Prof. Dr. H. Brenner **Osnabrück WS 2021/2022**

Elliptische Kurven

Arbeitsblatt 26

Aufgaben

Aufgabe 26.1. Es sei R ein Integritätsbereich und $r \in R$ ein Element, das keine Quadratwurzel in R besitze. Zeige, dass das Polynom $X^2 - r \in R[X]$ irreduzibel ist.

Aufgabe 26.2. Es sei K ein Körper. Zeige, dass ein Polynom der Form

$$Y^2 + rY + s - X^3 - aX^2 - bX - c$$

(mit $r, s, a, b, c \in K$) irreduzibel in $K[X, Y]$ ist.

Aufgabe 26.3. Bestimme für die beiden affinen Gleichungen

$$Y^2 = X^3 + 16$$

und

$$V^2 + V = U^3,$$

die nach Aufgabe 5.9 die gleiche elliptische Kurve über $\mathbb{Q}$ definieren, den Reduktionstyp für die Primzahlen p mit schlechter Reduktion.

Aufgabe 26.4. Es seien $p_1, \ldots, p_n$ endlich viele Primzahlen. Bestimme für jede Primzahl den Reduktionstyp der elliptischen Kurve, die durch die Gleichung $Y^2 = X^3 - p_1 \cdots p_n$ gegeben ist.

Aufgabe 26.5. Es sei eine Gleichung der Form

$$Y^2 = (X - a)(X - b)(X - c)$$

mit $a, b, c \in \mathbb{Z}$ verschieden gegeben und sei E die zugehörige elliptische Kurve. Zeige die folgenden Aussagen.

(1) E besitzt modulo einer Primzahl p genau dann schlechte Reduktion, wenn p ein Teiler des Produktes $(a - b)(a - c)(b - c)$ ist.
(2) E besitzt modulo p genau dann additive Reduktion, wenn p ein gemeinsamer Teiler von $a - b, a - c, b - c$ ist. Dies ist genau dann der Fall, wenn p ein gemeinsamer Teiler von zwei Differenzen ist.

(3) Es tritt genau dann gar keine additive Reduktion auf, wenn $a-b, a-c, b-c$ teilerfremd sind, und dies ist genau dann der Fall, wenn zwei dieser Differenzen teilerfremd sind.

Aufgabe 26.6.*

Bestimme für jede Primzahl den Reduktionstyp der elliptischen Kurve, die durch die Gleichung $Y^2 = X^3 - 2X$ gegeben ist.

Aufgabe 26.7.*

Wir betrachten die durch die Gleichung

$$Y^2 = X^3 + 2X - 3$$

gegebene elliptische Kurve über verschiedenen Körpern K.

(1) Zerlege das Polynom $X^3 + 2X - 3$ in $\mathbb{Q}[X]$ in irreduzible Faktoren.
(2) Skizziere den reellen Verlauf der Kurve.
(3) Zerlege das Polynom $X^3 + 2X - 3$ in $\mathbb{C}[X]$ in irreduzible Faktoren.
(4) Bestimme, für welche Primzahlen p sich keine elliptische Kurve über $\mathbb{Z}/(p)$ ergibt.
(5) Bestimme den Reduktionstyp für die Primzahlen mit schlechter Reduktion

Aufgabe 26.8.*

Wir betrachten die durch die Gleichung

$$Y^2 = X^3 + 3X - 4$$

gegebene elliptische Kurve über verschiedenen Körpern K.

(1) Zerlege das Polynom $X^3 + 3X - 4$ in $\mathbb{Q}[X]$ in irreduzible Faktoren.
(2) Skizziere den reellen Verlauf der Kurve.
(3) Zerlege das Polynom $X^3 + 3X - 4$ in $\mathbb{C}[X]$ in irreduzible Faktoren.
(4) Bestimme, für welche Primzahlen p sich keine elliptische Kurve über $\mathbb{Z}/(p)$ ergibt.
(5) Bestimme den Reduktionstyp für die Primzahlen mit schlechter Reduktion

Die folgenden beiden Aufgaben erläutern, warum man von additiver Reduktion spricht.

Aufgabe 26.9.*

Es sei K ein Körper und seien $s, t \in K$. Zeige, dass die drei Punkte

$$\left(s,\, s^3\right),\, \left(t,\, t^3\right),\, \left(-(s+t),\, -(s+t)^3\right) \in \mathbb{A}^2_K$$

auf einer Gerade liegen.

Aufgabe 26.10. Wir betrachten die ebene projektive Kurve

$$C = V_+(Y^2Z - X^3) \subseteq \mathbb{P}^2$$

über einem Körper K.

(1) Zeige, dass $P = (0,0,1)$ der einzige singuläre Punkt der Kurve ist.
(2) Zeige, dass man auf $C \setminus \{P\}$ wie im elliptischen Fall (mit $\mathfrak{O} = (0,1,0)$ als neutralem Element) eine Gruppenverknüpfung definieren kann.
(3) Zeige, dass die Normalisierungsabbildung

$$\mathbb{P}^1_K \longrightarrow C \subseteq \mathbb{P}^2_K,\ (u,v) \longmapsto (u^2v, u^3, v^3),$$

bijektiv ist.
(4) Zeige unter Verwendung von Aufgabe 26.9, dass die Normalisierungsabbildung aus (3) eingeschränkt auf

$$\mathbb{A}^1_K = D_+(v) = \mathbb{P}^1_K \setminus \{(0,1)\}$$

einen Gruppenisomorphismus zwischen $\mathbb{A}^1_K$ und $C \setminus \{P\}$ definiert, wobei die affine Gerade mit der Addition versehen ist.

Aufgabe 26.11.*

Es seien $a, b \in \mathbb{C}$ und es sei

$$x_{r+1} = ax_r + bx_{r-1}$$

die dadurch definierte lineare Rekursion. Es sei c_r die zugehörige Folge zu den Startwerten c_0, c_1 und d_r die zugehörige Folge zu den Startwerten d_0, d_1. Zeige, dass die Differenzen $f_r = c_r - d_r$ ebenfalls die lineare Rekursion erfüllen.

Aufgabe 26.12. Es sei E eine elliptische Kurve über $\mathbb{Z}$ mit guter Reduktion modulo einer Primzahl p. Es seien a_{p^r} die in der Definition 26.10 rekursiv definierten Zahlen und es seien

$$b_{p^r} := p^r + 1 - \#\left(E_p(\mathbb{F}_{p^r})\right).$$

Zeige, dass die Differenzen $f_r = b_{p^r} - a_{p^r}$ die Rekursion

$$f_{r+1} = a_p f_r - p f_{r-1}$$

mit $f_0 = 1$ und $f_1 = 0$ erfüllen.

Aufgabe 26.13. Die Koeffizienten a_{p^r} seien durch die Anfangsbedingungen $a_1 = 1$, $a_p = a_p$ und für $r \geq 2$ durch die Rekursionsbedingung

$$a_{p^{r+1}} = a_p \cdot a_{p^r} - p \cdot a_{p^{r-1}}$$

definiert. Zeige, dass bei $a_p = 0$ die Beschreibung

$$a_{p^r} = \begin{cases} 0 \text{ bei } r \text{ ungerade,} \\ (-p)^{r/2} \text{ bei } r \text{ gerade,} \end{cases}$$

gilt.

In der folgenden Aufgabe wird eine L-Reihe betrachtet, die zu einer elliptischen Kurve gehören würde, die für jede Primzahl gute Reduktion hat und wo stets die Anzahl der $\mathbb{Z}/(p)$-rationalen Punkte gleich $p+1$ ist. Eine solche Kurve gibt es zwar nicht, eine solche L-Reihe gibt es natürlich trotzdem.

Aufgabe 26.14.*

Es sei $a_1 = 1$ und $a_p = 0$ für alle Primzahlen p. Wir betrachten die Dirichletreihe

$$L(s) = \sum a_n n^{-s}$$

zu multiplikativen Koeffizienten a_n. Zeige unter Verwendung von Aufgabe 26.13, dass

$$L(s) = \sum_{k \in \mathbb{N}_+} \lambda(k) k^{1-2s}$$

ist, wobei

$$\lambda(k) = \begin{cases} 1, \text{ falls die Anzahl aller Primfaktoren von } k \text{ gerade ist,} \\ -1 \text{ sonst,} \end{cases}$$

bezeichnet.

Aufgabe 26.15.*

Es seien $a, b \in \mathbb{C}$. Wir schreiben

$$\sum_{\ell=0}^{\infty} (a+bt)^\ell t^\ell = \sum_m c_m t^m$$

mit $c_m \in \mathbb{C}$. Zeige, dass diese Koeffizienten die Anfangsbedingungen $c_0 = 1$, $c_1 = a$ und die Rekursionsbedingung

$$c_{m+1} = ac_m + bc_{m-1}$$

erfüllt.

Aufgabe 26.16. Es sei $n \in \mathbb{N}$ und es sei vorausgesetzt, dass die Menge $\{(x,y,z) \in \mathbb{Z}^3 \mid 2x^2 + y^2 + 8z^2 = n\}$ leer ist. Zeige, dass dann auch die Menge $\{(x,y,z) \in \mathbb{Z}^3 \mid 2x^2 + y^2 + 32z^2 = n\}$ leer ist.

Aufgabe 26.17. Zeige, dass für die ungeraden quadratfreien kongruenten Zahlen n unterhalb von 32, das sind die Zahlen

$$n = 5, 7, 13, 15, 21, 23, 29, 31,$$

die Menge $\{(x, y, z) \in \mathbb{Z}^3 \mid 2x^2 + y^2 + 8z^2 = n\}$ leer ist.

Aufgabe 26.18. Überprüfe, dass für die ungeraden quadratfreien Zahlen n unterhalb von 32, die nicht kongruent sind, die Anzahlbedingung

$$\begin{aligned} & \#\left(\left\{(x, y, z) \in \mathbb{Z}^3 \mid 2x^2 + y^2 + 8z^2 = n\right\}\right) \\ = \; & 2 \cdot \#\left(\left\{(x, y, z) \in \mathbb{Z}^3 \mid 2x^2 + y^2 + 32z^2 = n\right\}\right) \end{aligned}$$

nicht gilt.

Aufgabe 26.19. Zeige, dass die Mengen

$$\left\{(x, y, z) \in \mathbb{Z}^3 \mid 2x^2 + y^2 + 8z^2 = 37\right\}$$

und

$$\left\{(x, y, z) \in \mathbb{Z}^3 \mid 2x^2 + y^2 + 8z^2 = 39\right\}$$

leer sind.

Aufgabe 26.20.*

(1) Bestimme die Menge $\{(x, y, z) \in \mathbb{Z}^3 \mid 2x^2 + y^2 + 32z^2 = 41\}$ und ihre Anzahl.
(2) Bestimme die Menge $\{(x, y, z) \in \mathbb{Z}^3 \mid 2x^2 + y^2 + 8z^2 = 41\}$ und ihre Anzahl.

Aufgabe 26.21. (1) Bestimme die Menge

$$\left\{(x, y, z) \in \mathbb{Z}^3 \mid 2x^2 + y^2 + 32z^2 = 51\right\}$$

und ihre Anzahl.
(2) Bestimme die Menge

$$\left\{(x, y, z) \in \mathbb{Z}^3 \mid 2x^2 + y^2 + 8z^2 = 51\right\}$$

und ihre Anzahl.

Aufgabe 26.22. (1) Bestimme die Menge

$$\left\{(x, y, z) \in \mathbb{Z}^3 \mid 2x^2 + y^2 + 32z^2 = 65\right\}$$

und ihre Anzahl.
(2) Bestimme die Menge

$$\left\{(x, y, z) \in \mathbb{Z}^3 \mid 2x^2 + y^2 + 8z^2 = 65\right\}$$

und ihre Anzahl.

Abbildungsverzeichnis