menge, auf der sie definiert ist, in Äquivalenzklassen. Das sind paarweise disjunkte Teilmengen, die folgendermaßen definiert sind: Ist a ein Element der Menge, auf der die Äquivalenzrelation definiert ist, so besteht die Äquivalenzklasse von a aus allen Elementen, 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) Ist $a \in \mathbb{Z}$, so besteht die Restklasse von a aus allen ganzen Zahlen, die bei Division durch m den selben Rest haben wie a,

(ii) Ist $a \in \mathbb{Z}$, so ist die Restklasse von a die Menge $\{a+km \mid k \in \mathbb{Z}\}$.

(iii) $\mathbb{Z}$ zerfällt durch die Äquivalenzrelation der Kongruenz modulo m in genau m Restklassen.

Beweis: (i) Das folgt aus der Charakterisierung (i) der Kongruenz modulo m in Satz 36 und der Definition der Restklasse.

(ii) Das folgt aus der Charakterisierung (iii) der Kongruenz modulo m in Satz 36 und der Definition der Restklasse.

(iii) Bei Division mit Rest durch m gibt es genau m mögliche Reste, nämlich $0, 1, 2, \dots, m-1$. Jeder dieser Reste legt eine Restklasse fest, die sich von allen anderen unterscheidet. Die Behauptung folgt nun aus (i).

Beispiele: 1) Für $m=2$ zerfällt $\mathbb{Z}$ durch Kongruenz modulo 2 in zwei Restklassen. Diese bestehen nach Satz 38 (i) aus allen ganzen Zahlen, die bei Division durch 2 Rest 0 bzw. 1 haben. Da die erste der beiden Restklassen besteht aus allen geraden ganzen Zahlen $\dots, -4, -2, 0, 2, 4, \dots$ und die zweite aus allen ungeraden ganzen Zahlen $\dots, -5, -3, -1, 1, 3, 5, \dots$ Verwendet man stattdessen Satz 38 (ii), so kann man die beiden Restklassen auch als $\{0+2k \mid k \in \mathbb{Z}\} = \{2k \mid k \in \mathbb{Z}\}$ und $\{1+2k \mid k \in \mathbb{Z}\}$ schreiben.

2) Für $m=3$ zerfällt $\mathbb{Z}$ durch Kongruenz modulo 3 in drei Restklassen. Diese bestehen aus allen ganzen Zahlen, die bei Division durch 3 Rest 0, 1 bzw. 2 haben. Alternativ kann man sie auch als die Mengen $\{3k \mid k \in \mathbb{Z}\}$, $\{3k+1 \mid k \in \mathbb{Z}\}$ und $\{3k+2 \mid k \in \mathbb{Z}\} = \{3k-1 \mid k \in \mathbb{Z}\}$ schreiben.

Satz 39 (Rechenregeln für Kongruenzen) Es seien $m \in \mathbb{N}$, $m \geq 2$ und $a, b, c, d, n \in \mathbb{Z}$, wobei $n \neq 0$ gelten soll.

(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 $n \mid m$ (wobei $|n| \geq 2$ gelten soll) folgt $a \equiv b\ (|n|)$,

(iv) Aus $a \equiv b\ (m)$ folgt $na \equiv nb\ (|n|m)$,

(v) $na \equiv nb\ (m) \iff a \equiv b\ \left(\frac{m}{ggT(m,n)}\right)$.

Beweis: (i) Nach Satz 36 (iii) gibt es $k, l \in \mathbb{Z}$, sodass $a = b + km$ und $c = d + lm$. Daher ist $a+c = (b+km) + (d+lm) = b+d+(k+l)m$ und $a+c \equiv b+d\ (m)$ wegen Satz 36 (iii).

(ii) Wenn $k, l \in \mathbb{Z}$ die selbe Bedeutung haben wie im Beweis von (i), so ist

$$ac = (b+km)(d+lm) = bd + kdm + lbm + klm^2 = bd + (kd + lb + klm)m$$

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 gibt es ein $k \in \mathbb{Z}$, sodass $a - b = km$. Daraus folgt sofort $na - nb = n(a-b) = knm$. Also gilt $nm \mid (na - nb)$ und daher (wegen Satz 1 (iii)) auch $|n|m \mid (na - nb)$, also $na \equiv nb\ (|n|m)$.

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

($\Rightarrow$) Nach Satz 36 gilt $m \mid (na - nb)$, d.h. es gibt ein $k \in \mathbb{Z}$ mit der Eigenschaft $na - nb = km$ bzw. $n(a-b) = km$. Es folgt sofort $\frac{n}{d}(a-b) = k\frac{m}{d}$. Dabei sind $\frac{m}{d}, \frac{n}{d} \in \mathbb{Z}$ da $d = ggT(m,n)$. Also gilt $\frac{m}{d} \mid \frac{n}{d}(a-b)$. Wegen Korollar 10 ist $ggT\left(\frac{m}{d}, \frac{n}{d}\right) = 1$ und mit Hilfe von Satz 12 erhält man $\frac{m}{d} \mid (a-b)$.

Das besagt wegen Satz 36 aber gerade $a \equiv b\ \left(\frac{m}{ggT(n,m)}\right)$.

($\Leftarrow$) Nach Satz 36 gilt $\frac{m}{d} \mid (a-b)$, d.h. es gibt ein $k \in \mathbb{Z}$ mit der Eigenschaft $a - b = k\frac{m}{d}$. Daraus erhält man $na - nb = n(a-b) = k\frac{m}{d}n = \left(k\frac{n}{d}\right)m$.

Da $k\frac{n}{d} \in \mathbb{Z}$, gilt $m \mid (na - nb)$ und daher $na \equiv nb\ (m)$.

Bemerkung: Satz 39 (i) und (ii) besagen, dass die Restklassen der Summe $a+c$ und des Produkts $a \cdot c$ zweier ganzer Zahlen a und c nur von den Restklassen von a und c abhängt.

Korollar 40 (Vier 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 $a_1 \cdot \dots \cdot a_k \equiv b_1 \cdot \dots \cdot b_k\ (m)$ (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 $k \in \mathbb{N} \setminus \{0\}$),

(vi) Ist p ein Polynom mit ganzzahligen Koeffizienten 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 $\operatorname{ggT}(m,n) = 1$ folgt $a \equiv b\ (m)$ (für $a,b,n \in \mathbb{Z}$ und $n \neq 0$).

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

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

(iii) Induktion nach k. Im Fall $k = 1$ ist nichts zu beweisen und der Fall $k = 2$ wurde in Satz 39 (i) bewiesen. Es sei nun $k \geq 2$ und

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

Nach Induktionsvoraussetzung folgt aus den k ersten Kongruenzen $a_1 + \dots + a_k \equiv b_1 + \dots + b_k\ (m)$. Daraus und aus der letzten Kongruenz folgt mit Hilfe von Satz 39 (i)

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

30.5.2022

(iv) Induktion nach k. Im Fall $k = 1$ ist nichts zu beweisen und der Fall $k = 2$ wurde in Satz 39 (ii) bewiesen. Es sei nun $k \geq 2$ und

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

Nach Induktionsvoraussetzung folgt aus den k ersten Kongruenzen $a_1 \cdot \dots \cdot a_k \equiv b_1 \cdot \dots \cdot b_k\ (m)$. Daraus und aus der letzten Kongruenz folgt mit Hilfe von Satz 39 (ii)

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

(v) Das ist ein Spezialfall von (iv), den man für $a_1 = \dots = a_k = a$ und $b_1 = \dots = b_k = b$ erhält.

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

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

Aus (ii) folgt

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

Aus (iii) folgt schließlich

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

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

Beispiele: 1) Haben $m, n \in \mathbb{Z}$ die Gestalt $4k+1$, so hat auch das Produkt $m \cdot n$ diese Gestalt. Ist $m = 4k+1$ und $n = 4\ell+1$, so ist

$$m \cdot n = (4k+1)\cdot(4\ell+1) = 16k\ell + 4k + 4\ell + 1 = 4(4k\ell + k + \ell) + 1.$$

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

Ist $m = 4k+1$ und $n = 4\ell+3$, so ist

$$m \cdot n = (4k+1)\cdot(4\ell+3) = 16k\ell + 12k + 4\ell + 3 = 4(4k\ell + 3k + \ell) + 3.$$

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

Ist $m = 4k+3$ und $n = 4\ell+3$, so ist

$$m \cdot n = (4k+3)(4\ell+3) = 16k\ell + 12k + 12\ell + 9 = 4(4k\ell + 3k + 3\ell + 2) + 1.$$

Diese Rechnungen lassen sich durch die Verwendung von Kongruenzen stark verkürzen. Dass m und n die Gestalt $4k+1$ haben, besagt gerade $m \equiv 1\,(4)$ und $n \equiv 1\,(4)$. Wegen Satz 39 (ii) folgt $m \cdot n \equiv 1 \cdot 1 = 1\,(4)$.

Hat m die Gestalt $4k+1$ und n die Gestalt $4k+3$, so ist $m \equiv 1\,(4)$ und $n \equiv 3\,(4)$ und daher (wieder wegen Satz 39 (ii)) $m \cdot n \equiv 1 \cdot 3 = 3\,(4)$.

Haben m und n beide die Gestalt $4k+3$, so ist $m \equiv 3\,(4)$ und $n \equiv 3\,(4)$ und daher $m \cdot n \equiv 3 \cdot 3 = 9 \equiv 1\,(4)$. Diese Rechnung lässt sich noch weiter vereinfachen, wenn man stattdessen $m \equiv -1\,(4)$ und $n \equiv -1\,(4)$ verwendet, woraus $m \cdot n \equiv (-1)\cdot(-1) = 1\,(4)$ folgt.

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

$10 = 9 + 1$, $100 = 99 + 1 = 9 \cdot 11 + 1$, $1000 = 999 + 1 = 9 \cdot 111 + 1$, $10000 = 9999 + 1 = 9 \cdot 1111 + 1$

bzw. allgemein gilt $\underbrace{10\ldots0}_{k\text{ Nullen}} = \underbrace{9\ldots9}_{k\text{ Neunen}} + 1 = 9 \cdot \underbrace{1\ldots1}_{k\text{ Einsen}} + 1$.

Auch diese Rechnung wird durch die Verwendung von Kongruenzen stark vereinfacht. Aus $10 \equiv 1\ (9)$ folgt (mittels Korollar 40 (v)) $10^k \equiv 1^k = 1\ (9)$ für alle $k \in \mathbb{N} \setminus \{0\}$.

3) Wir bestimmen den Rest der Zahl $2 \cdot 3^2 \cdot 7^2 \cdot 13^2 \cdot 113^2$ bei Division durch 11.
Es ist natürlich möglich, zu multiplizieren und mit Rest durch 11 zu dividieren:

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

Bei Verwendung von Kongruenzen rechnen wir mit ein- und zweistellige Zahlen auf:

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

$$\equiv -1 \cdot 5 = -5 \equiv 6\ (11)$$

Es ist dabei sehr hilfreich auch negative Zahlen zu verwenden. Z.B. folgt aus $7 \equiv -4\ (11)$, dass $7^2 \equiv (-4)^2\ (11)$, da die auftretenden Zahlen sind (absolut) kleiner

Bemerkungen: 1) Die vorangegangenen Beispiele zeigen, dass viele Rechnungen mit Hilfe von Kongruenzen rascher und einfacher durchgeführt werden können. Man kann sich das Rechnen mit Kongruenzen modulo n als eine Art „Stern"-Version des Rechnens mit Resten bei Division durch n vorstellen.

2) Satz 39 (v) ist Quelle vieler Fehler. Aus $16 \equiv 6\ (10)$, da $2 \cdot 8 \equiv 2 \cdot 3\ (10)$, folgt nicht, dass $8 \equiv 3\ (10)$, was offensichtlich falsch ist. Anwendung von Satz 39 (v) ergibt aber korrekt $8 \equiv 3\ \left(\frac{10}{ggT(2,10)}\right)$, da $8 \equiv 3\ \left(\frac{10}{2}\right)$ bzw. $8 \equiv 3\ (5)$.
Es ist aber korrekt, aus $16 \equiv 6\ (5)$, da $2 \cdot 8 \equiv 2 \cdot 3\ (5)$ zu schließen, dass $8 \equiv 3\ (5)$, da $ggT(2,5) = 1$. (Man kann dafür Satz 39 (v) oder Korollar 40 (vii) verwenden.)

Vorbemerkung: Wir wollen nun mit Hilfe von Kongruenzen Teilbarkeitsregeln beweisen.
1) Offenbar gilt $2 \mid 7414$ aber $2 \nmid 7415$. Man kann das mittels Division mit Rest begründen ($7414 = 2 \cdot 3707$ und $7415 = 2 \cdot 3707 + 1$), wird aber in der Regel argumentieren, dass die Einerstellen 4 gerade bzw. 5 ungerade ist. Dabei werden implizit Kongruenzen modulo 2 verwendet:

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

Man erkennt, dass eine Zahl modulo 2 zu ihrer Einerstelle kongruent ist.
Man kann auch sagen, dass die Zahl in zwei Teile aufgeteilt wird: Einen Teil, der durch 2 teilbar ist (die Stellen vor der Einerstelle) und einen Rest (die Einerstelle). Bei der Teilbarkeit durch 2 kommt es dann nur darauf an, ob der Rest (also die Einerstelle) durch 2 teilbar ist.

2) Es gilt $3 \mid 2547$ aber $3 \nmid 2557$. Auch das kann man mittels Division mit Rest begründen ($2547 = 3 \cdot 849$ und $2557 = 3 \cdot 852 + 1$), wird aber normalerweise argumentieren, dass die Ziffernsumme $2+5+4+7 = 18$ durch 3 teilbar bzw. $2+5+5+7 = 19$ nicht durch 3 teilbar ist. Auch hier werden implizit Kongruenzen modulo 3 verwendet:

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

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

Man erkennt, dass eine Zahl modulo 3 zu ihrer Ziffernsumme kongruent ist. Man kann auch hier sagen, dass die Zahl in zwei Teile aufgeteilt wird: Einen Teil, der durch 3 teilbar ist und den Rest (die Ziffernsumme). Bei der Teilbarkeit durch 3 kommt es nun darauf an, ob der Rest (d.h. die Ziffernsumme) durch 3 teilbar ist.

13.6.2022

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

<u>Beweis</u>: Nach Satz 36 gibt es ein $k \in \mathbb{Z}$, derart dass $a = b + km$. Gilt $m \mid a$, so 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 $m \mid a$.

<u>Satz 42</u> Die Zahl $n \in \mathbb{N} \setminus \{0\}$ habe die dekadische Darstellung

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0 \quad \text{mit Ziffern } a_k, a_{k-1}, \ldots, a_1, a_0 \in \{0,1,\ldots,9\}$$

(wofür man $n = a_k a_{k-1} \cdots a_1 a_0$ schreibt). Dann gelten:

(i) $n \equiv a_0 \ (2)$ (D.h. jede Zahl ist modulo 2 zu ihrer Einerstelle kongruent.)

(ii) $n \equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \ (3)$
(D.h. jede Zahl ist modulo 3 zu ihrer Ziffernsumme kongruent.)

(iii) $n \equiv 10 \cdot a_1 + a_0 \ (4)$ (D.h. jede Zahl ist modulo 4 zu jener Zahl kongruent, die aus ihrer Zehner- und Einerstelle gebildet wird.)

(iv) $n \equiv a_0 \ (5)$ (D.h. jede Zahl ist modulo 5 zu ihrer Einerstelle kongruent.)

(v) $n \equiv 10^2 \cdot a_2 + 10 \cdot a_1 + a_0 \ (8)$ (D.h. jede Zahl ist modulo 8 zu jener Zahl kongruent, die aus ihrer Hunderter-, Zehner und Einerstelle gebildet wird.)

(vi) $n \equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \ (9)$
(D.h. jede Zahl ist modulo 9 zu ihrer Ziffernsumme kongruent.)

(vii) $n \equiv a_0 \ (10)$ (D.h. jede Zahl ist modulo 10 zu ihrer Einerstelle kongruent.)

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

(D.h. jede Zahl ist modulo 11 zu ihrer alternierenden Ziffernsumme kongruent.)

Beweis: (i) Für $i \geq 1$ ist $10^i = 10 \cdot 10^{i-1} = 2 \cdot (5 \cdot 10^{i-1}) \equiv 0 \ (2)$ und daher

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

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

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

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

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

(iv) Für $i \geq 1$ ist $10^i = 10 \cdot 10^{i-1} = 5 \cdot (2 \cdot 10^{i-1}) \equiv 0 \ (5)$ und daher

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

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

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

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

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

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

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

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

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

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

Bemerkung: Punkt (viii) ohne Verwendung von Kongruenzen zu beweisen, ist möglich aber schon recht umständlich, da man, um 10^i modulo 11 zu bestimmen, zwischen geraden und ungeraden Exponenten i unterscheiden muss.

Für gerades i verwendet man $99 = 9 \cdot 11$, $9999 = 909 \cdot 11$, $999999 = 90909 \cdot 11$, ...

Für ungerades i verwendet man $1001 = 91 \cdot 11$, $100001 = 9091 \cdot 11$, $10000001 = 909091 \cdot 11$, ...

Korollar 43 (Teilbarkeitsregeln) Die Zahl $n \in \mathbb{N} \setminus \{0\}$ habe die dekadische Darstellung

$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0$ mit Ziffern $a_k, a_{k-1}, \ldots, a_1, a_0 \in \{0,1,\ldots,9\}$

(wofür man $n = a_k a_{k-1} \cdots a_1 a_0$ schreibt). Dann gelten die folgenden Teilbarkeitsregeln:

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

(Eine Zahl ist genau dann durch 2 teilbar wenn ihre Einerstelle durch 2 teilbar ist.)

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

(Eine Zahl ist genau dann durch 3 teilbar wenn ihre Ziffernsumme durch 3 teilbar ist.)

(iii) $4 \mid n \iff 4 \mid (10a_1 + a_0)$ (Eine Zahl ist genau dann durch 4 teilbar, wenn die Zahl, die aus ihrer Zehner- und Einerstelle besteht, durch 4 teilbar ist.)

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

(Eine Zahl ist genau dann durch 5 teilbar wenn ihre Einerstelle durch 5 teilbar ist.)

(v) $8 \mid n \iff 8 \mid (100a_2 + 10a_1 + a_0)$ (Eine Zahl ist genau dann durch 8 teilbar, wenn die Zahl, die aus ihrer Hunderter-, Zehner- und Einerstelle besteht, durch 8 teilbar ist.)

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

(Eine Zahl ist genau dann durch 9 teilbar, wenn ihre Ziffernsumme durch 9 teilbar ist.)

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

(Eine Zahl ist genau dann durch 10 teilbar wenn ihre Einerstelle $= 0$ ist.)

(viii) $11 \mid n \iff 11 \mid (a_0 - a_1 + a_2 - + \cdots + (-1)^k a_k)$ (Eine Zahl ist genau dann durch 11 teilbar wenn ihre alternierende Ziffernsumme durch 11 teilbar ist.)

Beweis: (i) Die Äquivalenz $2 \mid n \iff 2 \mid a_0$ folgt sofort 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) Diese (ersten) Äquivalenzen folgen sofort aus Lemma 41 und den entsprechenden Punkten in Satz 42. Die zweiten Äquivalenzen in den Punkten (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 nur „die halbe Wahrheit", da sie nur die Implikation $3 \mid n \impliedby 3 \mid (a_0 + a_1 + \cdots + a_k)$ beschreiben.

2) Die Teilbarkeitsregeln (ii), (vi) und (viii) kann man mehrfach anwenden. Z.B. ist $3 \mid (296\,379\,633) \iff 3 \mid (2+9+6+3+7+9+6+3+3)$

$\iff 3 \mid 48 \iff 3 \mid (4+8) \iff 3 \mid 12 \iff 3 \mid (1+2) \iff 3 \mid 3$

Lemma 44 Es seien $d_1, \dots, d_\ell \in \mathbb{N} \setminus \{0,1\}$ paarweise relativ prim und $n \in \mathbb{N} \setminus \{0\}$. Dann sind äquivalent:

(i) $(d_1 \cdot \dots \cdot d_\ell) \mid n$,

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

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

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

Beispiele: Lemma 44 kann verwendet werden, um weitere Teilbarkeitsregeln aus den bisher bewiesenen abzuleiten, z.B.:

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

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

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

20.6.2022

[Ende Prüfungsstoff 1. Prüfungstermin]