

Rechnen mit dem Chinesischen Restsatz:
H16T2A5, H14T3A2 (c)

n -te Potenzen und Lösung von Polynom-
gleichung in Zshg. mit dem Chin. Restsatz:
H14T3A2, H12T3A4

Aufgabe

- (a) Zeigen Sie, dass es für jede ungerade
Primzahl p genau $\frac{p+1}{2}$ Quadrate in $\mathbb{F}_p$
gibt.
- (b) Bestimmen Sie die Anzahl der Quadrate

gibt.
(b) Bestimmen Sie die Anzahl der Quadrate
im Restklassenring $\mathbb{Z}/2024\mathbb{Z}$.

zu (a) Sei Q die Menge der Quadrate in $\mathbb{F}_p^\times$.
Dann ist Q genau das Bild der Abbildung
 $\phi: \mathbb{F}_p^\times \rightarrow \mathbb{F}_p^\times, a \mapsto a^2$. Die Abbildung
ist ein Gruppenhomomorphismus wegen $\phi(ab) = (ab)^2$
 $= a^2 b^2 = \phi(a) \phi(b) \forall a, b \in \mathbb{F}_p^\times$.
Homomorphismussatz für Gruppen $\Rightarrow$
 $\mathbb{F}_p^\times / \ker(\phi) \cong Q$. Beh. $\ker(\phi) = \{\pm 1\}$
denn: Für alle $a \in \mathbb{F}_p^\times$ gilt die Äquiva-
lenz $a \in \ker(\phi) \Leftrightarrow \phi(a) = 1 \Leftrightarrow a^2 = 1$

$$\Leftrightarrow a^2 - \bar{1} = \bar{0} \Leftrightarrow (a - \bar{1})(a + \bar{1}) = \bar{0} \Leftrightarrow a - \bar{1} = \bar{0}$$

oder $a + \bar{1} = \bar{0} \Leftrightarrow a \in \{\pm \bar{1}\} \quad (\Rightarrow \text{Beh.})$

Da p ungerade ist, gilt $-\bar{1} \neq \bar{1}$ und somit $|\ker(\phi)| = 2$

$$\mathbb{F}_p^* / \ker(\phi) \cong Q \Rightarrow |\mathbb{F}_p^* / \ker(\phi)| = |Q| \Rightarrow |Q| =$$

$$\frac{|\mathbb{F}_p^*|}{|\ker(\phi)|} = \frac{1}{2}(p-1) \quad \text{Da auch } \bar{0} \text{ wg. } \bar{0}^2 = \bar{0} \text{ in } \mathbb{F}_p$$

ein Quadrat ist, gibt es genau $\frac{1}{2}(p-1) + 1 = \frac{1}{2}(p+1)$

Quadrate in $\mathbb{F}_p$.

Alternative: $\mathbb{F}_p^*$ ist zyklisch (als multiplikative Gruppe eines Körpers) $\Rightarrow \exists c \in \mathbb{F}_p^*$ mit $\mathbb{F}_p^* = \langle c \rangle$

überprüfe: $Q = \langle c^2 \rangle \Rightarrow |Q| = |\langle c^2 \rangle| = \text{ord}(c^2) =$

Quadrates in $\mathbb{F}_p$.

Alternative: $\mathbb{F}_p^\times$ ist zyklisch (als multiplikative Gruppe eines Körpers) $\Rightarrow \exists c \in \mathbb{F}_p^\times$ mit $\mathbb{F}_p^\times = \langle c \rangle$

$$\frac{1}{2} \text{ord}(c) = \frac{1}{2}(p-1) \quad (\text{Details als Übung})$$

zu (b) $2024 = 8 \cdot 11 \cdot 23$ Da 8, 11 und 23 paarweise teilerfremd sind, existiert ein Isomorphismus von Ringen $\mathbb{Z}/2024\mathbb{Z} \cong \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/23\mathbb{Z}$

Beh. i) Sind R, S ^{endliche} isomorphe Ringe, dann existieren in R und S gleichviele Quadrate.

ii) Die Quadrate in $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/23\mathbb{Z}$ sind genau die Elemente von $Q_8 \times Q_{11} \times Q_{23}$, wobei Q_m für $m \in \{8, 11, 23\}$ jeweils die Menge der Quadrate in $\mathbb{Z}/m\mathbb{Z}$ bezeichnet.

zu ii) Sei $\phi: R \rightarrow S$ ein Ringisomorphismus. zeige: Für jedes $a \in R$ ist a genau dann ein Quadrat in R , wenn $\phi(a)$ ein Quadrat in S ist. Daraus folgt, dass ϕ eine Bijektion zwischen den Quadraten in R und denen von S liefert. Sei also $a \in R$

" $\Rightarrow$ " a Quadrat in $R \Rightarrow \exists b \in R$ mit $a = b^2 \Rightarrow \phi(a) = \phi(b^2) = \phi(b)^2$, dies ist ein Quadrat in S

" $\Leftarrow$ " $\phi(a)$ Quadrat in $S \Rightarrow \exists c \in S$ mit $\phi(a) = c^2 \Rightarrow a = \phi^{-1}(\phi(a)) =$

$\phi^{-1}(c^2) = \phi^{-1}(c)^2$ Dies ist ein Quadrat in $\mathbb{R}$.

zu (ii) Sei $\tilde{Q}$ die Menge der Quadrate in $\mathbb{R} = \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/23\mathbb{Z}$.

z.zg: $\tilde{Q} = Q_8 \times Q_{11} \times Q_{23}$

" $\supseteq$ " Seien $a \in Q_8, b \in Q_{11}, c \in Q_{23}$.

$$\Rightarrow \exists a_1 \in \mathbb{Z}/8\mathbb{Z}, b_1 \in \mathbb{Z}/11\mathbb{Z}, c_1 \in \mathbb{Z}/23\mathbb{Z}$$

$$\text{mit } a = a_1^2, b = b_1^2, c = c_1^2 \Rightarrow$$

$$(a, b, c) = (a_1^2, b_1^2, c_1^2) = (a_1, b_1, c_1)^2 \in \tilde{Q}$$

" $\subseteq$ " Sei $(a, b, c) \in \tilde{Q}$ mit $a \in \mathbb{Z}/8\mathbb{Z}$,

$$b \in \mathbb{Z}/11\mathbb{Z}, c \in \mathbb{Z}/23\mathbb{Z} \Rightarrow$$

$$\exists (a_1, b_1, c_1) \in \mathbb{R} \text{ mit } (a_1, b_1, c_1)^2 =$$

$$(a, b, c) \Rightarrow (a_1^2, b_1^2, c_1^2) = (a, b, c) \Rightarrow$$

$$a = a_1^2 \in Q_8, b = b_1^2 \in Q_{11}, c = c_1^2 \in Q_{23}$$

$$\Rightarrow (a, b, c) \in Q_8 \times Q_{11} \times Q_{23} \quad (\Rightarrow \text{Beh.})$$

Wegen li) ist die Anzahl der Quadrate in $\mathbb{Z}/2024\mathbb{Z}$ gleich $|\tilde{Q}|$, und nach lii) ist

$$\text{diese Anzahl gleich } |Q_8 \times Q_{11} \times Q_{23}| \\ = |Q_8| \cdot |Q_{11}| \cdot |Q_{23}|$$

Da 11 und 23 Primzahlen sind (und somit $\mathbb{Z}/11\mathbb{Z} = \mathbb{F}_{11}$, $\mathbb{Z}/23\mathbb{Z} = \mathbb{F}_{23}$)

$$\text{folgt aus Teil (a) } |Q_{11}| = \frac{11+1}{2} = 6$$

$$\text{und } |Q_{23}| = \frac{23+1}{2} = 12.$$

In $\mathbb{Z}/8\mathbb{Z}$ gilt $0^2 = 0, 1^2 = 1, 2^2 = 4,$
 $3^2 = 9 = 1, 4^2 = 0, 5^2 = 1, 6^2 = 4, 7^2 = 1$
 $\Rightarrow Q_8 = \{0, 1, 4\} \Rightarrow |Q_8| = 3$

Die Anzahl der Quadrate in $\mathbb{Z}/2024\mathbb{Z}$ ist
 somit gleich $3 \cdot 6 \cdot 12 = 216$. $\square$

Übung: (a) Bestimmen Sie die Anzahl der
 Quadrate in $\mathbb{Z}/2025\mathbb{Z}$ oder $\mathbb{Z}/2026\mathbb{Z}$.
 (b) Bestimmen Sie die Anzahl der dritten und
 fünften Potenzen in $\mathbb{Z}/2024\mathbb{Z}$.

H24T3A2 Sei $R = \mathbb{Z}[x]/(x^3+x)$

(a) Zeigen Sie, dass R zu $\mathbb{Z} \times \mathbb{Z}[i]$ isomorph ist.

In $\mathbb{Z}[x]$ gilt $x^3+x = x \cdot (x^2+1)$. Somit
das Hauptideal (x^3+x) gleich dem Produkt
der Hauptideale $I = (x)$ und $J = (x^2+1)$

Wegen $1 = (-x) \cdot x + 1 \cdot (x^2+1) \in I + J$
gilt $I + J = (1)$, d.h. die Ideale I und
 J sind teilerfremd. Chines. Restsatz $\Rightarrow$

Nach
 $\exists h$
 $\Rightarrow$
mit
 $\sum_{i=0}^n a_i$
 $\Rightarrow g$

Es existiert ein Isom. $\Phi: R \rightarrow \mathbb{Z}[x]/I \times \mathbb{Z}[x]/J$
mit $\Phi(g+(f)) = (g+I, g+J)$, wobei $f = x^3 + x$
ist. Beh.: (i) $\mathbb{Z}[x]/I \cong \mathbb{Z}$ (ii) $\mathbb{Z}[x]/J \cong \mathbb{Z}[i]$

Dann folgt $R \cong \mathbb{Z}[x]/I \times \mathbb{Z}[x]/J \cong \mathbb{Z} \times \mathbb{Z}[i]$
zu i) Für jedes $z \in \mathbb{C}$ sei $\phi_z: \mathbb{Z}[x] \rightarrow \mathbb{C}$ der
Auswertungshom. und $\phi_z(x) = z$.

Beh.: $\phi_0(\mathbb{Z}[x]) = \mathbb{Z}$ und $\ker(\phi_0) = I$

Ist das gezeigt, dann liefert der Homomorphismsatz für Ringe den ang. Isomorphismus.

Nachweis von $\phi_0(\mathbb{Z}[x]) = \mathbb{Z}$: " $\subseteq$ " Sei $\tilde{f} = \sum_{k=0}^n a_k x^k$
 mit $n \in \mathbb{N}_0$ und $a_0, \dots, a_n \in \mathbb{Z} \Rightarrow \phi_0(\tilde{f}) = \sum_{k=0}^n a_k \cdot 0^k$
 $= a_0 \in \mathbb{Z}$ " $\supseteq$ " Sei $a \in \mathbb{Z} \Rightarrow \phi_0(a) = a \Rightarrow a \in \phi_0(\mathbb{Z}[x])$

Nachweis von $\ker(\phi) = I$: " $\supseteq$ " $g \in I \Rightarrow g \in (x) \Rightarrow$
 $\exists h \in \mathbb{Z}[x]$ mit $g = xh \Rightarrow \phi_0(g) = \phi_0(xh) = 0 \cdot h(0) = 0$
 $\Rightarrow g \in \ker(\phi)$ " $\subseteq$ " Sei $g \in \ker(\phi)$, $g = \sum_{k=0}^n a_k x^k$
 mit $n \in \mathbb{N}_0$, $a_0, \dots, a_n \in \mathbb{Z} \Rightarrow \phi_0(g) = 0 \Rightarrow$
 $\sum_{k=0}^n a_k 0^k = 0 \Rightarrow a_0 = 0 \Rightarrow g = x \cdot \sum_{k=1}^n a_k x^{k-1}$
 $\Rightarrow g \in (x) \Rightarrow g \in I$

zu ii) Wende den Homomorphiesatz auf den Auswertungshomomorphismus ϕ_i an. zu überprüfen:

$$\text{ii) } \phi_i(\mathbb{Z}[x]) = \mathbb{Z}[i] \quad \text{iii) } \ker(\phi_i) = \mathcal{I}$$

zeige nur " $\subseteq$ " in Teil iii), Rest als Übung

$$\text{Sei } g \in \ker(\phi_i) \Rightarrow \phi_i(g) = 0 \Rightarrow g(i) = 0$$

$\Rightarrow g$ ist in $\mathbb{Q}[x]$ (!) ein Vielfaches des Minimalpolynoms von i über $\mathbb{Q}$, also Vielfaches von $x^2+1 \Rightarrow (x^2+1) | g$

in $\mathbb{Q}[x]$ x^2+1 ist primär in $\mathbb{Z}[x]$ (da normiert) $\Rightarrow (x^2+1) | g$ in $\mathbb{Z}[x] \Rightarrow \exists h \in \mathbb{Z}[x]$ mit $g = h \cdot (x^2+1)$

$$\Rightarrow g \in (x^2+1) \Rightarrow g \in \mathcal{I}$$

(b) Bestimmen Sie alle Einheiten des Rings $\mathbb{Z} \times \mathbb{Z}[i]$.

Allgemein gilt: Sind R, S beliebige Ringe, dann ist die Einheitsengruppe von $R \times S$ geg. durch $R^\times \times S^\times$.

bekannt aus der Vorlesung: $\mathbb{Z}^\times = \{\pm 1\}$
und $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ (Dies sind die Elemente der Norm 1 in $\mathbb{Z}[i]$.)

also: $(\mathbb{Z} \times \mathbb{Z}[i])^\times = \{\pm 1\} \times \{\pm 1, \pm i\}$.

Der Ring $\mathbb{Z} \times \mathbb{Z}[i]$ besitzt also genau acht Einheiten.

Nach T
und (b-
(a,b) ∈

(c) Bestimmen Sie alle $(a, b) \in \mathbb{Z}^2$ mit der Eigenschaft, dass $x^2 + ax + b + (f)$ in R eine Einheit ist.

Nach Teil (a) ist ϕ ein Isomorphismus. Aus der zweimaligen Anwendung des Homomorphiesatzes in Teil (a) ergibt sich, dass Isomorphismen $R/I \rightarrow \mathbb{Z}$, $g+I \mapsto g(0)$ und $R/I \rightarrow \mathbb{Z}[i]$, $g+I \mapsto g(i)$ existieren. Daraus folgt, dass auch die Abbildung $\psi: R \rightarrow \mathbb{Z} \times \mathbb{Z}[i]$, $g+(f) \mapsto (g(0), g(i))$ ein Ringisomorphismus ist, als Komposition der Isomorphismen $\phi: R \rightarrow \mathbb{Z}[x]/I \xrightarrow{\sim} \mathbb{Z}[i]/I$.

und $\mathbb{Z}[x]/I \times \mathbb{Z}[x]/J \rightarrow \mathbb{Z} \times \mathbb{Z}[i]$, $(g+I, h+J) \mapsto (g(0), h(i))$. Für alle $a, b \in \mathbb{Z}$ ist somit $x^2 + ax + b + (f)$ genau dann eine Einheit in R , wenn $\varphi(x^2 + ax + b + (f))$ in $(\mathbb{Z} \times \mathbb{Z}[i])^\times$ liegt.

$$\Leftrightarrow \text{gilt } \varphi(x^2 + ax + b + (f)) =$$

$$(0^2 + a \cdot 0 + b, i^2 + ai + b) = (b, (b-1) + ia)$$

Nach Teil (b) gilt $b \in \mathbb{Z}^\times \Leftrightarrow b \in \{\pm 1\}$

und $(b-1) + ia \in (\mathbb{Z}[i])^\times \Leftrightarrow$

$$(a, b) \in \{(1, 1), (-1, 1), (0, 2), (0, 0)\}$$

der

(f) in

$$\text{also: } (b, (b-1) + (a)) \in \mathbb{Z} \times \mathbb{Z} / i$$

$$\Leftrightarrow b \in \{\pm 1\} \text{ und } (a, b) \in \{(1, 1), (-1, 1), (0, 2), (0, 0)\} \Leftrightarrow (a, b) \in \{(1, 1), (-1, 1)\}$$

mus

s Homo-

sich, dass

$$i \mapsto g(0)$$

(i) existieren.

Abbildung

$$\rightarrow (g(0), g(i))$$

als Komposi-

$$= \mathbb{Z}[i] / i \times \mathbb{Z}[i] / i$$

Es gibt also genau zwei Paare mit der
angef. Eigenschaft, nämlich $(1, 1)$ und $(-1, 1)$.

In der schriftliche Lösung hatte ich in Teil (c) die Aufgabenstellung nicht genau beachtet und **alle** Einheiten im Ring R bestimmt, und nicht nur die Einheiten der angegebenen Form. Ich habe das ausgebessert. Die Lösung hier an der Tafel ist korrekt.