Elemente der Mathematik - Sommer 2017

Prof. Dr. Peter Koepke, Thomas Poguntke — Lösung 2

Aufgabe 57 (2+3 Punkte)**.**

(a) Zeigen Sie, dass eine ganze Zahl n genau dann als Summe dreier aufeinanderfolgender ganzer Zahlen dargestellt werden kann, wenn $3|n$.

(b) Formulieren und beweisen Sie eine allgemeine Regel für Summen von k aufeinanderfolgenden Zahlen.

Lösung.

(a) Sei $n \in \mathbb{Z}$. Sei $n_0 \in \mathbb{Z}$, so dass $n = n_0 + (n_0 + 1) + (n_0 + 2) = 3 \cdot n_0 + 3 = 3 \cdot (n_0 + 1)$. Also $3 \mid n$.

Sei umgekehrt $3 \mid n$, also existiert $m \in \mathbb{Z}$, mit $n = 3 \cdot m$. Nun ist $n = (m-1) + m + (m-1)$.

(b) Für k ungerade gilt die obige Aussage allgemein. Beweis:

Sei $n \in \mathbb{Z}$ die Summe von k aufeinanderfolgenden Zahlen. Dann ist

$$n = \sum_{i=0}^{k-1} (n_0 + i) = k \cdot n_0 + \sum_{i=0}^{k-1} i = k \cdot n_0 + \frac{k \cdot (k-1)}{2} = k \cdot (n_0 + \frac{k-1}{2})$$

Dabei ist $n_0 + \frac{k-1}{2} \in \mathbb{Z}$, da $k - 1$ gerade. Also $k \mid n$.

Umgekehrt genügt es festzustellen, dass aus $k \mid n$ folgt, dass es $n_0 \in \mathbb{Z}$ gibt, sodass $n = k \cdot (n_0 + \frac{k-1}{2})$. Nämlich, falls $n = km$, dann ist $n_0 = m - \frac{k-1}{2}$.

Für k gerade ist n eine Summe von k aufeinanderfolgenden Zahlen genau dann, wenn $n \equiv \frac{k}{2} \bmod k$ ist. (Äquivalent: $\frac{k}{2} \mid n$ und $\frac{2n}{k}$ ist ungerade).

Der Beweis ist wie oben, außer dass wir bemerken:

$$n - \frac{k}{2} = k \cdot n_0 + \frac{k \cdot (k-1)}{2} - \frac{k}{2} = k \cdot (n_0 + \frac{k-2}{2})$$

und dabei ist $n_0 + \frac{k-2}{2} \in \mathbb{Z}$, da $k - 2$ gerade.

Aufgabe 58 (2+3+2 Punkte)**.**

(a) Sei p eine Primzahl und $0 < k < p$. Zeigen Sie, dass $p \mid \binom{p}{k}$. Folgern Sie mit Hilfe des binomischen Lehrsatzes, dass für alle ganzen Zahlen $a, b \in \mathbb{Z}$ gilt

$$(a + b)^p \equiv a^p + b^p \bmod p.$$

(b) Nutzen Sie (a), um per Induktion nach $a \in \mathbb{N}$ zu beweisen:

$$a^p \equiv a \bmod p.$$

Folgern Sie, dass falls $\mathrm{ggT}(a, p) = 1$ ist, sogar $a^{p-1} \equiv 1 \bmod p$ gilt.

(c) Bestimmen Sie die Endziffer von 7^{2017} (mit Begründung).

Lösung.

(a) Sei p eine Primzahl und $0 < k < p$. Es ist $\binom{p}{k} = \frac{p!}{k!\cdot(p-k)!}$. Im Nenner ist jeder einzelne Faktor echt kleiner als p. Weiter ist p prim. Also bleibt p als Faktor in $\binom{p}{k}$ erhalten.
Nun gilt gemäß des binomischen Lehrsatzes für $a, b \in \mathbb{Z}$:

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k \cdot b^{p-k}.$$

Außer für $k = 0$ oder $k = p$ sind wie gezeigt alle Summanden durch p teilbar. Dies sind gerade $a^p + b^p$.

(b) Beweis per Induktion:
(IA) Sei $a = 1$. Dann ist $a^p = 1^p = 1 \equiv 1 \bmod p$.
(IV) Die Aussage sei für $a \in \mathbb{N}$ bewiesen.
(IS) $(a+1)^p \overset{\text{(a)}}{\equiv_p} a^p + 1^p \overset{\text{(IV)}}{\equiv_p} a + 1$. Also tatsächlich $a^p \equiv a \bmod p$ für alle $a \in \mathbb{N}$.
Sei nun $\mathrm{ggT}(a,p) = 1$ und $a^p \equiv a \bmod p$. Dann $p \mid (a^p - a)$. Somit $p \mid a \cdot (a^{p-1} - 1)$. Da p und a teilerfremd, muss demnach $p \mid (a^{p-1} - 1)$. Also $a^{p-1} \equiv 1 \bmod p$.

(c) Es gilt $7^{2017} \bmod 10$ zu bestimmen. Da $\mathrm{ggT}(7,5) = 1$, ist $7^{2016} \equiv 1 \bmod 5$ nach (b), und da 7 ungerade ist, auch $7^{2016} \equiv 1 \bmod 2$. Zusammen genommen also $7^{2016} \equiv 1 \bmod 10$, und daher $7^{2017} \equiv 7 \bmod 10$.

Aufgabe 59 (2+2+2+2+2 Punkte)**.** Sei R ein Ring. Wir nennen die Menge der invertierbaren Elemente (bzgl. der Multiplikation) die Einheitengruppe $R^\times$.

(a) Zeigen Sie, dass $R^\times$ eine Gruppe ist.

(b) Beweisen Sie, dass $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ ein Ring ist. (Hier ist $i^2 = -1$).

(c) Zeigen Sie: $\alpha \in \mathbb{Z}[i]$ ist genau dann eine Einheit ist, wenn α auf dem Einheitskreis liegt. Folgern Sie, dass die Einheitengruppe $\mathbb{Z}[i]^\times = \mu_4$ ist. (siehe Präsenzblatt 1 für die Definition von μ_n).

(d) Sei p eine Primzahl. Konstruieren Sie einen Gruppenisomorphismus

$$(\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \mathbb{Z}/(p-1)\mathbb{Z}.$$

Hinweis: Benutzen Sie Aufgabe 58 (b).

(e) Geben Sie einen Ringhomomorphismus $\mathbb{Z}[i] \to \mathbb{Z}/5\mathbb{Z}$ an, dessen Einschränkung auf die Einheitengruppen ein Gruppenisomorphismus ist.

Hinweis: Ein Ringhomomorphismus auf $\mathbb{Z}[i]$ ist eindeutig durch seine Einschränkung auf die Einheitengruppe bestimmt. (Weshalb?)

Lösung. (a) Das neutrale Element $e. \in R^\times$ ist dasselbe wie in R. Weiter existiert zu jedem $a \in R^\times$ ein a^{-1}, weil $R^\times$ gerade die Menge der Elemente ist, für die genau dies gilt. Die Assoziativität vererbt sich aus R. Damit ist $R^\times$ eine Gruppe.

(b) Die Multiplikation ist abgeschlossen, denn es ist für $(a+b\cdot i), (a'+b'\cdot i) \in \mathbb{Z}[i].(a+b\cdot i)\cdot(a'+b'\cdot i) = a\cdot a'+a\cdot b'\cdot i+a'\cdot b\cdot i-b\cdot b' = a\cdot a'-b\cdot b'+i\cdot(a\cdot b'+a'\cdot b) \in \mathbb{Z}[i]$. Die Assoziativität von $'+','\cdot'$ bei $\mathbb{Z}[i]$ folgt aus der Assoziativität von $'+','\cdot'$ bei $\mathbb{Z}$. Die neutralen Elemente sind ebenfalls identisch. $1 = 1+0\cdot i$, bzw. $0 = 0+0\cdot i$. Für ein Elemente $a+b\cdot i$ existiert nun $-a-b\cdot i$ als das Inverse bezüglich der Addition. Damit ist $(\mathbb{Z}[i],+)$ schon mal eine Gruppe. Diese ist abelsch, da die Addition kommutativ ist. Die Verknüpfung von $'+','\cdot'$ ergibt sich aus dem Distributivgesetz auf dem Ring $\mathbb{Z}$. Damit ist $\mathbb{Z}[i]$ ein Ring.

(c) Sei $a+bi \in \mathbb{Z}[i]^\times$, also existiert $c+di \in \mathbb{Z}[i]$ mit $(a+bi)\cdot(c+di) = 1$. Damit ist auch $1 = (a+bi)\cdot(c+di)\cdot(a-bi)\cdot(c-di) = (a^2+b^2)\cdot(c^2+d^2)$. Da $a^2+b^2 \in \mathbb{N}$, muss $a^2+b^2 = 1$ und a liegt auf dem Einheitskreis. Sei andersrum $(a+b\cdot i)$ auf dem Einheitskreis, so ist $(a+b\cdot i)\cdot(a-b\cdot i) = a^2+b^2 = 1$, da $(a+b\cdot i)$ auf dem Einheitskreis liegt. Für $a,b \in \mathbb{Z}$ sind $a = \pm 1 \wedge b = 0$, bzw. $a = 0 \wedge b = \pm 1$ die einzigen Lösungen für $a^2+b^2 = 1$. Damit sind die Einheiten $\{1, i, -1, -i\}$. Dies ist gerade μ_4.

(d) Sei p eine Primzahl und $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ mit $\langle a\rangle := \{1, a, a^2, \ldots\} = (\mathbb{Z}/p\mathbb{Z})^\times$. Für den zu konstruierenden Homomorphismus $f\colon \mathbb{Z}/(p-1)\mathbb{Z} \to (\mathbb{Z}/p\mathbb{Z})^\times$ schicken wir nun $n \mapsto a^n$. Nach Aufgabe 58 (b) ist f wohldefiniert. Dies ist ein Gruppenhomomorphismus, da gerade $f(n+m) = a^{n+m} = a^n\cdot a^m = f(n)\cdot f(m)$. Weiter ist f surjektiv nach Definition, daher ein Isomorphismus, da beide Seiten $p-1$ Elemente haben (noch einmal 58 (b)).

Nun müssen wir noch die Existenz von a zeigen. Sei dafür $n := |\langle a\rangle|$ maximal. Wir müssen sehen, dass $n = p-1$ ist. Wir zeigen, dass $b^n = 1$ für jedes $b \in (\mathbb{Z}/p\mathbb{Z})^\times$ gilt. Dann folgt $p-1 \leq n$, da das Polynom x^n-1 höchstens n Nullstellen (modulo p) haben kann, und wir sind fertig.

Es sei $m := |\langle b\rangle|$. Nach Definition ist $m \leq n$, aber wir behaupten, dass sogar $m \mid n$ gilt. Für $m = 1$ ist nichts zu zeigen, also sei $b \neq 1$.

Angenommen $m \nmid n$. Dann können wir $m = p^d\cdot k$ und $n = p^e\cdot l$ schreiben, mit (p,k) und (p,l) teilerfremd und $d > e$. Aber dann sind auch $|\langle a^{p^e}\rangle| = l$

und $|\langle b^k \rangle| = p^d$ teilerfremd. Dementsprechend ist $|\langle a^{p^e} \cdot b^k \rangle| = l \cdot p^d = n \cdot p^{d-e} > n$, ein Widerspruch zur Maximalität von n.

(e) Es genügt einen Gruppenisomorphismus von den Einheitengruppen anzugeben, da $\mathbb{Z}[i]$ von den Einheiten $1, i$ erzeugt wird. Dieser ist

$$f : \mathbb{Z}[i]^\times \to (\mathbb{Z}/5\mathbb{Z})^\times, f(1) = 1, f(i) = 2, f(-1) = 4 = -1, f(-i) = 3.$$

Dies ist wohldefiniert, da $2^2 \equiv -1 \bmod 5$ ist. Es ist offensichtlich, dass f ein Isomorphismus ist. Somit erhalten wir den Ringhomomorphismus

$$g : \mathbb{Z}[i] \to \mathbb{Z}/5\mathbb{Z}, g(a + b \cdot i) = a + b \cdot 2.$$