H24-T2-A1

Sei R ein Ring und eine Folge $(a_n)_{n\geq 0}$ von Elementen von R rekursiv definiert wie folgt:

$$a_0 = a_1 = 1, \quad a_{n+2} = 2a_{n+1} + a_n.$$

a) Sei $\alpha \in R$ mit $\alpha^2 = 2$. Zeigen Sie, dass dann für alle $n \geq 0$ gilt

$$2a_n = (1+\alpha)^n + (1-\alpha)^n.$$

b) Sei p eine ungerade Primzahl, sodass es ein $\alpha \in R = \mathbb{F}_p$ (der Körper mit p Elementen) gibt mit $\alpha^2 = 2$.
Zeigen Sie, dass die Folge (a_n) periodisch ist mit einer minimalen Periode, die $p-1$ teilt.

c) Bestimmen Sie die kleinste ganze Zahl $k > 0$, sodass für $R = \mathbb{F}_7$ gilt $a_{n+k} = a_n$ für alle $n \geq 0$.

d) Zeigen Sie, dass es für $R = \mathbb{Z}$ keine ganzen Zahlen $m, n \geq 0$ mit der Eigenschaft $a_n = m^6 + 4$ gibt.

Lösung

a) Wir zeigen die Aussage mittels Induktion nach n. Für $n \in \{0, 1, 2\}$ rechnet man es einfach nach (Nachrechnen!). Wir folgern nun, dass wenn die Aussage für n und $n+1$ gilt, dann auch für $n+2$. Dazu rechnet man

$$2a_{n+2} = 2(2a_{n+1} + a_n) = 4a_{n+1} + 2a_n \overset{\text{IV}}{=} 2((1+\alpha)^{n+1} + (1-\alpha)^{n+1}) + (1+\alpha)^n + (1-\alpha)^n.$$

Da $(1+\alpha)^2 = 1 + 2\alpha + 2 = 2\alpha + 3$, sowie $(1-1\alpha)^2 = 3 - 2\alpha$ gilt, sieht man durch geschicktes Ausklammern, dass obige Gleichung sich in folgende Form bringen lässt

$$(1+\alpha)^n(2(1+\alpha)+1)+(1-\alpha)^n(2(1-\alpha)+1) = (1+\alpha)^n(3+2\alpha)+(1-\alpha)^n(3-2\alpha) = (1+\alpha)^{n+2}+(1-\alpha)^{n+2}.$$

Das zeigt die Behauptung.

b) Aus der Angabe folgt, dass $p \geq 3$ eine Primzahl ist. Wir berechnen a_p. Dazu betrachte

$$2a_p = (1+\alpha)^p + (1-\alpha)^p = 1 + \alpha^p + 1 - \alpha^p = 2 \Rightarrow a_p = 1.$$

Weiter berechnen wir a_{p-1}. Es gilt

$$2a_{p-1} = (1+\alpha)^{p-1} + (1+\alpha)^{p-1} = 1 + 1 = 2 \Rightarrow a_{p-1} = 1.$$

Hierbei haben wir genutzt, dass $\left|\mathbb{F}_p^\times\right| = p - 1$ und $\alpha \neq -1$ demnach ist $1 + \alpha \in F_p^\times$ und deshalb gilt $(1-\alpha)^{p-1} = 1$. Da die Folge rekursiv definiert ist, beginnt spätestens bei a_{p-1} die Folge von vorne. Es folgt also die geforderte Behauptung.

c) Wir rechnen einfach die Folgenglieder in $\mathbb{F}_7$ aus. Es gilt:

$$a_0 = 1, a_1 = 1, a_2 = 3, a_3 = 0, a_4 = 3, a_5 = 6, a_6 = 1, a_7 = 1.$$

Auch das bitte Nachrechnen! Die kleinste Periode ist also 6.

d) Angenommen es gibt $m, n \geq 0$ mit $a_n = m^6 + 4$. Dann muss diese Gleichung auch in $\mathbb{F}_7$ gelten. Demnach muss in $\mathbb{F}_7$ $a_n = m^6 + 4 = 1 + 4 = 5$ gelten. Da wir jedoch alle Folgeglieder (da Folge periodisch) in c) berechnet haben, und da keine 5 vorkommt, kann die Gleichung in $\mathbb{F}_7$ nicht gelten. Demnach auch nicht in $\mathbb{Z}$.