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

Elliptische Kurven

Arbeitsblatt 24

Aufgaben

AUFGABE 24.1. Berechne die Koeffizienten der Zetafunktion

$$\exp\left(\sum_{r=1}^{\infty} N_r \frac{t^r}{r}\right)$$

bis zum fünften Glied.

AUFGABE 24.2. Bestimme die Weilsche Zeta-Funktion für die einpunktige Varietät über $\mathbb{Z}/(p)$ mit Restekörper $\mathbb{Z}/(p)$.

AUFGABE 24.3. Bestimme die Weilsche Zeta-Funktion für die einpunktige Varietät über $\mathbb{F}_{p^e}$ mit Restekörper $\mathbb{F}_{p^e}$.

AUFGABE 24.4.*

Bestimme die Weilsche Zeta-Funktion für die einpunktige Varietät über $\mathbb{Z}/(p)$ mit Restekörper $\mathbb{F}_{p^e}$.

AUFGABE 24.5. Es sei $X = X_1 \uplus X_2$ die disjunkte Vereinigung der Varietäten X_1 und X_2 über dem endlichen Körper $\mathbb{F}_q$. In welcher Beziehung stehen die Zeta-Funktionen von X_1 und X_2 zur Zeta-Funktion von $X_1 \uplus X_2$?

AUFGABE 24.6. Bestimme die Weilsche Zeta-Funktion für die Produktvarietät $\mathbb{P}^1_{\mathbb{Z}/(p)} \times \mathbb{P}^1_{\mathbb{Z}/(p)}$ über $\mathbb{Z}/(p)$.

AUFGABE 24.7. Zeige, dass die Reihe $\sum_{r=1}^{\infty} \frac{N_r}{r} t^r$, wobei N_r die Anzahl der $\mathbb{F}_{q^r}$-rationalen Punkte des projektiven Raumes $\mathbb{P}^n_{\mathbb{F}_q}$ bezeichnet, für $|t| < \frac{1}{q^n}$ konvergiert.

Aufgabe 24.8. Es sei X eine projektive Varietät über einem endlichen Körper $\mathbb{F}_q$ und sei N_r die Anzahl der $\mathbb{F}_{q^r}$-rationalen Punkte von X. Zeige, dass es ein $m \in \mathbb{N}$ derart gibt, dass die Reihe $\sum_{r=1}^{\infty} \frac{N_r}{r} t^r$ für $|t| < \frac{1}{m}$ konvergiert.

Aufgabe 24.9.*

Es sei E eine elliptische Kurve über $\mathbb{Z}/(p)$ und sei

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

Zeige, dass diese Zahlen (mit $b_{p^0} = b_1 = 2$) für $r \geq 2$ die rekursive Bedingung

$$b_{p^{r+1}} = b_p \cdot b_{p^r} - p \cdot b_{p^{r-1}}$$

erfüllen.

Aufgabe 24.10.*

Es seien α und β komplexe Zahlen mit der Eigenschaft, dass sowohl $\alpha+\beta$ als auch $\alpha \cdot \beta$ ganzzahlig sind. Zeige, dass dann zu jedem $n \in \mathbb{N}$ auch $\alpha^n + \beta^n$ und $\alpha^n \cdot \beta^n$ ganzzahlig sind.

Aufgabe 24.11. Beweise die Hasseschranke mit Hilfe von Satz 24.3.

Aufgabe 24.12.*

Wir betrachten die durch die Gleichung

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

gegebene elliptische Kurve E über $\mathbb{Z}/(5)$.

(1) Bestimme die Anzahl der $\mathbb{Z}/(5)$-rationalen Punkte von E.
(2) Bestimme die Zeta-Funktion von E.
(3) Erstelle eine Formel für die Anzahl der $\mathbb{F}_{5^r}$-rationalen Punkte von E für jedes $r \in \mathbb{N}_+$.
(4) Bestimme die Anzahl der $\mathbb{F}_{5^r}$-rationalen Punkte von E für $r = 2, 3, 4$.

Abbildungsverzeichnis