Restklassen $\mathbb{Z}_m$

Def.: Seien $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$.
$a \equiv b \pmod m$, falls $m \mid (a-b)$
„a kongruent b modulo m"

Def.: Die Äquivalenzklassen, der durch die Kongruenz modulo m definierten Äquivalenzrelation ($m \in \mathbb{N}$) auf $\mathbb{Z}$, nennt man <u>Restklassen modulo m</u>.

Def.: Eine Menge $\{x_1, x_2, \ldots, x_m\}$ von m ganzen Zahlen heißt ein vollständiges Restsystem modulo m, falls die Zahlen paarweise nicht kongruent modulo m sind, also $x_i \not\equiv x_j \pmod m$ für $i \neq j$.

Bspe: a) $\{0, 1, 2, 3, 4, 5, 6\}$ ist für $m = 7$ das kleinste nicht negative Restsystem modulo 7.

b) $\{0, 1, 2, \ldots, m-1\}$ ist für $m \in \mathbb{N}$ das kleinste nicht negative Restsystem modulo m.

Def.: Seien $\bar{x}, \bar{y} \in \mathbb{Z}_m$. Dann def. man durch

$\bar{x} \oplus \bar{y} := \overline{x+y}$ eine <u>Addition</u> und

$\bar{x} \odot \bar{y} := \overline{x \cdot y}$ eine <u>Multiplikation</u>

in der Menge der Restklassen modulo m.

Satz: Die Restklassen modulo m bilden bezüglich der Addition eine abelsche Gruppe, also: $(\mathbb{Z}_m, \oplus)$ ist abelsche Gruppe.

In $(\mathbb{Z}_m, \odot)$ gelten Assoziativ- und Kommutativgesetz und es gibt das neutrale Element $\bar{1} \in \mathbb{Z}_m$.

Satz: $(\mathbb{Z}_m, \oplus, \odot)$ ist ein kommutativer Ring $(m \in \mathbb{N})$ mit Einselement.

Frage: Gibt es Ringe $(\mathbb{Z}_m, \oplus, \odot)$, in denen es zu jedem Element ein multiplikatives Inverses gibt (außer für das Element $\bar{0}$)?

Antwort: Ja, falls m eine Primzahl ist.

Satz: Sei m Primzahl. Dann ist $(\mathbb{Z}_m \setminus \{\bar{0}\}, \odot)$ eine Gruppe. $[\mathbb{Z}_m^* := \mathbb{Z}_m \setminus \{\bar{0}\}]$

genauer: endl. abelsche Gruppe [prime Restkl.gruppe mod m]

Satz: $(\mathbb{Z}_m, \oplus, \odot)$ ist genau dann ein Körper, wenn m eine Primzahl ist.

Ein Blick zur Zahlentheorie

Bereits um 500 v. Chr. war chinesischen Mathematikern bekannt, dass für jede Primzahl p die Kongruenz

$$2^p \equiv 2 \pmod{p}$$

gilt, also $p \mid 2^p - 2$.

1640 formulierte Pierre de Fermat eine Verallgemeinerung auf bel. ganze Zahlen, die als „kleiner Satz von Fermat" bekannt wurde. Nicht zu verwechseln mit dem „großen Satz von Fermat", der auch als „Fermats letzter Satz" bekannt wurde. Dieser besagt, dass die diophantische Gleichung

$$x^n + y^n = z^n \quad \text{für } n > 2$$

nur triviale Lösungen besitzt.

[Bereits nach mehr als 350 Jahren durch Andrew Wiles!]

Satz: „Kleiner Satz von Fermat"

Sei p Primzahl, $a \in \mathbb{Z}$ und $ggT(a,p)=1$.

Dann ist $$a^{p-1} \equiv 1 \pmod{p}$$

Anm.: Ein Beweis wurde erstmals von Euler im 18. Jahrhundert (1736) publiziert.

Bew.-Skizze:

Betrachte die $p-1$ ganzen Zahlen

$$a, 2a, 3a, \dots, (p-1)\cdot a.$$

$p \nmid ia$ für $i = 1, \dots, (p-1)$, da $ggT(a,p)=1$ und $ggT(i,p)=1$ für alle $i=1,\dots,p-1$

Keine zwei Zahlen aus $a, 2a, \dots, (p-1)a$ sind kongruent mod p. [Ann: Es ex. $i,j \in \{1,\dots,p-1\}$, $i \neq j$, mit $ai \equiv aj \pmod{p}$. Dann gilt

$ai - aj = a\cdot(i-j) \equiv 0 \pmod{p}$ und

da $ggT(a,p)=1$ gilt, erhält man $p \mid (i-j)$.

Somit gilt $i \equiv j \pmod{p}$, was jedoch nicht möglich ist, da i und j unterschiedliche Elte. des primen Restsystems $1,\dots,(p-1)$ sind.]

Die Zahlen $a, 2a, 3a, \dots, (p-1)a$ bilden somit Restsystem modulo p, das $p-1$ Reste enthält, die alle modulo p verschieden sind und zu denen 0 nicht gehört.

Dies gilt auch für $1, 2, \dots, (p-1)$, also folgt für die Produkte

$$a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \pmod{p}$$

Man erhält

$$a^{p-1} \underbrace{(1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1))}_{(p-1)!} \equiv \underbrace{1 \cdot 2 \cdot \dots \cdot (p-1)}_{(p-1)!} \pmod{p}$$

Da p und $(p-1)!$ teilerfremd sind, folgt:

$$a^{p-1} \equiv 1 \pmod{p}$$

□

(s. S. 217) *

Folgende Folgerung findet man in der Literatur auch manchmal als „kleinen Satz von Fermat“:

Satz:
Sei p Primzahl und $a \in \mathbb{Z}$. Dann ist

$$a^p \equiv a \pmod{p}$$

Beweis-Andeutung: 1. Fall: $\operatorname{ggT}(a,p) = 1$. Die Beh. folgt aus dem kl. Satz v. Fermat. 2. Fall $\operatorname{ggT}(a,p) \neq 1$. $\overset{p \text{ prim}}{\Rightarrow} p \mid a \Rightarrow p \mid a^p \Rightarrow a^p \equiv a \equiv 0 \pmod{p}$

(*) Etwas ausführlichere Argumentation:

$$a^{p-1}\,(p-1)! - (p-1)! \equiv 0 \pmod{p}$$

$$(a^{p-1} - 1)\cdot(p-1)! \equiv 0 \pmod{p}$$

$$p \mid (a^{p-1} - 1) \iff a^{p-1} - 1 \equiv 0 \pmod{p}$$

$$\iff a^{p-1} \equiv 1 \pmod{p}$$

Beweis-Alternative mit vollständiger Induktion

Sei p Primzahl, $a \in \mathbb{Z}$. Dann gilt

$$(*) \quad a^p \equiv a \pmod{p}$$

Bew.-Skizze:

Ind.-Anf. zz. die Beh. (*) gilt für $a = 1$.

$1^p = 1 \equiv 1 \pmod{p}$.

Ind.-Vor. Die Beh. gilt für ein $a_0 \in \mathbb{N}$, also $a_0^p \equiv a_0 \pmod{p}$.

Ind.-Schritt: zz. die Beh. gilt für $a_0 + 1$.

[zz. $(a_0+1)^p \equiv a_0 + 1 \pmod{p}$]

$$(a_0+1)^p - (a_0+1) = \underbrace{a_0^p + \binom{p}{1} a_0^{p-1} + \binom{p}{2} a_0^{p-2} + \ldots + \binom{p}{p-1} a_0 + 1}_{(a_0+1)^p} - (a_0+1)$$

Binomischer Lehrsatz

$$p \mid \binom{p}{i} \text{ mit } i = 1, \ldots, p-1 \Rightarrow \binom{p}{i} a^{p-i} \equiv 0 \pmod{p}$$

$$\Rightarrow a_0^p + 1 - (a_0+1) = a_0^p - a_0 \overset{\text{Ind.Vor.}}{\equiv} 0 \pmod{p}$$

$$\Rightarrow (a_0+1)^p \equiv a_0 + 1 \pmod{p}$$

Die Beh. gilt für alle $a \in \mathbb{N}$.

Die Beh. (*) ist für alle $a \in \mathbb{N}$ bewiesen.

Nun folgt der Beweis für $a \in \mathbb{Z} \setminus \mathbb{N}$.

1) Für $a = 0$ ist die Beh. sofort klar, denn

$$0^p - 0 = 0 \text{ ist durch } p \text{ teilbar.}$$

2) Mit $a > 0$ gilt

$$(-a)^2 - (-a) = a^2 + a = \underbrace{\underbrace{a^2 - a}_{2 \mid a^2 - a} + \underbrace{2a}_{2 \mid 2a}}_{2 \mid (a^2 - a + 2a)}$$

Die Beh. gilt also für $p = 2$.
auch für negative Zahlen.

Für eine ungerade Primzahl p rechnet man

$$(-a)^p - (-a) = -a^p + a = -(a^p - a)$$

$$p \mid a^p - a \implies p \mid -(a^p - a)$$

$$\Rightarrow p \mid (-a)^p - (-a)$$

$\Rightarrow$ Beh. gilt für alle $a \in \mathbb{Z}$ und $p \in \mathbb{P}$.

□