$$(*')\qquad \begin{aligned} x &\equiv 1 \mod 11 \\ x &\equiv 3 \mod 12 \\ x &\equiv 1 \mod 13 \end{aligned}$$

für $x = 1\cdot 936 - 3\cdot 143 + 1\cdot 924 = 1431$.

$x \equiv 1431 \mod 1716$ ist "die Lsg" von $(*')$.

⌈Lautet die Aufgabe "Bestimme alle $x \in \mathbb{Z}$, die $(*')$ erfüllen", so bemühe man sich um eine präzise Antwort, etwa: Genau die $x \in \mathbb{Z}$ mit $x \equiv 1431 \mod 1716$". Eine Antwort wie: "Alle $x \equiv 1431 \mod 1716$ erfüllen $(*')$" wäre nicht vollständig (sondern nur eine Teilantwort. Eine korrekte Antwort ist auch: Die Lösungsmenge L von $(*')$ ist die Menge $L = \{x \in \mathbb{Z} \mid x \equiv 1431 \mod 1716\}$. Oder auch: Die Lösungsmenge L von $(*')$ ist die Restklasse $1431 \mod 1716$.⌋

<u>Bem.</u> Rechenfehler sind vielleicht verzeihlich, aber nicht, die Probe zu unterlassen!

<u>Bem.</u> Man kann das System (2) schrittweise lösen, indem man jeweils nur Systeme von 2 Kongruenzen löst.

Für das System $(*')$ findet man mit "Probieren" zunächst

$$\begin{aligned} x &\equiv 1 \mod 11 \\ x &\equiv 3 \mod 12 \end{aligned} \iff x \equiv 111 \mod 132 \qquad [132 = 11\cdot 12]$$

Damit

$$(*') \iff \begin{aligned} x &\equiv 111 \mod 132 \\ x &\equiv 1 \mod 13 \end{aligned} \iff \begin{aligned} x &\equiv -21 \mod 132 \\ x &\equiv 1 \mod 13 \end{aligned} \iff$$

$$\begin{aligned} x &\equiv -285 \mod 132 \\ x &\equiv -285 \mod 13 \end{aligned} \iff x \equiv -285 \mod \overbrace{132\cdot 13}^{1716}$$

$(\iff x \equiv 1431 \mod 1716)$.

Korollar: Sei $f \in \mathbb{Z}[X]$ Polynom (mit ganzen Koeffizienten), $m = m_1 m_2 \dots m_r$ mit paarw. teilerfremden $m_i > 1$. Dann:

$$f(X) \equiv 0 \bmod m \underset{(\text{in } \mathbb{Z})}{\text{lösbar}} \iff f(X) \equiv 0 \bmod m_i \underset{(\text{in } \mathbb{Z})}{\text{lösbar}} \text{ für } \underline{\text{jedes}}\ 1 \le i \le r$$

Die natürliche Abb. $\mathbb{Z}/m \longrightarrow \prod_{i=1}^{r} \mathbb{Z}/m_i$ vermittelt eine Bijektion

(*) $$\{\alpha \in \mathbb{Z}/m \mid f(\alpha) = 0\} \longrightarrow \prod_{i=1}^{r} \{\alpha_i \in \mathbb{Z}/m_i \mid f(\alpha_i) = 0\}$$

Für die Lösungsanzahlen (für bel. $n \in \mathbb{N}$ setze $N_f(n) = \#\{\alpha \in \mathbb{Z}/n \mid f(\alpha) = 0\}$) gilt also

$$N_f(m_1 m_2 \dots m_r) = N_f(m_1) N_f(m_2) \dots N_f(m_r)$$

Bew. Für $x \in \mathbb{Z}$ gilt

$$f(x) \equiv 0 \bmod m \implies f(x) \equiv 0 \bmod m_i \text{ für alle } 1 \le i \le r$$

Die Abbildung (*) ist injektiv (nach Satz 2).
Ist sie auch surjektiv? Seien $a_1, \dots, a_r \in \mathbb{Z}$ gegeben mit

$$f(a_i) \equiv 0 \bmod m_i \text{ für } 1 \le i \le r.$$

Nach Satz 2' existiert ein $x \in \mathbb{Z}$ mit $x \equiv a_i \bmod m_i$ für $1 \le i \le r$.

$$\implies f(x) \equiv f(a_i) \bmod m_i \text{ für alle } i, \implies$$

$$f(x) \equiv 0 \bmod m_i \text{ für alle } i, \implies f(x) \equiv 0 \bmod m.$$

Also insgesamt

$$f(x) \equiv 0 \bmod m, \quad x \equiv a_i \bmod m_i \text{ für alle } 1 \le i \le r.$$

Somit ist (*) auch surjektiv!

§4 Die prime Restklassengruppe mod m

$m \in \mathbb{N},\ m > 1$

$\mathbb{Z}/m\mathbb{Z}$ Restklassenring mod m. $\quad \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$

$\qquad a \mapsto \bar{a} := a \bmod m$,

Def. $(\mathbb{Z}/m\mathbb{Z})^\times$ heißt die prime Restklassengruppe mod m. Wir wissen:

(1) $\quad \bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times \Longleftrightarrow (a,m) = 1$

(2) $\quad M := \{ k \in \mathbb{Z} \mid 0 \le k < m,\ (k,m) = 1 \}$ ist ein Vertretersystem von $(\mathbb{Z}/m\mathbb{Z})^\times$

$(\mathbb{Z}/m\mathbb{Z})^\times$ hat $\varphi(m) = \# M$ Elemente

$(\mathbb{Z}/m\mathbb{Z}^\times)$ ist eine abelsche Gruppe der Ordnung $\varphi(m)$

(3) $\quad \alpha \in (\mathbb{Z}/m\mathbb{Z})^\times \Longrightarrow \alpha^{\varphi(m)} = 1 \quad$ (Satz von Euler-Fermat)

$\alpha = \bar{a}$

$$\Updownarrow$$

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

Def. Ein $\omega \in (\mathbb{Z}/m\mathbb{Z})^\times$ heißt eine Primitivwurzel von $(\mathbb{Z}/m\mathbb{Z})^\times$, wenn sich jedes Element $\alpha \in (\mathbb{Z}/m\mathbb{Z})^\times$ in der Form

$$\alpha = \omega^i \quad \text{mit einem } i = 0, 1, 2, \ldots$$

schreiben läßt; jedes $g \in \mathbb{Z}$ mit $\omega = \bar{g} = g \bmod m$ heißt dann eine Primitivwurzel mod m.

$\boxed{!}$ $(\mathbb{Z}/m\mathbb{Z})^\times$ braucht keine Primitivwurzel zu besitzen.

Beispiele: 1) $m = 7$. $\quad 2^0 = 1,\ 2^1 = 2,\ 2^2 = 4,\ 2^3 \equiv 1 \bmod 7,\ 2^4 \equiv 2 \bmod 7, \ldots$

also ist 2 keine Primitivwurzel mod 7

$3^0 = 1,\ 3^1 = 3,\ 3^2 \equiv 2 \bmod 7,\ 3^3 \equiv 6 \bmod 7,\ 3^4 \equiv 4 \bmod 7, 3^5 \equiv 5 \bmod 7,$

also ist 3 eine Primitivwurzel mod 7.

2) $m = 8$. Vertretersystem: $1, 3, 5, 7$ bzw. $1, 3, -3, -1$

$3^2 \equiv 1 \bmod 8$
$5^2 \equiv 1 \bmod 8$
$7^2 \equiv 1 \bmod 8$

also: $(\mathbb{Z}/8\mathbb{Z})^\times$ besitzt überhaupt keine Primitivwurzel!

Satz 1 (Gauß): Ist p eine Primzahl, so besitzt $(\mathbb{Z}/p\mathbb{Z})^\times$ eine Primitivwurzel. Es gibt also ein $\omega \in (\mathbb{Z}/p\mathbb{Z})^\times$, so daß sich jedes $\alpha \in (\mathbb{Z}/p\mathbb{Z})^\times$ darstellen läßt in der Form

(*) $$\alpha = \omega^i \text{ mit } 0 \leq i < p-1$$

Die Darstellung (*) ist [unter der Bedingung $0 \leq i < p-1$] eindeutig; $i = i(\alpha) = i_\omega(\alpha)$ heißt der Index von α (bzgl. ω).

Wählt man ein $g \in \mathbb{Z}$ mit $\omega = g \bmod m$, so gilt also: Zu jedem $a \in \mathbb{Z}$ mit $p \nmid a$ gibt es genau ein $i \in \mathbb{Z}$ mit

$$a \equiv g^i \bmod p, \quad 0 \leq i < p-1.$$

$i = i(a) = i_g(a)$ heißt der Index von a (bzgl. g).

Zusatz: Es gibt genau $\varphi(p-1)$ verschiedene Primitivwurzeln von $(\mathbb{Z}/p\mathbb{Z})^\times$.

Der Satz 1 ist alles andere als trivial (und eigentlich der erste Satz der Vorlesung, mit dem wir über die Schulmathematik wesentlich hinausgehen.)

Wir führen den Beweis erst nach einigen gruppentheoretischen Vorbereitungen:

Gruppentheoretische Vorbereitungen:

Def. Sei G eine (abelsche) Gruppe der Ordnung n. ⌜$\#G = n$⌟

⌜cf. Lemma, S. 63⌟ Sei $\alpha \in G$. Wir wissen: $\alpha^n = 1$. Unter allen $m \in \mathbb{N}$ mit $\alpha^m = 1$ sei nun k das kleinste. Setze dann

$$\mathrm{ord}(\alpha) := k \qquad \underline{\text{Ordnung von } \alpha}$$

$\langle\alpha\rangle := \{\alpha^j \mid j \in \mathbb{Z}\}$, ist offenbar eine Untergruppe von G.

Lemma 1: In der Situation der Def. gelten:

① $\quad \langle\alpha\rangle = \{1, \alpha, \alpha^2, \dots, \alpha^{k-1}\}$, insb.

$$\boxed{\mathrm{ord}(\langle\alpha\rangle) = \mathrm{ord}(\alpha)}$$

Denn: $\alpha^k = 1$, $\alpha^{k+1} = \alpha$, $\alpha^{k+2} = \alpha^2, \dots$

$\alpha^{-1} = \alpha^{k-1}$, also $\langle\alpha\rangle = \{1, \alpha, \alpha^2, \dots, \alpha^{k-1}\}$

$\alpha^j = \alpha^{j'}$, $0 \le j \le j' \le k-1 \Rightarrow \alpha^{j'-j} = 1 \xRightarrow{0 \le j'-j < k} j'-j = 0$, d.h. $j' = j$;

also $1, \alpha, \alpha^2, \dots, \alpha^{k-1}$ paarw. verschieden!

② $\alpha^m = 1$ für $m \in \mathbb{Z} \Rightarrow \underset{k}{\underset{\parallel}{\mathrm{ord}(\alpha)}} \mid m$

Denn: $m = qk + r$ mit $0 \le r < k$, also

$$1 = \alpha^m = \alpha^{qk+r} = \alpha^{qk}\alpha^r = \alpha^r, \quad \xRightarrow{\text{Def. von } k} r = 0$$

③ Sei $\mathrm{ord}(\alpha) = k$ wie oben. Dann vermittelt der (Gruppen-)Homomorphismus

$$\mathbb{Z} \to \langle\alpha\rangle, \text{ def. durch } 1 \mapsto \alpha \ (\text{also } j \mapsto \alpha^j)$$

einen Gruppenisomorphismus

$$(*) \quad \mathbb{Z}/k\mathbb{Z} \to \langle\alpha\rangle,$$

⌜$\mathbb{Z}/k\mathbb{Z}$ "additive Gruppe", $\langle\alpha\rangle$ "multiplikative Gruppe"⌟

also

$$\langle\alpha\rangle \simeq \mathbb{Z}/k\mathbb{Z}$$

Def. Sei G eine endliche Gruppe. G heißt zyklisch, wenn es ein $\alpha \in G$ gibt mit $G = \langle \alpha \rangle$; letzteres ist nach ① äquivalent mit $ord(\alpha) = \# G = ord(G)$. Insbesondere hat man

④ G zyklisch $\Longleftrightarrow$ $\exists \alpha \in G$ mit $ord(\alpha) = ord(G)$

Bem. Definitionsgemäß gilt:

$(\mathbb{Z}/m\mathbb{Z})^\times$ besitzt Primitivwurzel $\Leftrightarrow$ $(\mathbb{Z}/m\mathbb{Z})^\times$ ist zyklisch

Und nach dem zuvor Gesagtem:

ω ist Primitivwurzel von $(\mathbb{Z}/m\mathbb{Z})^\times \Longleftrightarrow ord(\omega) = \varphi(m)$

$(\mathbb{Z}/8\mathbb{Z})^\times$ ist nicht zyklisch (denn für alle $\alpha \neq 1$ in $(\mathbb{Z}/8\mathbb{Z})^\times$ gilt $ord(\alpha) = 2$.)

Zum Beweis von Satz 1 ist also folgende Frage positiv zu beantworten:
Gibt es ein $\alpha \in (\mathbb{Z}/p\mathbb{Z})^\times$ mit $ord(\alpha) = p-1$?

Def. Sei G endliche Gruppe. Das kgV aller $ord(\alpha), \alpha \in G$ heißt der Exponent

$$e = e(G)$$

der Gruppe G.

Bem. Ist $n = ord(G)$, $e = e(G)$, so gilt stets

$$e \mid n$$

Denn für jedes $\alpha \in G$ gilt $\alpha^n = 1$, $\overset{②}{\Longrightarrow} ord(\alpha) \mid n \overset{\text{Def. von } e}{\Longrightarrow} e \mid n$.

F1: Sei G eine endliche abelsche Gruppe, und sei e ihr Exponent. Dann gibt es ein Element ω in G mit

$$ord(\omega) = e$$

Beweis: siehe w.u.

<u>Satz 1':</u> Sei K ein Körper und G eine <u>endliche</u> Untergruppe von $K^\times$. Dann ist G <u>zyklisch</u>.

(Daraus folgt Satz 1: Nehme $K = \mathbb{Z}/p\mathbb{Z}$, dann $K^\times = (\mathbb{Z}/p\mathbb{Z})^\times$ endlich)

<u>Bew.</u> Sei $e = e(G)$. Für jedes $\alpha \in G$ gilt nach Def. von e

$$\mathrm{ord}(\alpha) \mid e$$

Es gilt also

$$(*) \qquad \alpha^e = 1 \quad \text{für alle } \alpha \in G$$

Wir befinden uns in einem Körper K. Alle $\alpha \in G$ sind nach $(*)$ Nullstellen des Polynoms

$$(**) \qquad X^e - 1 \quad \in K[X]$$

Nun gibt es nach F1 aber ein $\omega \in G$ mit $\mathrm{ord}(\omega) = e$. Dann sind

$$(***) \qquad 1, \omega, \omega^2, \dots, \omega^{e-1}$$

e verschiedene Nullstellen von $(**)$. Aber $X^e - 1$ hat in K höchstens e Nullstellen (K Körper!). Jedes $\alpha \in G$ ist Nullstelle von $(**)$. Also ist jedes $\alpha \in G$ eines der Elemente in $(***)$, d.h. $\alpha = \omega^j$ für ein j. Somit ist $G = \langle \omega \rangle$, d.h. G ist zyklisch!