(9.30) SATZ: Für $n \in \mathbb{N}, n \geq 2$ sind folgende Aussagen äquivalent:

a) n ist eine Primzahl

b) n besitzt keinen Teiler $t \in \mathbb{N}$ mit $2 \leq t \leq \lfloor\sqrt{n}\rfloor$

c) n besitzt keinen Primteiler p mit $p \leq \lfloor\sqrt{n}\rfloor$.

(9.31) BEM: Primzahltest

Es soll eine Zahl $n \in \mathbb{N}, n \geq 2$ auf Primzahleigenschaft getestet werden:

a) Untersuche, ob eine der Zahlen $2, 3, \ldots, \lfloor\sqrt{n}\rfloor$ ein Teiler von n ist. Wenn ja, ist n keine Primzahl, wenn nein, so ist n nach (9.30) prim. In diesem Falle sind $\lfloor\sqrt{n}\rfloor - 1$ Divisionen erforderlich, problematisch für große n.

b) Untersuche, ob eine der Primzahlen $\leq \lfloor\sqrt{n}\rfloor$ ein Teiler von n ist. Aufwand, falls n prim: $\pi(\lfloor\sqrt{n}\rfloor)$ Divisionen. Problematisch: Erstellen von Primzahllisten. Dafür gibt es Siebverfahren, in der einfachsten Form: **Sieb von Eratosthenes**.

c) Sei $\mathbb{P}' := \{2, 3, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, \ldots\}$. Diese Menge besteht aus 2,3 und allen Zahlen der Form $6k-1, 6k+1$ $(k \in \mathbb{N})$. Nach Aufgabe 39 gilt $\mathbb{P} \subseteq \mathbb{P}'$. Nach (9.30) gilt

$$n \in \mathbb{P} \iff \forall t \in \mathbb{P}', t \leq \lfloor\sqrt{n}\rfloor : t \not| \, n.$$

Im Gegensatz zur Menge aller Primzahlen $\leq \lfloor\sqrt{n}\rfloor$ läßt sich die Menge $\mathbb{P}'$ leicht bilden: beginnend mit 5 addiere abwechselnd 2 und 4. Im Falle daß n Primzahl ist, sind ungefähr $\lfloor\sqrt{n}\rfloor/3$ Divisionen erforderlich.

In allen Fällen erhält man für "große" n kein Ergebnis in vernünftiger Zeit. Effizientere Methoden erfordern einen viel größeren mathematischen Aufwand.

(9.32) BEM: Primfaktorzerlegung

Um die Primfaktorzerlegung einer natürlichen Zahl $n \geq 2$ zu finden, gehe man folgendermaßen vor: Versuche, einen Teiler t von n mit $2 \leq t \leq \lfloor\sqrt{n}\rfloor$ zu bestimmen. Gibt es den nicht, so ist n eine Primzahl und die Primfaktorzerlegung von n ist n. Gibt es ihn dagegen, so verfahre mit t und $\frac{n}{t} \in \mathbb{N}$ analog. Nach endlich vielen Schritten ist n als Produkt von Primzahlen dargestellt.

(9.33) DEF: Seien $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$. a heißt **kongruent zu** b **modulo** m, in Zeichen $a \equiv b \pmod{m}$, wenn gilt

$$a \bmod m \;=\; b \bmod m$$

Die hierdurch definierte Relation auf $\mathbb{Z}$ heißt **Kongruenzrelation modulo** m.

$2 \equiv 5 \pmod{3}$ $\quad 3 \not\equiv 6 \pmod{4}$

(9.34) BEM: $a \equiv b \pmod{m} \iff m | a - b$

(9.35) SATZ: Für jedes $m \in \mathbb{N}$ ist die Kongruenzrelation modulo m eine Äquivalenzrelation auf $\mathbb{Z}$. Die Äquivalenzklassen nach dieser Relation heißen **Restklassen modulo** m. Mit $\mathbb{Z}_m$ wird die Menge aller Restklassen modulo m bezeichnet.

S. Beispiel 12 in §4, Def (4.8) und (4.9)

$[a]_m = \{ x \mid x \in \mathbb{Z}, x \equiv a \pmod m \} \subseteq \mathbb{Z}$ Restklasse von a modulo m. In einer Restklasse modulo m liegen alle ganzen Zahlen, die bei Division durch m denselben Rest haben.

$[2]_3 = \{ x \mid x \in \mathbb{Z}, x \equiv 2 \pmod 3 \} \subseteq \mathbb{Z}$ ist die Menge aller ganzen Zahlen, die bei Division durch 3 den Rest 2 haben. $[2]_3 = \{ \dots, -7, -4, -1, 2, 5, 8, 11, \dots \}$

$[0]_5 = \{ x \mid x \in \mathbb{Z}, x \equiv 0 \pmod 5 \} \subseteq \mathbb{Z}$ ist die Menge aller ganzen Zahlen, die bei Division durch 5 den Rest 0 haben, die also durch 5 teilbar sind.

$[0]_2 = \{ x \mid x \in \mathbb{Z}, x \equiv 0 \pmod 2 \}$ Menge der geraden ganzen Zahlen.

$[1]_2 = \{ x \mid x \in \mathbb{Z}, x \equiv 1 \pmod 2 \}$ Menge der ungeraden ganzen Zahlen.

Nach (4.10b) gilt $[a]_m = [b]_m \iff a \equiv b \pmod m$

(9.36) SATZ: Es gilt $\mathbb{Z}_m = \{ [0]_m, [1]_m, \dots, [m-1]_m \}$ und $|\mathbb{Z}_m| = m$.

Bew: $0, 1, \dots, m-1$ sind die möglichen Reste bei Division einer ganzen Zahl durch m.

Für das Rechnen mit Kongruenzen gelten die folgenden Regeln:

(9.37) SATZ: Gelte $a \equiv b \pmod m$ und $c \equiv d \pmod m$. Dann folgt:

a) $a + c \equiv b + d \pmod m$ **b)** $a \cdot c \equiv b \cdot d \pmod m$

c) $a^k \equiv b^k \pmod m \quad \forall\, k \in \mathbb{N}_0$.

Anwendung: Teilbarkeitsregel für 3:

Es gilt $10 \equiv 1 \pmod 3$, woraus nach (9.35c) $10^k \equiv 1 \pmod m$ für alle $k \in \mathbb{N}_0$ folgt. Sei $n = \sum_{k=0}^{r} a_k 10^k$ eine natürliche Zahl in Dezimaldarstellung. Dann ergibt sich $n \equiv \sum_{k=0}^{r} a_k \pmod m$ (rechts steht die Quersumme von n).

Also: $3|n \iff n \equiv 0 \pmod 3 \iff \sum_{k=0}^{r} a_k \equiv 0 \pmod 3 \iff 3 \mid \sum_{k=0}^{r} a_k$

Fazit: Eine ganze Zahl ist genau dann durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist.
Es gibt weitere einfache Teilbarkeitsregeln, etwa für die Teilbarkeit durch 2,4,5,8,9,11 .

(9.38) SATZ: Auf der Menge $\mathbb{Z}_m$ aller Restklassen modulo m lassen sich eine Addition und eine Multiplikation erklären, so daß $\mathbb{Z}_m$ ein kommutativer Ring ist. Diese Rechenoperationen sind definiert durch:

$$[a]_m + [b]_m := [a+b]_m \quad , \quad [a]_m \cdot [b]_m := [a \cdot b]_m$$

$[2]_5 + [4]_5 := [2+4]_5 = [6]_5 = [1]_5$, $[4]_6 \cdot [5]_6 = [4 \cdot 5]_6 = [20]_6 = [2]_6$

Für die Addition gelten die A_0) bis A_4) aus (1.1) entsprechenden Eigenschaften. Das Nullelement ist in diesem Fall $[0]_m$, und das zu $[a]_m$ negative Element ist die Restklasse $[-a]_m$. Für die Multiplikation gelten die M_0) bis M_3) entsprechenden Eigenschaften. Das Einselement ist hier $[1]_m$. Das Analoge zu M_4) gilt i.a. nicht, jedoch in Spezialfällen, wie wir gleich sehen werden. Das Distributive Gesetz ist wieder gültig.

Man nennt $\mathbb{Z}_m$ einen **kommutativen Ring** ($\mathbb{R}$ hatten wir als **Körper** bezeichnet).

Für die Addition und Multiplikation auf $\mathbb{Z}_m$ können wir sog. **Verknüpfungstafeln** aufstellen, z.B. für $\mathbb{Z}_3$ oder $\mathbb{Z}_4$.

(9.39) DEF: Eine Restklasse $[a]_m \in \mathbb{Z}_m$ heißt **invertierbar** (bzgl. der Multiplikation), wenn es eine Restklasse $[b]_m \in \mathbb{Z}_m$ gibt mit $[a]_m \cdot [b]_m = [1]_m$. $[b]_m$ heißt dann das **Inverse** von $[a]_m$.

(9.40) SATZ: Eine Restklasse $[a]_m \in \mathbb{Z}_m$ ist genau dann invertierbar, wenn a und m teilerfremd sind. Das Inverse läßt sich mit Hilfe des EEA berechnen.

Bew: Es sei $[a]_m$ invertierbar. Dann gibt es $b \in \mathbb{Z}$ mit $[1]_m = [a]_m \cdot [b]_m = [a \cdot b]_m$, d.h.es gilt $ab \equiv 1 \pmod m$, oder $m|1-ab$. Folglich gibt es ein $c \in \mathbb{Z}$ mit $mc = 1-ab$ oder $mc+ab = 1$. Sei nun $g := \mathrm{ggT}(a,m)$. Aus $g|a$ und $g|m$ folgt $g|mc+ab$, also $g|1$ und damit $g = 1$.

Gelte umgekehrt $\mathrm{ggT}(a,m) = 1$. Dann existieren nach (9.12) $x, y \in \mathbb{Z}$ mit $1 = xa + ym$. Für die zugehörigen Restklassen modulo m bedeutet dies:

$$[1]_m = [xa + ym]_m = [xa]_m + [ym]_m = [xa]_m + [0]_m = [x]_m[a]_m$$

Folglich ist $[x]_m$ die inverse Restklasse zu $[a]_m$ und x läßt sich mit dem EEA berechnen.

(9.41) FOLG: Ist p eine Primzahl, so ist jede Restklasse $[a]_p \neq [0]_p$ invertierbar, d.h. $\mathbb{Z}_p$ ist ein Körper.

Bew: $\mathbb{Z}_p = \{[0]_p, [1]_p, \ldots, [p-1]_p\}$. Für $k = 1, 2, \ldots, p-1$ ist $\mathrm{ggT}(k,p) = 1$, so daß die Restklassen $[1]_p, [2]_p, \ldots, [p-1]_p$ alle invertierbar sind. Dies sind aber alle von $[0]_p$ verschiedenen Restklassen, so daß auch das Analoge von M_4) aus (1.1) gilt. Daher ist $\mathbb{Z}_p$ ein Körper.

$\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7$ sind Körper, $\mathbb{Z}_4, \mathbb{Z}_6, \mathbb{Z}_8$ sind keine Körper.

19.1.2001

(9.42) SATZ: Es sei p eine Primzahl. Dann gilt für alle $a \in \mathbb{Z}$

$$a^p \equiv a \pmod p$$

Bew: : Wir beweisen die Behauptung für $a \geq 0$ durch vollständige Induktion:

$a = 0$ klar

$a \longrightarrow a+1$ Nach der binomischen Formel (7.11) gilt

$$(a+1)^p = \binom{p}{0}a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \ldots + \binom{p}{p-1}a + \binom{p}{p}$$

Nach Aufg. 41 sind die Binomialkoeffizienten $\binom{p}{1}$ bis $\binom{p}{p-1}$ alle durch p teilbar, also kongruent 0 modulo p. Folglich

$$(a+1)^p \equiv \binom{p}{0}a^p + \binom{p}{p} \equiv a^p + 1 \overset{(IV)}{\equiv} a + 1 \pmod p$$