F18T2A4 (Forts.)

zu(a) Ergebnis:

(i) Für jedes $n \in \mathbb{N}_0$ ist 2^n+3 teilbar durch eine der Primzahlen 3, 5, 7, 13, wenn $n \equiv 1\ (4)$ oder $n \equiv 2\ (3)$ oder $n \equiv 10\ (12)$ gilt

(ii) Für jedes $n \in \mathbb{N}_0$ ist 2^n+5 teilbar durch eine dieser vier Primzahlen, wenn $n \equiv 0\ (2)$ oder $n \equiv 1\ (3)$ oder $n \equiv 3\ (12)$ gilt.

zu (b) ges: die Menge aller $n \in \mathbb{N}_0$ mit der Eigenschaft, dass 2^n+3 und 2^n+5 beides Primzahlen sind

Für $n \geq 4$ gilt $2^n+3 > 13$ und $2^n+5 > 13$.
Es können 2^n+3, 2^n+5 also beides nur dann Primzahlen sein, wenn die Zahlen durch keine der vier Primzahlen 3, 5, 7, 13 teilbar sind.
Nach Teil (a) ist 2^n+3 durch eine dieser Zahlen teilbar, falls $n \equiv a \ (12)$ mit $a \in \{\underbrace{1, 5, 9}_{n \equiv 1 \bmod 4}, \underbrace{2, 8, 11}_{n \equiv 2 \bmod 3}, 10\}$. Ebenso ist 2^n+5 durch eine

dieses Zahlen teilbar, wenn $n \equiv a \ (12)$ mit $a \in \{\underbrace{0,2,4,6,8,10}_{n \equiv 0 \ (2)}, \underbrace{1,7}_{n \equiv 1 \ (3)}, 3\}$. Insgesamt ist 2^n+3 oder 2^n+5 durch eine der vier Primzahlen teilbar, wenn $n \equiv a \ (12)$ mit $a \in \{0,1,2,3,4,5,6,7,8,9,10,11\}$ erfüllt ist. Dies ist für alle $n \in \mathbb{N}$ mit $n \geq 4$ der Fall. Also gibt es keines dieser n, dass 2^n+3 und 2^n+5 beide prim sind. Überprüfe die restlichen $n \in \mathbb{N}_0$ per Hand.

$n = 0$ $\quad 2^0+3 = 4$ (nicht prim), $2^0+5 = 6$ (nicht prim)

$n = 1$ $\quad 2^1+3 = 5$ (prim), $2^1+5 = 7$ (prim)

$n = 2$ $\quad 2^2+3 = 7$ (prim), $2^2+5 = 9$ (nicht prim)

$n = 3$ $\quad 2^3+3 = 11$ (prim), $2^3+5 = 13$ (prim)

Also ist $\{1, 3\}$ die gesuchte Teilmenge von $\mathbb{N}_0$. □

Irreduzibilitätskriterien für Polynome

Satz:

(i) Irreduzibilität von Polynomen über Körpern und Existenz von Nullstellen Sei K ein Körper und $f \in K[x] \setminus K$.

(1) $\operatorname{grad}(f) = 1 \Rightarrow f$ ist irred. in $K[x]$

(2) $\operatorname{grad}(f) \in \{2, 3\}$ und f hat in K keine Nullstelle $\Rightarrow f$ ist in $K[x]$ irreduzibel

(3) $\operatorname{grad}(f) \in \{4, 5\}$ und f hat in K keine Nullstellen und f hat keinen irred. Teiler vom Grad 2

$\Rightarrow f$ ist in $K[x]$ irreduzibel

(ii) Ist R ein faktorieller Ring, K sein Quotientenkörper, $f = a_n x^n + \dots + a_1 x + a_0 \in R[x]$ mit $a_n \neq 0$, $n \geq 1$, und ist $\alpha = \frac{p}{q} \in K$ eine Nullstelle von f mit $p, q \in R$ und $ggT(p,q) = 1_R$ dann gilt $p \mid a_0$ und $q \mid a_n$.

wichtiger Spezialfall: f ist normiert, d.h. $a_n = 1_R$ Dann liegt jede Nullstelle $\alpha \in K$ von f in R, und es gilt $\alpha \mid a_0$.

(iii) Sei R ein faktorieller Ring, K sein Quotientenkörper und $f \in R[x]$.

(1) Ist f in $R[x]$ irreduzibel, dann auch

in $K[x]$.

(2) Ist $f \in R[x]$ primitiv (d.h. die Koeff. von f haben keinen gem. Primteiler), dann gilt auch die Umkehrung).

(iv) Eisenstein-Kriterium: Sei R ein faktorieller Ring, $f = \sum_{k=0}^{n} a_n x^n$ ein primitives, nicht-konstantes Polynom und $p \in R$ ein Primelement mit den Eig. $p \nmid a_n$, $p \mid a_k$ für $0 \le k < n$ und $p^2 \nmid a_0$, dann ist f in $R[x]$ irreduzibel.

(v) Reduktionskriterium. Sei R ein faktorielles Ring, $\mathfrak{p}$ ein Primideal von R, $\overline{R} = R/\mathfrak{p}$ und $f = \sum_{k=0}^{n} a_k x^k \in R[x]$ ein primitives Polynom mit $a_n \notin \mathfrak{p}$. Sei $\overline{f}$ das Bild von

ein Quo-
$\in R[x]$
x eine
$gT(p,q) = 1_R$

ot, d.h.
le $\alpha \in K$ von

K sein
$[x]$.
el, dann auch

f in $\bar{R}[x]$. Ist f in $\bar{R}[x]$ irreduzibel, dann ist f in $R[x]$ irreduzibel (Achtung: Die Umkehrung dieser Aussage ist im Allg. falsch!)

Beispiele:

zu (i), (ii) $f = x^3 + x + 1 \in \mathbb{Z}[x]$

f ist normiert $\Rightarrow$ Jede Nullstelle $r \in \mathbb{Q}$ liegt in $\mathbb{Z}$ und erfüllt $r \mid 1 \Rightarrow r \in \{\pm 1\}$

$f(1) = 3 \neq 0$, $f(-1) = -1 \neq 0$ Also hat f in $\mathbb{Q}$ keine Nullstelle $\xrightarrow{\text{grad}(f)=3}$ f ist in $\mathbb{Q}[x]$ irreduzibel $\xrightarrow[\text{also primitiv}]{f \text{ ist normiert}}$ f ist auch in $\mathbb{Z}[x]$ irreduzibel.

zu (iii) Das Polynom $f = 2x + 6 \in \mathbb{Z}[x]$

ist irreduzibel in $\mathbb{Q}[x]$ (wegen grad $f = 1$),
aber reduzibel in $\mathbb{Z}[x]$, denn es ist
$f = 2 \cdot (x+3)$, und 2, $x+3$ sind beides keine
Einheiten in $\mathbb{Z}[x]$, wegen $(\mathbb{Z}[x])^\times = \mathbb{Z}^\times = \{\pm 1\}$
$\uparrow_{\mathbb{Z} \text{ Int.-B.}}$
Das Polynom f ist außerdem nicht primitiv.

zu (iv) Das Polynom $f = x^3 + 8x + 6 \in \mathbb{Z}[x]$
ist irreduzibel (in $\mathbb{Z}[x]$) nach dem Eisenstein-Kriterium,
denn f ist normiert und somit primitiv, und die
Primzahl 2 teilt $2+1$, $2 \cdot 0$, $2 \cdot 1$, $2 \cdot 1$, $2^2 + 6$,
Wegen (iii) ist f damit auch irred. in $\mathbb{Q}[x]$.

zu (v) $f = x^3 + x + 1 \in \mathbb{Z}[x]$ ist normiert, also
primitiv. Das Bild $\bar{f} = x^3 + x + \bar{1}$ von f in
$\mathbb{F}_2[x]$ ist nullstellenfrei (wg. $\bar{f}(\bar{0}) = f(\bar{1}) = \bar{1}$),
wg. grad$(\bar{f}) = 3$ also irreduzibel in $\mathbb{F}_2[x]$.

Nach dem Reduktionskriterium ist also f irreduzibel in $\mathbb{Z}[x]$, und damit auch in $\mathbb{Q}[x]$.

aber: Das Polynom $f = x^2 + 1$ ist in $\mathbb{Z}[x]$ irreduzibel (denn: f irred. in $\mathbb{Q}[x]$ (da $\operatorname{grad}(f) = 2$ ist und f keine Nullst. in $\mathbb{Q}$ hat) und als primitives Polynom somit auch in $\mathbb{Z}[x]$), obwohl das Bild $\overline{f} = x^2 + \overline{1} \in \mathbb{F}_2[x]$ nicht irreduzibel ist ($\overline{f} = (x + \overline{1})^2$)

H24T3A3 (Übung: F13T1A2)

Sei $f = x^{2024} + 2024 \in \mathbb{Z}[x]$. Es sei $(f_n)_{n \in \mathbb{N}_0}$ die Folge in $\mathbb{Z}[x]$ rek. durch $f_0 = x$ und $f_{n+1} = f(f_n) = f_n^{2024} + 2024 \quad \forall n \in \mathbb{N}_0$.

(a) Zeigen Sie, dass f in $\mathbb{Z}[x]$ irred. ist.

(b) Zeigen Sie, dass $f_n(0) \equiv 2024 \ (2024^2)$ für alle $n \geq 1$ gilt

(c) Beweisen Sie, dass f_n für alle $n \in \mathbb{N}_0$ irreduzibel ist.

zu (a) $2024 = 2^3 \cdot 11 \cdot 23$ Das Polynom f ist normiert und somit primitiv. Die Primzahl 11 teilt nicht den Leitkoeff. 1, aber alle anderen Koeff. (0 bzw. 2024), und es gilt $11^2 \nmid 2024$. Also ist f nach dem Eisensteinkrit. in $\mathbb{Z}[x]$ irreduzibel.

zu (b) Beweis der Aussage durch vollst. Induktion

Ind.-Anf. $n=1$ $f_1 = f = x^{2024} + 2024 \Rightarrow$

$f_1(0) = 2024 \Rightarrow f_1(0) \equiv 2024 \ (2024^2)$

Ind.-Schritt: Sei $n \in \mathbb{N}$, setze $f_n(0) \equiv 2024 \ (2024^2)$

voraus. $\Rightarrow \exists a \in \mathbb{Z}$ mit $f_n(0) = 2024 + 2024^2 \cdot a$.

z.z.: $f_{n+1}(0) \equiv 2024 \mod 2024^2$

$f_{n+1} = f_n^{2024} + 2024 \Rightarrow f_{n+1}(0) \equiv f_n(0)^{2024} + 2024$

$\equiv (2024 + 2024^2 \cdot a)^{2024} + 2024 \equiv (2024 + 0 \cdot a)^{2024} + 2024$

$\equiv 2024^{2024} + 2024 \equiv (2024^2)^{1012} + 2024 \equiv 0^{1012} + 2024$

$\equiv 2024 \; (2024^2)$

zu (c) Wenn die Primzahl 11 den Leitkoeff. von f_n nicht teilt, aber alle anderen Koeff., wenn 11^2 kein Teiler des konstanten Koeff. $f_n(0)$ ist und f_n am Boden prim ist, dann ist f_n jeweils irreduzibel, für jedes $n \in \mathbb{N}$.

Offenbar ist $f_1 = f$ normiert, und ist f_n normiert für ein $n \in \mathbb{N}$, dann offenbar auch f_n^{2024} (jede Potenz eines normierten Polynoms ist normiert), und somit auch $f_{n+1} = f_n^{2024} + 2024$. Vollst. Induktion zeigt also, dass die Polynome f_n mit $n \geq 1$ alle normiert sind. Damit ist 11 auch kein Teiler des Leitkoeff. von f_n, für alle $n \geq 1$.

Sei $\overline{f_n}$ jeweils das Bild von f_n in $\mathbb{F}_{11}[x]$.

Beh: $\overline{f_n} = x^{2024^n} \quad \forall n \in \mathbb{N}_0$

Beweis durch vollst. Ind.

Ind.-Anf. $n=0$: $\overline{f_0} = x = x^1 = x^{2024^0}$

Ind.-Schritt: Sei $n \in \mathbb{N}$, setze $\overline{f_n} = x^{2024^n}$ voraus.

Dann folgt $\overline{f_{n+1}} = \overline{f_n}^{2024} + \overline{2024} = \overline{f_n}^{2024}$

$11 \mid 2024$

Ind.V. $= (x^{2024^n})^{2024} = x^{2024^n \cdot 2024} = x^{2024^{n+1}}$ ($\Rightarrow$ Beh.)

Aus der Beh. folgt, dass das Bild aller Koeff. von f_n in $\mathbb{F}_{11}$ mit Ausnahme des Leitkoeff. jeweils gleich $\overline{0}$, der Koeff. also durch 11 teilbar ist, für alle $n \geq 1$.

Sei $n \in \mathbb{N}$ mit $n \geq 1$. noch z.zg. $11^2 \nmid f_n(0)$

Teil (b) $\Rightarrow f_n(0) \equiv 2024 \ (2024^2) \Rightarrow$

$\exists a \in \mathbb{Z}$ mit $f_n(0) = 2024 + 2024^2 \cdot a$

$\Rightarrow f_n(0) \equiv 2024 + 2024^2 \cdot a \equiv 2024 + 0 \cdot a$

$\uparrow 11^2 \mid 2024^2$

$\equiv 8 \cdot 11 \cdot 23 \ (11^2) \rightarrow \exists\, b \in \mathbb{Z} : f_n(0) =$

$8 \cdot 11 \cdot 23 + 11^2 \cdot b$ Ang. $11^2 \mid f_n(0) \rightarrow$

$11^2 \mid 8 \cdot 11 \cdot 23 \rightarrow 11 \mid 8 \cdot 23$ ↯

Also erfüllt f_n für jedes $n \geq 1$ die Voraussetzungen des Eisenstein-Kriteriums und ist somit in $\mathbb{Z}[x]$ irreduzibel.

Das Polynom $f_0 = X$ ist irred. in $\mathbb{Q}[x]$ (weg. $\text{grad}(f_0) = 1$), außerdem primitiv (da normiert), also auch irred. in $\mathbb{Z}[x]$.

□

Übung: F13T3A4 (Reduktionskriterium)
H17T1A5 (Eisenstein-Kriterium)
F08T2A4 (Eisen-Kriterium, schwer)
F09T1A4 (" " , schwer)