F26T1A4

Idempotent in einem Ring R = Element $a \in R$ mit $a^2 = a$

(a) Sei p Primzahl und $k \in \mathbb{N}$. Zeigen Sie, dass es im Ring $\mathbb{Z}/p^k\mathbb{Z}$ genau zwei Idempotente gibt.

Sei $\bar{a} = a + p\mathbb{Z} \in \mathbb{Z}/p^k\mathbb{Z}$ mit $\bar{a}^2 = \bar{a}$, wobei $a \in \mathbb{Z}$ ist.

1. Fall: $p \nmid a$ Dann gilt $ggT(a, p^k)$

$= 1$, und somit $\bar{a} \in (\mathbb{Z}/p^k\mathbb{Z})^\times$. $\bar{a}^2 = \bar{a}$

$\rightarrow \bar{a}^{-1} \cdot \bar{a}^2 = \bar{a}^{-1} \cdot \bar{a} \Rightarrow \bar{a} = \bar{1}$

2. Fall: $p \mid a$ Dann gibt es ein $b \in \mathbb{Z}$ und ein $l \in \mathbb{N}$ mit $a = p^l b$ und $p \nmid b$.

$\bar{a}^2 = \bar{a} \Rightarrow (\bar{p}^l \bar{b})^2 = \bar{p}^l \bar{b} \rightarrow$

$\bar{p}^{2l} \bar{b}^2 = \bar{p}^l \bar{b} \Rightarrow p^{2l} b^2 \equiv p^l b \bmod p^k$

$\Rightarrow p^k \mid (p^{2l} b^2 - p^l b)$

Allgemein gilt:

Sind $a, b, c \in \mathbb{Z}$ mit $a \mid bc$, wobei

a und b teilerfremd sind, dann gilt a|c.

hier: • Die Zahlen p^k und b sind teilerfremd wegen $p \nmid b$

• Außerdem gilt $p \nmid (p^l b - 1)$, somit sind auch p^k und $p^l b - 1$ teilerfremd

$\Rightarrow$ p^k und $b(p^l b - 1)$ sind teilerfremd

$\Rightarrow$ $p^k \mid p^l \Rightarrow l \geq k \Rightarrow \bar{a} = p^l b + p^k \mathbb{Z} = \bar{0}$

$\uparrow$ $p^k \mid (p^l b)$

Also gibt es in $\mathbb{Z}/p^k\mathbb{Z}$ keine Idempotenten $\neq \bar{0}, \bar{1}$.

Diese beiden Elemente sind offenbar idempotent, da $\bar{0}^2 = \bar{0}$ und $\bar{1}^2 = \bar{1}$. Also sind $\bar{0}, \bar{1}$ die einzigen beiden Idempotenten in $\mathbb{Z}/p^k\mathbb{Z}$ (und $\bar{0} \neq \bar{1}$ wegen $k \geq 1$).

Sei nun $N = 2^2 \cdot 5 \cdot 37$.

(b) Bestimmen Sie die Anzahl der Idempotenten im Ring $\mathbb{Z}/N\mathbb{Z}$.

Da die Zahlen 2^2, 5 und 37 paarweise teilerfremd sind, existiert nach dem Chin. Restsatz ein Isom.

$\phi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/37\mathbb{Z}$ von Ringen

mit $\phi(a+N\mathbb{Z}) = (a+4\mathbb{Z}, a+5\mathbb{Z}, a+37\mathbb{Z})$ $\forall a \in \mathbb{Z}$.

Es sei $E \subseteq \mathbb{Z}/N\mathbb{Z}$ die Menge der Idempotenten in $\mathbb{Z}/N\mathbb{Z}$ und E_k die Menge der Idempotenten in $\mathbb{Z}/k\mathbb{Z}$ für $k \in \{4, 5, 37\}$.

Beh. (1) Seien $a, b, c, d \in \mathbb{Z}$ mit $\phi(\bar{a}) = (\bar{b}, \bar{c}, \bar{d})$, wobei $\bar{a}$ das Bild von a in $\mathbb{Z}/N\mathbb{Z}$ bezeichnet, entsprechend für b, c, d. Dann gilt

$\bar{a} \in E \iff (b, c, d) \in E_4 \times E_5 \times E_{37}$.

(2) $\phi|_E$ ist eine Bijektion zwischen E und $E_4 \times E_5 \times E_{37}$

zu (1) $\bar{a} \in E \iff \bar{a}^2 = \bar{a} \overset{\phi \text{ bij}}{\iff} \phi(\bar{a}^2) = \phi(\bar{a})$

ϕ Ringhom. $\iff \phi(\bar{a})^2 = \phi(\bar{a}) \iff (\bar{b}, \bar{c}, \bar{d})^2 =$

$(\bar{b}, \bar{c}, \bar{d}) \iff (\bar{b}^2, \bar{c}^2, \bar{d}^2) = (\bar{b}, \bar{c}, \bar{d}) \iff$

$\bar{b}^2 = b \wedge \bar{c}^2 = \bar{c} \wedge \bar{d}^2 = \bar{d} \Leftrightarrow \bar{b} \in E_4 \wedge$

$\bar{c} \in E_5 \wedge \bar{d} \in E_{37} \Leftrightarrow (\bar{b}, \bar{c}, \bar{d}) \in E_4 \times E_5 \times E_{37}$

zu (2) Nach Teil (1) gilt für alle $\bar{a} \in \mathbb{Z}/N\mathbb{Z}$:
jeweils $\bar{a} \in E \Rightarrow \phi(\bar{a}) \in E_4 \times E_5 \times E_{37}$. Also
ist $\phi_{|E}$ eine Abb. $E \to E_4 \times E_5 \times E_{37}$.

noch zzg.: (2.1) $\phi_{|E}$ ist injektiv
(2.2) $\phi_{|E}$ ist surjektiv

zu (2.1) folgt aus der Injektivität von ϕ

zu (2.2) Sei $(\bar{b}, \bar{c}, \bar{d}) \in E_4 \times E_5 \times E_{37}$.
ϕ surjektiv $\Rightarrow \exists\, \bar{a} \in \mathbb{Z}/N\mathbb{Z}: \phi(\bar{a}) = (\bar{b}, \bar{c}, \bar{d})$
Aus $(\bar{b}, \bar{c}, \bar{d}) \in E_4 \times E_5 \times E_{37}$ und (1) folgt
$\bar{a} \in E \Rightarrow (\phi_{|E})(\bar{a}) = (\bar{b}, \bar{c}, \bar{d})$ ($\Rightarrow$ Beh.)

Da 4, 5, 37 Primzahlpotenzen > 1 sind, folgt aus Teil (a) $|E_4| = |E_5| = |E_{37}| = 2$.

Aus der Bijektivität von Φ_{IE} folgt somit

$$|E| = |E_4 \times E_5 \times E_{37}| = |E_4| \cdot |E_5| \cdot |E_{37}|$$
$$= 2 \cdot 2 \cdot 2 = 8.$$

(c) Bestimmen Sie ein $e \in \mathbb{Z}$, so dass $\bar{e} = e + N\mathbb{Z}$ ein Idempotentes in $\mathbb{Z}/N\mathbb{Z}$ ist und $e \equiv 0 \bmod 20$, $e \equiv 1 \bmod 37$ ist.

Anwendung des Euklidischen Algorithmus auf die Zahlen 37 und 20:

Bild

echend

E_{37}.

hon E

$(\bar{a}^2) = \phi(\bar{a})$

$d)^2 =$

$) \Leftrightarrow$

q	a_n	x_n	y_n
–	37	1	0
–	20	0	1
1	17	1	−1
1	3	−1	2
5	2	6	−11
1	1	−7	13

$\Longrightarrow ggT(37,20) = 1 = (-7)\cdot 37 + 13\cdot 20$

$\Rightarrow 1 + 7\cdot 37 = 13\cdot 20 = 260$

Sei $e = 260$. noch zu zeigen: $\bar{e} = e + N\mathbb{Z}$

ist Idempotentes.

Es gilt $e \equiv 1 \bmod 37$, und aus $e \equiv 0 \bmod 20$ folgt $e \equiv 0 \bmod 4$ und $e \equiv 0 \bmod 5$ (wegen $4 \mid 120$ und $5 \mid 120$). Die Abbildung ϕ aus Teil (b) hat somit den Wert $\phi(\bar{e}) = (0+4\mathbb{Z}, 0+5\mathbb{Z}, 1+37\mathbb{Z})$, und alle drei Elemente sind in ihrem jeweiligen Ring Idempotente (siehe Teil (a)). Aus der Beh. in Teil (b) folgt, dass $\bar{e}$ ein Idempotentes in $\mathbb{Z}/N\mathbb{Z}$ ist. $\square$

F25T2A2 (Übung: H13T3A5)

(a) Sei p eine Primzahl und q ein Primteiler von $2^p - 1$. Zeigen Sie, dass $q \equiv 1 \bmod p$ gilt.

Hinweis: Betrachten Sie die Ordnung von $\bar{2}$ in $(\mathbb{Z}/q\mathbb{Z})^\times$.

$q \mid (2^p - 1) \Rightarrow 2^p \equiv 1 \bmod q \Rightarrow \bar{2}^p = \bar{1}$ im Ring $\mathbb{Z}/q\mathbb{Z} \Rightarrow \bar{2} \in (\mathbb{Z}/q\mathbb{Z})^\times$ und $\operatorname{ord}(\bar{2})$ ist Teiler von $p \xrightarrow{p \text{ Primzahl}}$

$\operatorname{ord}(\bar{2}) \in \{1, p\}$ Ang. $\operatorname{ord}(\bar{2}) = \bar{1}$.

$\Rightarrow \bar{2} = \bar{1}$ in $(\mathbb{Z}/q\mathbb{Z})^*$ $\rightarrow$ $2 \equiv 1 \bmod q$ $\Rightarrow$

$q \mid (2-1) \Rightarrow q = 1$ $\lightning$ da q Primzahl

also: $\mathrm{ord}(\bar{2}) = p$ in $(\mathbb{Z}/q\mathbb{Z})^*$.

Da q eine Primzahl ist, gilt $|(\mathbb{Z}/q\mathbb{Z})^*| = q-1$.

Nach dem Satz von Lagrange muss $\mathrm{ord}(\bar{2})$ ein Teiler dieser Zahl sein. $\Rightarrow$ $p \mid (q-1)$ $\Rightarrow$ $q \equiv 1 \bmod p$.

$\square$

20

F20T3A2 Bestimmen Sie die letzten beiden Ziffern von $2018^{(2019^{2020})}$. Gehen Sie dabei folgendermaßen vor.

(a) Bestimmen Sie die Restklasse der Zahl in $\mathbb{Z}/25\mathbb{Z}$.

(b) Bestimmen Sie die Restklasse in $\mathbb{Z}/4\mathbb{Z}$.

(Übung: H20T1A1, H20T2A1(a), F22T1A2)

zu(a) Wegen $5 \nmid 2018$ gilt $\operatorname{ggT}(2018, 25) = 1$.

$\Rightarrow \overline{2018} = \overline{18} = -\overline{7}$ ist ein Einheit in $\mathbb{Z}/25\mathbb{Z}$

Wegen $|(\mathbb{Z}/25\mathbb{Z})^\times| = \varphi(25) = 20$ muss die Ord-

nung ein Teiler von 20 sein.

$\overline{18}^2 = (\overline{-7})^2 = \overline{49} = -\overline{1} + \overline{1}$

$\overline{18}^4 = (\overline{18}^2)^2 = (-\overline{1})^2 = \overline{1}$

$\Rightarrow$ ord $(\overline{18}) = 4$ in $(\mathbb{Z}/25\mathbb{Z})^\times$.

Ist nun $r \in \{0,1,2,3\}$ mit $2019^{2020} \equiv r \mod 4$, dann folgt $2018^{(2019^{2020})} \equiv 18^r \mod 25$, denn: $2019^{2020} \equiv r \mod 4$

$\Rightarrow \exists k \in \mathbb{Z}$ mit $2019^{2020} = 4k + r$

$\Rightarrow \overline{2018}^{2019^{2020}} = \overline{18}^{4k+r} = (\overline{18}^4)^k \cdot \overline{18}^r$

$= \overline{1}^k \cdot \overline{18}^r = \overline{18}^r \Rightarrow 2018^{(2019^{2020})} \equiv 18^r \mod 25$

$2019 \equiv -1 \mod 4 \rightarrow 2019^{2020} \equiv$

$\uparrow_{4 \mid 2020}$

$(-1)^{2020} \equiv ((-1)^2)^{1010} = 1^{1010} \equiv 1 \mod 4.$

$\Rightarrow 2018^{(2019^{2020})} \equiv 18^1 \equiv 18 \mod 25$

Also ist $\overline{18} + 25\mathbb{Z}$ die gesuchte Restklasse.

zu (b)

Die Zahl 2018 ist durch 2 teilbar, und folglich ist 2018^n für alle $n \geq 2$ durch 4 teilbar. Insbesondere gilt $a = 2018^{(2019^{2020})}$ wegen $2019^{2020} \geq 2$ durch 4 teilbar. Das Bild von a in $\mathbb{Z}/4\mathbb{Z}$ stimmt also mit $0 + 4\mathbb{Z}$ überein.

zu (c)

Nach Teil (a) und (b) gilt $a \equiv 18 \mod 25$ und $a \equiv 0 \mod 4$. Wegen $\mathrm{ggT}(4, 25) = 1$ ist der Chinesische Restsatz anwendbar, und demnach existiert ein eindeutig bestimmtes $b \in \{0, 1, ..., 99\}$ mit $b \equiv 18 \mod 25$ und $b \equiv 0 \mod 4$. Die Zahlen in diesem Bereich, die die erste Kongruenz erfüllen, sind 18, 43, 68 und 93. Die einzige Zahl, die auch kongruent zu 0 modulo 4 ist, ist 68. Es gilt also $a \equiv 68 \mod 100$. Folglich sind 6 und 8 die letzten beiden Dezimalstellen von a.