F6: $m \in \mathbb{N}$ gegeben.

(i) $\mathbb{Z}/m\mathbb{Z}$ ist auf nat. Weise ein komm. Ring mit Eins ($\neq$ Null, falls $m>1$)
Die Restklassenabb.

$$\begin{aligned} \mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \\ a &\longmapsto \bar{a} = a + m\mathbb{Z} =: a \bmod m \end{aligned}$$

ist ein *Ringhomomorphismus*. Für $m>1$ ist

$$\mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}_{(m)}/m\mathbb{Z}_{(m)} \text{ ein Ring}\textit{isomorphismus}$$

(Man darf identifizieren: $\mathbb{Z}_{(m)}/m\mathbb{Z}_{(m)} = \mathbb{Z}/m\mathbb{Z}$.)

(ii) $\mathbb{Z}/m\mathbb{Z}$ hat genau m Elemente.

(iii) Für bel. $c \in \mathbb{Z}$ ist $c, c+1, \dots, c+(m-1)$ ein Vertretersystem mod m.

$S \subseteq \mathbb{Z}$ heißt ein Vertretersystem mod m (bzw. von $\mathbb{Z}/m\mathbb{Z}$), wenn gilt:
Zu jedem $x \in \mathbb{Z}$ gibt es genau ein $a \in S$ mit $x \equiv a \bmod m$;
anders ausgedrückt: Die Einschränkung

$$(*) \quad S \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

der Restklassenabb. $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ auf S ist eine *Bijektion*. Äquiv. dazu:

$$|S| = m \text{ und } (*) \text{ injektiv oder surjektiv.}$$

(iv) $\mathbb{Z}/m\mathbb{Z}$ Integritätsring $\Leftrightarrow$ $\mathbb{Z}/m\mathbb{Z}$ Körper $\Leftrightarrow$ m Primzahl
Für Primzahl p heißt $\mathbb{Z}/p\mathbb{Z}$ *Restklassenkörper modulo p*.

(v) $(a,m) = d$, $x \equiv a \bmod m$ $\Longrightarrow$ $(x,m) = d$
"d ist ggT von $a + m\mathbb{Z}$ und m"

(vi) $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times \Longleftrightarrow (a,m) = 1$
(d.h. $\bar{a}$ Einheit in $\mathbb{Z}/m\mathbb{Z}$)
Die Elemente $\bar{a}$ von $(\mathbb{Z}/m\mathbb{Z})^\times$ heißen *prime Restklassen mod m*.

Beweis: (i) klar, vgl. F2(ii).
(ii) $0, 1, 2, \dots, m-1$ ist ein Vertretersystem von $\mathbb{Z}/m\mathbb{Z}$ (vgl. Def. 1)
(iii) $c+i \equiv c+j \bmod m \Longleftrightarrow i \equiv j \bmod m$

(v) folgt aus F2(vi).

Beh. Für bel. $\bar{a} = a \bmod m$ aus $\mathbb{Z}/m$ gilt:

$$\bar{a} \text{ kein Nullteiler in } \mathbb{Z}/m \iff (a,m) = 1.$$

"$\Rightarrow$": Wäre $(a,m) = d > 1$, so $a\left(\frac{m}{d}\right) = \frac{a}{d}\cdot m \equiv 0 \bmod m$ und $\frac{m}{d} \not\equiv 0 \bmod m$, also

$\bar{a}$ doch Nullteiler in $\mathbb{Z}/m$

"$\Leftarrow$": Gelte $\bar{a}\,\bar{b} = 0$ mit $\bar{b}$ bel. z.z. $\bar{b} = 0$. Aus $\overline{ab} = \bar{a}\,\bar{b} = 0$ folgt $m \mid ab$, $\xRightarrow{(a,m)=1} m \mid b \Rightarrow \bar{b} = 0.$

(vi) und (iv) folgen nun aus nachstehendem

<u>Lemma:</u> Sei R endlicher komm. Ring mit Eins. Dann

$$R^\times = \{a \in R \mid a \text{ kein Nullteiler von } R\}$$

(d.h. $\forall x \in R:\ ax = 0 \Rightarrow x = 0$)

Bew. $a \in R^\times \Rightarrow a$ kein Nullteiler.
Sei a kein Nullteiler. Dann ist die Abb. $\begin{matrix} R \to R \\ x \mapsto ax \end{matrix}$ injektiv, $\xRightarrow{R \text{ endlich}}$ auch surjektiv, $\Rightarrow \exists x \in R$ mit $ax = 1$, d.h. $a \in R^\times$.

<u>Anwendung:</u> p Primzahl. $(p-1)! = \prod_{k=1}^{p-1} k$. $F := \mathbb{Z}/p\mathbb{Z}$ Körper.

$$\prod_{\alpha \in F^\times} \alpha = \prod_{\substack{\alpha \in F^\times \\ \alpha \neq \alpha^{-1}}} \alpha \cdot \prod_{\substack{\alpha \in F^\times \\ \alpha = \alpha^{-1}}} \alpha = 1 \cdot (1 \cdot (-1)) = -1$$

$\lceil \alpha = \alpha^{-1} \iff \alpha^2 = 1 \overset{F \text{ Körper!}}{\iff} \alpha = 1$ oder $\alpha = -1$

<u>F7 (Satz von Wilson[*])</u> Für $n \in \mathbb{N}$, $n > 1$ gilt:

$$n \text{ Primzahl} \iff (n-1)! \equiv -1 \bmod n$$

Bew. $\Rightarrow$: obige Anwendung.
$\Leftarrow$: Sei $q < n$ ein Primteiler von n. $\Rightarrow \left.\begin{matrix} q \mid (n-1)! \\ q \mid n \end{matrix}\right\} \xRightarrow{(n-1)! \equiv -1 \bmod n}$ $q \mid -1$. W!

[*] $\Leftarrow$ von Lagrange
davor vermutlich schon Leibniz und Alhazen (965-1039) aus Basra

Sei p Primzahl $\neq 2$. Nach F3 war

$$(p-1)! \equiv 1^2 \cdot 2^2 \cdot 3^2 \cdot \ldots \cdot \left(\tfrac{p-1}{2}\right)^2 \cdot (-1)^{\frac{p-1}{2}} \bmod p .$$

Nach F7 wissen wir jetzt

$$(*) \qquad -1 \equiv 1^2 \cdot 2^2 \cdot 3^2 \cdot \ldots \cdot \left(\tfrac{p-1}{2}\right)^2 \cdot (-1)^{\frac{p-1}{2}} \bmod p$$

F8: Sei p Primzahl $\neq 2$. Dann ist die Kongruenz

$X^2 \equiv -1 \bmod p$ genau dann lösbar in $\mathbb{Z}$,

wenn $p \equiv 1 \bmod 4$ (d.h. p von der Gestalt $p = 4k+1$ mit $k \in \mathbb{N}$)

Bew. 1) Sei $p = 4k+1$. Dann nach (*)

$$-1 \equiv \left(\tfrac{p-1}{2}\right)!^2 \bmod p \quad ,$$

also ist die ganze Zahl $\left(\frac{p-1}{2}\right)!$ eine Lösung der Kongruenz $X^2 \equiv -1 \bmod p$.

2) Umgekehrt: Es gebe ein $c \in \mathbb{Z}$ mit $c^2 \equiv -1 \bmod p$. Es folgt

$$(c^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \bmod p, \text{ d.h. } \quad c^{p-1} \equiv (-1)^{\frac{p-1}{2}} \bmod p \quad ,$$

$$\xrightarrow[(p \nmid c)]{\text{Satz von Fermat}} \quad (-1)^{\frac{p-1}{2}} \equiv 1 \bmod p \; , \quad \xrightarrow{p \neq 2} \quad (-1)^{\frac{p-1}{2}} = 1$$

(denn $-1 \equiv 1 \bmod p$ unmöglich für $p \neq 2$)

$$\Longrightarrow \tfrac{p-1}{2} \text{ gerade} \Rightarrow 4 \mid p-1,$$

d.h. $p \equiv 1 \bmod 4$.

Bem'n: 1) F8 in anderer Formulierung. Setze $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ Körper!

$$\sqrt{-1} \in \mathbb{F}_p \iff p \equiv 1 \bmod 4 \quad \text{oder } p = 2$$

(d.h. die Gleichung $X^2 = -1$ lösbar in $\mathbb{F}_p$)

2) p Primzahl $\neq 2$. Dann $\quad \left(\frac{p-1}{2}\right)!^2 \equiv \begin{cases} -1 \bmod p & \text{für } p \equiv 1 \bmod 4 \\ +1 \bmod p & \text{für } p \equiv 3 \bmod 4 \end{cases}$

Für $p \equiv 3 \bmod 4$ gilt also $\left(\frac{p-1}{2}\right)! \equiv \pm 1 \bmod p$; wann $+1$ oder -1, ist eine spannende Frage, siehe §6. Die Sache ist ziemlich tiefliegend.[*)]

*) englische Ausgabe von F. Lorenz, Algebra I, S. 253.

Jetzt nochmal zum Ausgangspunkt von §3: Zunächst der

<u>Def.</u> Für jede natürliche Zahl m definiere

$$\varphi(m) := \#(\mathbb{Z}/m\mathbb{Z})^\times \qquad \ulcorner \varphi(1) = 1 \lrcorner$$

⌜Die Elementanzahl einer endlichen Menge M bez'n wir mit $\#M$ oder $|M|$ ⌟

Nach F6 gilt:

$$\varphi(m) = \#\{a \in \{0,1,2,\dots,m-1\} \mid a \text{ teilerfremd zu } m\}$$

Für eine Primzahl p ist daher

$$\varphi(p) = p-1.$$

φ heißt *Eulersche φ-Funktion.*

<u>Satz 1' (Euler-Fermat)</u>: Aus $(a,m)=1$ folgt

$$a^{\varphi(m)} \equiv 1 \bmod m$$

(Satz 1 ist Spezialfall von Satz 1': $m=p$, $\varphi(m)=p-1$)

<u>Bew.</u> $(\mathbb{Z}/m\mathbb{Z})^\times$ ist eine abelsche Gruppe der Ordnung $\varphi(m)$ (=Elementanzahl). Damit folgt Satz 1' aus nachstehendem

<u>Lemma:</u> Sei G eine abelsche Gruppe der Ordnung n. Dann gilt

$$x^n = 1 \text{ für alle } x \in G. \text{ [1]}$$

<u>Bew.</u> $x \in G$ gegeben. Da G abelsch, ist $z := \prod_{y\in G} y$ ein wohlbestimmtes Element von G. Nun ist

$$z = \prod_{y\in G} y \overset{*)}{=} \prod_{y\in G}(xy) = x^n\Big(\prod_{y\in G} y\Big) = x^n z, \text{ und es folgt}$$

$$x^n = 1.$$

*) denn $y \mapsto xy$ ist Bijektion in einer Gruppe.

---

[1] Dies gilt auch ohne die Voraussetzung abelsch, wie man in Algebra I lernt.

Simultane Kongruenzen

Satz 2: Ist $m = m_1 m_2 \dots m_r$ mit paarweise teilerfremden nat. Zahlen $m_1, \dots, m_r > 1$, so ist die Abbildung

(1) $$\mathbb{Z}/m \longrightarrow \mathbb{Z}/m_1 \times \mathbb{Z}/m_2 \times \dots \times \mathbb{Z}/m_r$$
$$a \bmod m \longmapsto (a \bmod m_1, a \bmod m_2, \dots, a \bmod m_r)$$

ein Isomorphismus von Ringen. Ist insbesondere

$$m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

die Primfaktorzerlegung einer nat. Zahl $m > 1$, so gilt

$$\mathbb{Z}/m \simeq \mathbb{Z}/p_1^{e_1} \times \dots \times \mathbb{Z}/p_r^{e_r} \quad \text{(mit kanonischem Isomorphie)}$$

Der Isomorphismus (1) vermittelt einen Isomorphismus

$$(\mathbb{Z}/m)^\times \xrightarrow{\sim} (\mathbb{Z}/m_1)^\times \times \dots \times (\mathbb{Z}/m_r)^\times$$

der primen Restklassengruppen; insb. gilt

$$\varphi(m) = \varphi(m_1) \cdot \varphi(m_2) \cdot \dots \cdot \varphi(m_r)$$

Bew. 1) Die Abb. (1) ist wohldefiniert [denn aus $a \equiv b \bmod m$ folgt $a \equiv b \bmod m_i$] und offenbar ein Ringhomomorphismus. Sie ist injektiv: Aus $a \equiv 0 \bmod m_i$ für alle $1 \le i \le r$ folgt $a \equiv 0 \bmod m_1 m_2 \dots m_r$ [denn $m_1, m_2, \dots, m_r$ paarw. teilerfremd], also $a \equiv 0 \bmod m$, d.h. $a \bmod m$ ist Null.

2) $\# \mathbb{Z}/m = m$, $\#(\mathbb{Z}/m_1 \times \dots \times \mathbb{Z}/m_r) = m_1 m_2 \dots m_r = m$. Also ist (1) auch surjektiv. Insgesamt ist (1) also ein Ringisomorphismus.

3) Ein Ringisom. $h: R \to S$ vermittelt offenbar einen Isomorphismus $h: R^\times \to S^\times$ der Einheitengruppen. Ferner gilt offenbar $(S_1 \times \dots \times S_r)^\times = S_1^\times \times S_2^\times \times \dots \times S_r^\times$ für Ringe S_i.

q.e.d.

<u>Satz 2'</u> (Lösung simultaner Kongruenzen, <u>Chinesischer Restsatz</u>)

Sei $m = m_1 m_2 \cdots m_r$ mit paarw. teilerfremden nat. Zahlen $m_1, \ldots, m_r > 1$. Sind dann $a_1, \ldots, a_r$ beliebige ganze Zahlen, so gibt es eine ganze Zahl x mit

$$(2) \quad \begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ &\vdots \\ x &\equiv a_r \bmod m_r \end{aligned}$$

Durch (2) ist x modulo m eindeutig bestimmt; ferner:

$$x \text{ prim zu } m \iff a_i \text{ prim zu } m_i \text{ für alle } i$$

Beweis: Klar nach Satz 2: Lösbarkeit : Surjektivität von (1)
Eindeutigkeit mod m : Injektivität von (1).

<u>2. Beweis (für Lösbarkeit):</u> Setze

$$q_i := \frac{m}{m_i} = m_1 m_2 \cdots \check{m}_i \cdots m_r$$

$ggT(q_1, \ldots, q_r) = 1$ (klar, oder folgt die Regel $(q_1, \ldots, q_r)\underbrace{[m_1, \ldots, m_r]}_{=m} = m$) S. 16

Es gibt daher $x_1, \ldots, x_r \in \mathbb{Z}$ mit

(3) $\quad x_1 q_1 + x_2 q_2 + \cdots + x_r q_r = 1, \quad \Rightarrow$

(3') $\quad x_1 q_1 + x_2 q_2 + \cdots + x_r q_r \equiv 1 \bmod m$

Setze $\quad e_i := x_i q_i \quad$ für $1 \le i \le r$. Dann

$$e_1 + e_2 + \cdots + e_r \equiv 1 \bmod m$$

und

$$e_i \equiv \begin{cases} 1 \bmod m_i \\ 0 \bmod m_j & \text{für } j \neq i \end{cases}$$

Dann erfüllt $x := a_1 e_1 + a_2 e_2 + \cdots + a_r e_r$ die Kongruenzen

$$x \equiv a_i \bmod m_i \quad \text{für } 1 \le i \le r$$

__Bem.__ Der 2. Beweis liefert Rechenverfahren zur Lösung von (2).

Es genügt, sich x_i zu verschaffen mit

(3') $\quad x_1 q_1 + x_2 q_2 + \ldots + x_r q_r \equiv 1 \bmod m \quad \left[q_i = \frac{m}{m_i} \right]$

Dann wird (2) wie gesagt erfüllt von

$$x = a_1(x_1 q_1) + \ldots + a_r(x_r q_r).$$

Für jedes $1 \le i \le r$ bestimme (notfalls mit Kettenbruchmethode) ein $x_i \in \mathbb{Z}$ mit

$$q_i x_i \equiv 1 \bmod m_i \qquad (\text{beachte: } (q_i, m_i) = 1\ )$$

Dann ist

$$x_1 q_1 + \ldots + x_r q_r \equiv 1 \bmod m_i \text{ für alle } 1 \le i \le r,$$

und es folgt (3').

__Bsp.__ Finde $x \in \mathbb{Z}$ mit

$$(*) \quad \begin{aligned} x &\equiv 1 \bmod 11 \\ x &\equiv 2 \bmod 12 \\ x &\equiv 3 \bmod 13 \end{aligned}$$

$m = 11 \cdot 12 \cdot 13 = 1716$

$q_1 = 12 \cdot 13 = 156$

$q_2 = 11 \cdot 13 = 143$

$q_3 = 11 \cdot 12 = 132$

$$\begin{aligned} 156 x_1 &\equiv 1 \bmod 11 \\ 2 x_1 &\equiv 1 \bmod 11 \\ x_1 &\equiv 6 \bmod 11 \end{aligned} \qquad \begin{aligned} 143 x_2 &\equiv 1 \bmod 12 \\ - x_2 &\equiv 1 \bmod 12 \\ x_2 &\equiv -1 \bmod 12 \end{aligned} \qquad \begin{aligned} 132 x_3 &\equiv 1 \bmod 13 \\ 2 x_3 &\equiv 1 \bmod 13 \\ x_3 &\equiv 7 \bmod 13 \end{aligned}$$

$e_1 = x_1 q_1 = 6 \cdot 156 = 936, \quad e_2 = x_2 q_2 = -143, \quad e_3 = x_3 q_3 = 7 \cdot 132 = 924$

$x = 1 \cdot 936 - 2 \cdot 143 + 3 \cdot 924 = 3422, \Rightarrow x \equiv -10 \bmod 1716$

Also ist -10 Lsg. von $(*)$. Hätten wir erraten können (in diesem Fall eigentlich müssen). Arbeit aber nicht umsonst, wenn wir entspr. System mit anderen a_i lösen wollen, z.B.