Elliptische Kurven: Blatt 1

Abgabe: 27.4.2005 um 11:00 Uhr c.t.

1. Der Ring $\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\}$ heißt der Ring der *Gauß'schen Zahlen*. Wir schreiben $\mathbb{Z}[i]^\times$ für die Gruppe der multiplikative Einheiten von $\mathbb{Z}[i]$.

(a) Zeigen Sie dass $z = a + bi \in \mathbb{Z}[i]$ eine Einheit ist genau dann wenn $z \in \{\pm 1, \pm i\}$.

Sei $\Gamma = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot i = \mathbb{Z}[i] \subset \mathbb{C}$, und $E = \mathbb{C}/\Gamma$. In der Vorlesung ist der Ring

$$\mathrm{End}(E) = \{z \in \mathbb{C} \,|\, z\Gamma \subset \Gamma\}$$

der Endomorphismen von E definiert worden. Ein Endomorphismus $\varphi \in \mathrm{End}(E)$ heißt *Automorphismus* falls es ein $\psi \in \mathrm{End}(E)$ gibt mit

$$\psi \circ \varphi = \varphi \circ \psi = \mathrm{Id}_E \,.$$

Sei $\mathrm{Aut}(E) \subset \mathrm{End}(E)$ die Menge der Automorphismen von E.

(b) Zeigen Sie dass $\mathrm{End}(E) = \mathbb{Z}[i]$.

(c) Zeigen Sie dass $\mathrm{Aut}(E) = \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

2. Sei $z \in \mathbb{C} - \mathbb{R}$ und $\Gamma = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \tau \subset \mathbb{C}$ das zugehörige Gitter, und sei $E = \mathbb{C}/\Gamma$. Wähle $n \in \mathbb{Z}_{n>1}$ fest. Wir sagen dass $P = z + \Gamma \in E$ ein n-Teilungspunkt ist, falls $n \cdot P = nz + \Gamma = 0 + \Gamma$ gilt. Wir schreiben $E[n]$ fúr die Menge der n-Teilungspunkte von E.

(a) Bestimmen Sie die Menge $E[n]$. Was ist die Kardinalität von $E[n]$?

(b) Zeigen Sie dass $E[n] \subset E$ eine Untergruppe ist.

(c) Zeigen Sie dass

$$\varphi : E \to E, \qquad z + \Gamma \mapsto nz + \Gamma$$

einen Endomorphismus von E definiert, und dass

$$\mathrm{Kern}(\varphi) = \{z + \Gamma \in E \,|\, \varphi(z + \Gamma) = 0 + \Gamma\} = E[n].$$

(d) Schliesse aus (a) und (c) dass der Grad von φ gleich n^2 ist.

3. Sei $\Lambda \subset \mathbb{R}^2$ ein Gitter, und seien $a, b \in \Lambda$ linear unabhängig. Definiere

$$\Gamma = \{ma + nb \,|\, m, n \in \mathbb{Z}\}.$$

(a) Zeigen Sie dass $\Gamma \subset \Lambda$ ein Untergitter ist.

Der *Index* von Γ in Λ ist der Index als Untergruppe, dass heißt, die Anzahl der Elementen des Quotients Λ/Γ.

(b) Sei $\Lambda = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot i$ und $\Gamma = \mathbb{Z} \cdot 2 + \mathbb{Z} \cdot (1 + i)$. Zeigen Sie dass der Index von Γ in Λ gleich 3 ist.

(c) Seien Γ und Λ wie in (a). Zeigen Sie dass der Index von Γ in Λ die Anzahl der Gitterpunkten von Λ in dem Parallelogram $0, a, b, a + b$ welche **nicht** auf der Kanten $[a, a + b]$ und $[b, a + b]$ liegen ist.

d Zeigen Sie dass

$$\mathbb{C}/\Gamma \to \mathbb{C}/\Lambda, \qquad z \bmod \Gamma \mapsto z \bmod \Lambda$$

einen Homomorphismus elliptischer Kurven definiert, und dass der Grad dieses Homomorphismus der Index von Γ in Λ ist.

Elliptische Kurven: Blatt 2

Abgabe: 4.5.2005 um 11:00 Uhr c.t.

1. Sei $f \in \mathbb{Z}_{>0}$ eine positive ganze Zahl und $D > 0$ eine quadrat-freie ganze Zahl mit $D \equiv 1 \bmod 4$. Sei $\alpha = f\sqrt{-D}$.

(a) Bestimmen Sie das Minimalpolynom von α über $\mathbb{Q}$. Zeigen Sie dass $\mathcal{O} = \mathbb{Z}[\alpha] = \{a + b\alpha \,|\, a, b \in \mathbb{Z}\}$ ein Ring ist.

(b) Sei $\Gamma = \mathcal{O} = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \alpha$ dass zugehörige Gitter. Zeigen Sie dass die elliptische Kurve $E := \mathbb{C}/\Gamma$ komplexe Multiplikation hat, und dass $\mathrm{End}(E) = \mathcal{O}$.

Der Ring $\mathcal{O}$ heißt die Ordnung des Körpers $\mathbb{Q}(\sqrt{-D})$ mit Führer f. Falls $f = 1$, so heißt $\mathcal{O}$ die Maximalordnung.

2. Sei $\Gamma \subset \mathbb{C}$ ein Gitter. In der Vorlesung ist gezeigt dass Γ äquivalent ist zu ein Gitter $\mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \tau$, wobei $\tau \in \mathbb{H} = \{\tau \in \mathbb{C} \,|\, \mathrm{Im}(\tau) > 0\}$. Wir nennen $\mathbb{H}$ die obere Halbebene. Ziel dieser Aufgabe ist es zu zeigen dass wir sogar

$$\tau \in D := \{\tau \in \mathbb{H} \,|\, |\tau| \geq 1, |\Re(\tau)| \leq 1/2\}$$

nehmen dürfen. Vieleicht ist es nutzlich ein Bild von D zu skizzieren.

(a) Sei

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}).$$

Für $\tau \in \mathbb{H}$ definieren wir $A\tau = \dfrac{a\tau + b}{c\tau + d}$. Zeigen Sie dass $\mathrm{Im}(A\tau) = \mathrm{Im}(\tau)/|c\tau + d|^2$. Schliessen Sie dass dies eine Gruppenoperation von $\mathrm{SL}_2(\mathbb{R})$ auf $\mathbb{H}$ definiert.

Wir betrachten nun die Matrizen

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ in } \mathrm{SL}_2(\mathbb{Z}).$$

Sei $G \subset \mathrm{SL}_2(\mathbb{Z})$ die von S un T erzeugte Untergruppe. Wir nennen S Spiegelung und T Translation. (Wieso?)

(b) Sei $\tau \in \mathbb{H}$ mit $|\tau| < 1$. Zeigen Sie dass $|S\tau| > 1$.

(c) Sei $\tau \in \mathbb{H}$. Zeigen Sie es ein $n \in \mathbb{Z}$ gibt sodass

$$-\frac{1}{2} \leq \Re(T^n\tau) \leq -\frac{1}{2}.$$

Zeigen Sie dass für alle $n \in \mathbb{Z}$ gilt dass $|T^n\tau| = |\tau|$.

(d) Schliessen Sie dass jedes Gitter Γ äquivalent ist zu ein Gitter $\mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \tau$ mit $\tau \in D$.

3. Sei $\rho = e^{2\pi i/3} \in \mathbb{C}$ und $R = \mathbb{Z}[\rho] = \{a + b\rho \,|\, a, b \in \mathbb{Z}\}$. Es gilt dass $\rho^2 + \rho + 1 = 0$. Für $a + b\rho \in R$, definieren wir die Norm durch

$$N(a + b\rho) = (a + b\rho)(a + b\rho^2) = a^2 - ab + b^2.$$

(a) Seien $\alpha, \beta \in R$ mit $\beta \neq 0$. Schreibe $\alpha/\beta = x + y\rho$ mit $x, y \in \mathbb{Q}$. Zeigen Sie dass es $a, b \in \mathbb{Z}$ gibt sodass $N(x + \rho y - (a + b\rho)) < 1$ ist. (Skizziere ein Bild des Gitters $\mathbb{Z}[\rho]$.)

(b) Benutze (a) um zu zeigen dass R ein euklidischer Ring ist.

(c) Berechnen Sie $\mathrm{ggT}(4, 1 + 2\rho)$.

Elliptische Kurven: Blatt 3

Abgabe: 11.5.2005 um 11:00 Uhr c.t.

1. Sei E eine elliptische Kurve, und $P \in En$ ein echter n-Teilungspunkt, das heisst $nP = 0$, aber $mp \neq 0$ für alle $m < n$. Sei $f : E \to E'$ die Isogenie mit $\ker(f) =< P >$ (die Untergruppe von E welche von P erzeugt ist.

Elliptische Kurven: Blatt 4

Abgabe: 18.5.2005 um 11:00 Uhr c.t.

1. Sei $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ eine nichtkonstante meromorphe Funktion. Wir nennen

$$\Lambda_f = \{\omega \in \mathbb{C} \mid f(z+\omega) = f(z) \quad \text{für alle } z \in \mathbb{C}\}$$

die Menge der Perioden.

(a) Zeigen Sie dass Λ_f eine diskrete Untergruppe von $\mathbb{C}$ ist. Tip: benutzte der Index Satz.

(b) Schliesse aus (a) dass der Rang van Λ_f höchstens 2 ist.

(c) Sei $g : \mathbb{C} \to \mathbb{C} - \{0\}, z \mapsto \exp(2\pi i z/\omega)$, für $\omega \in \mathbb{C} - \{0\}$. Zeigen Sie dass $\Lambda_g = \mathbb{Z}\omega$.

(d) Sei f periodisch mit Periode $\omega \neq 0$. Zeigen Sie dass es eine meromorphe Funktion $F : \mathbb{C} - \{0\} \to \mathbb{C} \cup \{\infty\}$ gibt sodass

$$f(z) = F(\exp(2\pi i z/\omega))$$

ist.

2. Sei

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C}).$$

A definiert eine meromorphe Funktion

$$f_A : \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}, \qquad z \mapsto \frac{az+b}{cz+d}$$

definiert. Dies heisst ein *Möbiustransformation*.

(a) Sei $A \in \mathrm{SL}_2(\mathbb{C})$ mit $A^n = E$, für ein $n \in \mathbb{Z}_{>0}$. Zeigen Sie dass es ein Matrix $B \in \mathrm{GL}_2(\mathbb{C})$ gibt sodass

$$B^{-1}AB = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix},$$

wobei $\zeta \in \mathbb{C}$ ein $n$te Einheitswurzel ist, dass heisst $\zeta^n = 1$.

(b) Für $a \in \mathbb{C} \cup \{\infty\}$, bestimmen Sie alle $A \in \mathrm{GL}_2(\mathbb{C})$ welche der Punkt a festlassen.

(c) Sei

$$g : \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$$

die meromorphe Funktion definiert durch $z \mapsto w := \frac{1}{2}(z + \frac{1}{z})$. Finden Sie alle $w = a$ sodass $|g^{-1}(a)| = 1$. Diese Punkten heissen *Verzweigunspunkten*.

(d) Bestimmen Sie alle $A \in \mathrm{GL}_2(\mathbb{C})$ sodass

$$g \circ f_A = g.$$

Tip: Zeigen Sie dass $f_A(1) = 1$ und $f_A(-1) = -1$ und $f_A(0) \in \{0, \infty\}$.

3. (a) Berechnen Sie Polstellen und Residuen der folgende Funktionen:

$$\frac{1}{(z^2+1)(z-1)^2}, \qquad \frac{\exp(z)}{(z-1)^2}.$$

(b) Sei $a > 1$ eine reelle Zahl. Benutzen Sie die Residuensatz um folgende Integral zu berechnen:

$$\int_0^{2\pi} \frac{\mathrm{d}\,\theta}{a + \cos(\theta)}.$$

Siehe Freitag–Busam, *Funktionentheorie*. Seite 174–176.

Elliptische Kurven: Blatt 5

Abgabe: 25.5.2005 um 11:00 Uhr c.t.

1. Sei $\Lambda \subset \mathbb{C}$ ein Gitter.

(a) Sei f einer gerade elliptische Funktion zu Λ welches holomorph ausserhalb von Λ ist. Benutzte der Satz von Liouville um zu zeigen dass es ein Polynom $g \in \mathbb{C}[t]$ gibt sodass $f(z) = g(\wp(z))$ ist.

(b) Sei

$$g_2(\Lambda) = 60 \sum_{\substack{w \in \Lambda \\ w \neq 0}} \frac{1}{w^4}.$$

Zeigen Sie dass

$$\wp''(z) = 6\wp(z) - g_2(\Lambda)/2.$$

2. Sei $f(y) = y^3 + py + q \in \mathbb{C}[y]$ und $\alpha_1, \alpha_2, \alpha_3$ die Nulstellen von f. Also $f(y) = 4(y - \alpha_1)(y - \alpha_2)(y - \alpha_3)$. Die Diskriminante von f ist definiert als

$$\Delta = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Man kann zeigen dass $\Delta = -4p^3 - 27q^2$. Sei $\lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2 \subset \mathbb{C}$ ein Gitter, und sei $w_3 = w_1 + w_2$. Wir definieren

$$g_3(\Lambda) = 140 \sum_{\substack{w \in \Lambda \\ w \neq 0}} \frac{1}{w^6}.$$

In der Vorlesung wird gezeigt dass

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3. \tag{1}$$

Sei $f(y) = 4y^3 - g_2 y - g_3$ und $\Delta = \Delta(\Lambda)$ die Diskriminante von $f/4$. (Meistens multipliziert man Δ mit 16.) Ziel dieser Aufgabe ist es zu zeigen dass Δ ungleich null ist.

(a) Benutzen Sie (1) um zu zeigen dass $e_i := \wp(\omega_i/2)$ Nullstellen von f sind.

(b) Sei $H(z) := \wp(z) - \wp(w_i/2)$. Zeigen Sie dass H eine gerade Funktion ist mit einen Nullstelle in $w_i/2$ der Ordnung ≥ 2.

(c) Schliessen Sie dass $w_i/2$ der einzige Nullstelle von H ist, da $\wp$ der Ordnung 2 hat. Folgern Sie dass e_1, e_2, e_3 verschieden sind.

(d) Zeigen Sie dass $\Delta \neq 0$ ist.

3. Sei $\zeta = \exp(2\pi i/3) \in \mathbb{C}$ und $\Lambda = \mathbb{Z}[\zeta]$.

(a) Sei $(a, b) \in \mathbb{Z} \times \mathbb{Z} - \{(0, 0)\}$. Zeigen Sie dass

$$\frac{1}{(a + b\zeta)^4} + \frac{1}{(a\zeta^2 + b)^4} + \frac{1}{(a\zeta + b\zeta^2)^4} = 0.$$

Tip: benutze dass $\zeta = 1/(\zeta^2)^4$.

(b) Benutzte (a) um zu zeigen dass $g_2(\Lambda) = 0$.

Elliptische Kurven: Blatt 6

Achtung: Übung diese Woche am Freitag 27.05 9-11 Uhr c.t. in Raum 25.13 U1.32
Abgabe: 1.6.2005 um 11:00 Uhr c.t.

1. Sei $\Lambda = \mathbb{Z}[\zeta_3] \subset \mathbb{C}$ und $E = \mathbb{C}/\Lambda$. Von Blatt 5 Aufgabe 3 wissen wir dass $g_2(\Lambda) = 0$.

(a) Schliessen Sie aus Blatt 5 Aufgabe 2 dass $g_3(\Lambda) \neq 0$.

(b) In der Vorlesung wurde gezeigt dass es eine Einbettung

$$E - E[2] \hookrightarrow V(y^2 - 4x^3 - g_3(\Lambda)) \hookrightarrow \mathbb{C}^2$$

gibt. Zeigen Sie dass es $\alpha, \beta \in \mathbb{C} - \{0\}$ gibt so dass $(\tilde{x}, \tilde{y}) := (\alpha x, \beta y)$ die Gleichung

$$\tilde{y}^2 = \tilde{x}^3 - 1$$

erfüllen. Sei

$$C = \{(x, y) \in \mathbb{C}^2 \,|\, y^2 - x^3 + 1 = 0\}.$$

(c) Finden Sie alle $\gamma, \delta \in \mathbb{C} - \{0\}$ sodass

$$\sigma_{\gamma,\delta}(x, y) = (\gamma x, \delta y) : C \to C$$

eine Bijektion ist. Zeigen Sie dass die Gruppe $G := \{\sigma_{\gamma,\delta}\}$ (mit Verknüpfung als Gruppenoperation) eine zyklische Gruppe der Ordnung 6 ist.

(d) Sei $g \in G$. Bestimme alle $(x, y) \in C_F$ welche von g festgelassen werden. (Die Antwort hängt von der Wahl von g ab!)

2. Sei K ein Körper der Charakteristik $p \geq 0$ (also nicht notwendigerweise $K = \mathbb{C}$!) Sei $F \in K[x, y]$ ein Polynom mit $F \neq 0$. Sei $C_F = V(F) \hookrightarrow K^2$ die (affine) Kurve definiert von F. Wir sagen dass $P \in C_F$ eine Singularität von C_F ist falls

$$\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = 0.$$

Wir sagen dass C_F glatt ist falls C_F keine Singularitäten hat.

(a) Sei $F = y^2 - x^3 + 1$. Bestimmen Sie für welche Körper K die Kurve C_F glatt ist. (Tip: betrachte die Fälle $p = 2$, $p = 3$ und $p \neq 2, 3$.)

(b) Sei $F = y^2 + y - x^3$. Bestimmen Sie für welche Körper K die Kurve C_F glatt ist.

(c) Sei nun $K = \mathbb{C}$ und $F = y^2 - x^3 - x^2$. Bestimme die Singularitäten von C_F und skizziere $C_F \cap \mathbb{R}^2$.

3. Sei $\mathbb{P}^2_{\mathbb{C}} = \mathbb{C}^3 - \{(0,0,0)\}/\sim$, wobei $(x_0, x_1, x_2) \sim (y_0, y_1, y_2)$ falls es ein $\lambda \in \mathbb{C} - \{0\}$ gibt, sodass $x_i = \lambda y_i$ für $i = 0, 1, 2$. Wir bezeignen die Äquivalenzklasse von (x_0, x_1, x_2) mit $[x_0 : x_1 : x_2]$. Eine Gerade $L = L_a \subset \mathbb{P}^1_{\mathbb{C}}$ ist die Menge

$$L = L_a = \{[x_0 : x_1 : x_2] \in \mathbb{P}^1_{\mathbb{C}} \,|\, a_0 x_0 + a_1 x_1 + a_2 x_2 = 0\},$$

wobei $a = (a_0, a_1, a_2) \in \mathbb{C}^3 - \{(0,0,0)\}$.

(a) Für welche a und b sind L_a und L_b gleich?

(b) Zeigen Sie dass zwei Geraden L_a und L_b in $\mathbb{P}^2_{\mathbb{C}}$ sich immer schneiden. Falls $L_a \neq L_b$, zeigen Sie dass $L_a \cap L_b$ genau einen Punkt hat.

(c) Seien $A, B \in \mathbb{C}$ mit $-4A^3 - 27B^2 \neq 0$. Betrachte $X = \{[x : y : z] \,|\, y^2 z - 4(x^3 - Axz^2 - Bz^3) = 0\}$. Berechnen Sie die Schnittmengen $X \cap L_{(0,0,1)}$, $X \cap L_{(1,0,0)}$ und $X \cap L_{(0,1,0)}$. (Benutzte Blatt 5, Aufgabe 2.c.)

Elliptische Kurven: Blatt 7

Abgabe: 8.6.2005 um 11:00 Uhr c.t.

1. Sei $L = V_+(y) \subset \mathbb{P}^2_{\mathbb{C}}$.

(a) Berechnen Sie die Schnittmenge von L und $C = V_+(-yz^2 + x^3) \subset \mathbb{P}^1_{\mathbb{C}}$. Berechnen Sie auch die Schnittmultiplizitäten. Gleiche Frage für $C = V_+(-yz^2 + x^3 - x^2z)$.

(b) Sei $C = V_+(x^4 + y^4 + z^4 + 3(x^2y^2 + y^2z^2 + x^2z^2)$ und $P = (1 : i : 1)$. Sei L die Tangente an C in P. Berechnen Sie die Schnittmultiplizität von C und L in P.

2. Sei $E = V_+(y^2z - x^3 + z^3) \subset \mathbb{P}^2_{\mathbb{C}}$ und $P = (a : b : 1)$ einen Punkt von E. Sei $\mathcal{O} = (0 : 1 : 0)$ den Punkt von E in unendlich.

(a) Berechnen Sie eine Formel für die Tangente $L_{E,P}$ an E in P (in dem Teil von $\mathbb{P}^2_{\mathbb{C}}$ wo $z = 1$ ist).

(b) Zeigen Sie dass $3P = \mathcal{O}$ genau dann wenn die Schnittmultiplizität von $L_{E,P}$ und E drei ist.

(c) Berechnen Sie alle Punkten P von E so dass $3P = \mathcal{O}$. (Tip: kontrolieren Sie dass Sie alle Punkten gefunden haben mit Aufgabe 2 von Blatt 1. Betrachten Sie die Punkten mit $a = 0$ separat. Die Punkten mit $b = 0$ sind die 2-Teilungspunkten.)

3. Sei $k = \mathbb{F}_q$ ein endlicher Körper und sei $C = V(y^2 + y - x^3) \subset \mathbb{C}^2$.

(a) Sei $q = 3^n$. Zeigen Sie dass

$$\varphi : \mathbb{F}_q \to \mathbb{F}_q, \qquad x \mapsto x^3$$

ein Ringisomorphismus ist.

(b) Benutzen Sie (a) um die Kardinalität von

$$C(\mathbb{F}_{3^n}) = \{(x, y) \in \mathbb{F}^2_{3^n} \mid y^2 + y = x^3\}$$

zu bestimmen.

(c) Sei nun $q = 2^n$. Zeigen Sie dass

$$\psi : \mathbb{F}_q \to \mathbb{F}_q, \qquad y \mapsto y^2 + y$$

ein Gruppenhomomorphismus (von additive Gruppen) ist, und berechnen Sie den Kern von ψ.

(d) Sei $q = 2^n$ mit n ungerade. Zeigen Sie dass

$$\varphi : \mathbb{F}_q^\times \to \mathbb{F}_q^\times, \qquad x \mapsto x^3$$

ein Gruppenisomorphismus (von Multiplikative Gruppen) ist.

(e) Sei q wie in (d). Berechnen Sie die Kardinalität von $C(\mathbb{F}_q)$.

Elliptische Kurven: Blatt 8

Abgabe: 16.6.2005 um 11:00 Uhr c.t.

1. Sei $a, b \in \mathbb{C}$ mit $4a^2 + 27b^2 \neq 0$.

$$F = y^2z - x^3 - axz^2 - bz^3, \qquad E = V_+(F) \subset \mathbb{P}^2_{\mathbb{C}}.$$

   (a) Sei $P = (a : b : 1)$ und $Q = (b : c : 1)$ zwei Punkte von E mit $a, b, c, d \in \mathbb{Q}$ so dass $P \neq -Q$. Sei $P + Q = R$ (Addition auf der elliptische Kurve). Zeigen Sie dass $R = (e : f : 1)$ mit $e, f \in \mathbb{Q}$.

   (b) Falls $a, b, c, d \in \mathbb{Z}$, gilt dann auch $e, f \in \mathbb{Z}$? (Tip: betrachte die Kurve $y^2 = x^3 + 17$.)

   (c) Wir bezeichnen mit $E(\mathbb{Q})$ die Menge der Punkte von E mit "Koordinaten in $\mathbb{Q}$". Geben Sie eine genaue Definition dieser Menge, und zeigen Sie, dass $E(\mathbb{Q})$ eine Gruppe ist.

2. (a) Sei

$$F = y^2z - yz^2 - x^3 + x^2z, \qquad E = V_+(F) \subset \mathbb{P}^2_{\mathbb{C}}.$$

   Zeigen Sie, dass E eine glatte Kurve definiert, und dass $\mathcal{O} = (0 : 1 : 0)$ der einzige Punkt von E mit $z = 0$ ist. Wir bezeichnen mit $+$ die Addition auf E, wobei $\mathcal{O}$ der Ursprung ist.

   (b) Sei $P = (a, b)$ ein Punkt von $E - \{\mathcal{O}\}$ (also $z = 1$). Sei L die Gerade durch P und $\mathcal{O}$. Sei Q der dritte Schnittpunkt von L mit E, also $Q = -P$. Berechnen Sie die x- und y-Koordinaten von Q.

   (c) Sei nun $P = (1, 1) \in E - \mathcal{O}$. Berechnen Sie die Ordnung von P.

3. (a) Sei $\Lambda \subset \mathbb{C}$ ein Gitter, und sei $\alpha \in \mathbb{C} - \{0\}$. Zeigen Sie, dass

$$g_2(\alpha\Lambda) = \alpha^{-4} g_2(\Lambda), \qquad g_3(\alpha\Lambda) = \alpha^{-6} g_3(\Lambda).$$

   (b) Sei $\Lambda = \mathbb{Z}[i] \subset \mathbb{C}$, und $E = \mathbb{C}/\Lambda$. Zeigen Sie, dass $i\Lambda = \Lambda$. Schliessen Sie, dass $g_3(\Lambda) = 0$. Zeigen Sie, dass $j(\Lambda) = 1728$.

   (c) Sei $\Gamma \subset \mathbb{C}$ ein Gitter mit $j(\Gamma) = 1728$. Zeigen Sie dass es ein α gibt so, dass $\Gamma = \alpha\mathbb{Z}[i]$. (Benutzen Sie die Laurent-Entwicklung von $\wp$ um $z = 0$.)

Elliptische Kurven: Blatt 9

Abgabe: 22.6.2005 um 11:00 Uhr c.t.

1. Sei $m > 0$ eine ganze Zahl. Wir definieren

$$\Gamma_0(m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \,|\, c \equiv 0 \bmod m \right\}.$$

   (a) Zeigen Sie dass $\Gamma_0(m)$ eine Untergruppe von $\mathrm{SL}_2(\mathbb{Z})$ ist.

   (b) Sei $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(m)$. Zeigen Sie dass

$$A' := \begin{pmatrix} a & bm \\ c/m & d \end{pmatrix}$$

   ein Element von $\mathrm{SL}_2(\mathbb{Z})$ ist.

   (c) Wir definieren eine Function $J_m : \mathbb{H} \to \mathbb{C} \cup \{\infty\}$ durch

$$J_m(\tau) = j(m\tau).$$

   Sei $A \in \Gamma_0(m)$. Zeigen Sie dass $J_m(A\tau) = J_m(\tau)$.

2. Sei p ein Primzahl, und sei

$$C := \left\{ \sigma_p := \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_b := \begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix}, \quad b = 0, \ldots, p-1 \right\}.$$

   (a) Zeigen Sie dass

$$\sigma_p^{-1} \mathrm{SL}_2(\mathbb{Z}) \sigma_p \cap \mathrm{SL}_2(\mathbb{Z}) = \Gamma_0(p).$$

   (b) Wir definieren

$$\Gamma_b = \sigma_p^{-1} \mathrm{SL}_2(\mathbb{Z}) \sigma_b \cap \mathrm{SL}_2(\mathbb{Z}), \qquad b = 0, \ldots, p.$$

   Sei $A \in \Gamma_b$. Zeigen Sie dass für alle $B \in \Gamma_b$ gilt $BA^{-1} \in \Gamma_0(p)$. Schliessen Sie dass Γ_b eine Rechtsnebenklasse von $\Gamma_0(p)$ in $\mathrm{SL}_2(\mathbb{Z})$ ist.

   (c) Zeigen Sie dass $\Gamma_b \cap \Gamma_{b'} = \emptyset$, falls $b \neq b'$.

   (d) Zeigen Sie dass

$$\mathrm{SL}_2(\mathbb{Z}) = \coprod_{b=0}^{p} \Gamma_b.$$

   Schliessen Sie dass der Index von $\Gamma_0(p)$ in $\mathrm{SL}_2(\mathbb{Z})$ gleich $p+1$ ist.

   (e) Sei nun $p = 3$. Zeigen Sie dass

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, ST^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

   die Rechtsnebenklassen von $\Gamma_0(p)$ in $\mathrm{SL}_2(\mathbb{Z})$ darstellen.

3. Sei $\Lambda = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \tau \subset \mathbb{C}$ ein Gitter, und sei $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C$ (die Menge definiert in Aufgabe 2.)

   (a) Zeigen Sie dass $\Lambda' := \mathbb{Z} \cdot d + \mathbb{Z} d\sigma\tau$ ein Untergitter von Λ ist. Benutzen Sie Aufgabe 2 von Blatt 1 um zu zeigen dass der Index von Λ' in Λ gleich p ist.

   (b) Zeigen Sie dass $j(\Lambda') = j(\sigma\Lambda)$.

Elliptische Kurven: Blatt 10

Abgabe: 30.6.2005 um 11:00 Uhr c.t.

Referenz für die erste zwei Aufgaben: Serre, *A course in arithmetic*, Abschnitt 7.4. Aufpassen: Serre benutzt eine andere Definition von B_k.

1. (a) Sei $z \in \mathbb{C}$. Die Produktformel für $\sin(z)$ sagt:

$$\sin(z) = z \prod_{n=1}^{\infty} (1 - \frac{z^2}{n^2\pi^2}).$$

Siehe zum Beispiel Ahlfors *Complex Analyses*, Seite 197. Berechnen Sie die logarithmische Abgeleite von $\sin(\pi z)$, also $\mathrm{d}\sin(\pi z)/\sin(\pi z)$. Zeigen Sie dass

$$\pi \cot(\pi z) = \frac{1}{z} + \sum_{n=1}^{\infty} \left(\frac{1}{z+n} + \frac{1}{z-n} \right) = \sum_{n \in \mathbb{Z}} \frac{1}{z+n}. \qquad (2)$$

(b) Benutzen Sie (a, erste Gleichung von (2)) und die geometrische Reihe um zu zeigen dass

$$\pi z \cot(\pi z) = 1 - 2 \sum_{n=1}^{\infty} \sum_{k=1}^{\infty} \frac{z^{2k}}{n^{2k}}.$$

(c) Sei jetzt $x = 2\pi i z$. Benutzte die Definition der complexe trigoneometrische Funktionen um zu zeigen dass

$$\pi z \cot(\pi z) = \frac{x}{2} - \frac{x}{e^x - 1} = -\frac{x}{2} - x \sum_{n=1}^{\infty} e^{xn}.$$

(d) Die Bernoulli-Zahlen sind definiert durch

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}.$$

Zeigen Sie dass

$$\zeta(2k) = -\frac{(2\pi i)^{2k}}{2} \frac{B_{2k}}{(2k)!}, \qquad \text{für alle } k > 0.$$

(e) Zeigen Sie die folgende Identität:

$$\sum_{n \in \mathbb{Z}} \frac{1}{(z+n)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} e^{2\pi i n z}.$$

Tip: Vergleichen Sie die Ausdruecke in (a) und (c), und differentiere beide Seiten.

2. Sei

$$G_{2k}(z) = \sum_{(c,d) \neq (0,0)} \frac{1}{(cz+d)^{2k}},$$

die Eisenstein-Reihe von Gewicht $2k$. Ziel dieser Aufgabe ist es die q-Expansion von G_{2k} zu berechnen.

Sei $k, m \in \mathbb{Z}_{\geq 1}$. Wir definieren

$$\sigma_k(m) = \sum_{d|m} d^k.$$

(a) Zeigen Sie

$$G_{2k} = 2\zeta(2k) + 2\sum_{m=1}^{\infty}\sum_{n=-\infty}^{\infty}\frac{1}{(mz+n)^{2k}}.$$

(b) Zeigen Sie dass

$$G_{2k} = 2\zeta(2k)\left(1 - \frac{k}{B_{2k}}\sum_{m=1}^{\infty}\sigma(2k-1)q^m\right),$$

wobei $q = e^{2\pi iz}$ ist.

3. Wir definieren die normalisierte Eisenstein-Reihen als

$$E_{2k} = \frac{G_{2k}}{2\zeta(2k)}.$$

(a) Zeigen Sie dass $E_4^2 = E_8$ und $E_4E_6 = E_{10}$ ist.

(b) Drücken Sie $\sigma_7(m)$ aus in $\sigma_3(m)$, für alle m.

Elliptische Kurven: Blatt 11

Abgabe: 6.7.2005 um 11:00 Uhr c.t.
Klausur: Freitag 22.07.05, 11-13, nach vereinbarung.

1. Referenz für diese Aufgabe: Silverman, *Advanced topics in the arithmetic of elliptic curves*, Abschnitt 1.9. Sei $\mathcal{L} = \{ \Lambda \subset \mathbb{C} \,|\, \Lambda \text{ ist ein volles Gitter}\}$.

   (a) Sei $\Lambda = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \tau$, mit $\tau \in \mathbb{H}$ ein volles Gitter. Für $b = 0, \ldots p$ definieren wir $\sigma_b \in C$ wie in Blatt 9, Aufgabe 2. Sei $\Lambda_b \subset \Lambda$ das zugehörige Untergitter von Λ von Index p, wie definiert in Aufgabe 3 von Blatt 9. Zeigen Sie dass dies alle Untergitter von Λ sind welche Index p haben.

   (b) Zeigen Sie dass für alle b gilt dass

   $$p\Lambda \subset \Lambda_b \subset \Lambda.$$

   (c) Wir betrachten nun den Hecke-Operator $T_p : \mathbb{Z}[\mathcal{L}] \to \mathbb{Z}[\mathcal{L}]$. Es gilt

   $$T_p(\Lambda) = \sum_{b=0}^{p} 1 \cdot \Lambda_b.$$

   Für jedes Untergitter $\Gamma \subset \Lambda$ von Index p^2 definieren wir

   $$a(\Gamma) = \#\{b \,|\, \Gamma \subset \Lambda_b \subset \Lambda\}.$$

   Zeigen Sie dass

   $$T(p) \circ T(p)\Lambda = \sum_{\Gamma \subset \Lambda} a(\Gamma) \cdot \Gamma,$$

   wobei die Summe läuft über alle Untergitter $\Gamma \subset \Lambda$ von Index p^2.

   (d) Sei $\Gamma \subset \Lambda$ ein Untergitter von Index p^2. Wir nehmen an dass Γ enthalten ist in $p\Lambda$. Zeigen Sie dass $\Gamma = p\Lambda$. Schliessen Sie dass $a(\Gamma) = 1 + p$.

   (e) Sei $\Gamma \subset \Lambda$ ein Untergitter von Index p^2. Wir nehmen an dass Γ nicht enthalten ist in $p\Lambda$. Zeigen Sie dass es ein $b \in \{0, \ldots p\}$ gibt, so dass $\Gamma \subset \Lambda_b$.

   (f) Sei Γ wie in (e). Zeigen Sie dass

   $$\Gamma/(\Gamma \cap p\Lambda) = \Lambda_b/(\Lambda_b \cap p\Lambda).$$

   Tip: benutze (b). Schliessen Sie dass $\Gamma = \Lambda_b + p\Lambda$, und dass $a(\Gamma) = 1$.

2. (a) Wir betrachten die elliptische Kurve E mit Gleichung

   $$y^2 z = x^3 - xz^2$$

   in Charakteristik 3. Finden Sie alle Punkten von E mit Koeffizienten in $\mathbb{F}_9$. Tip: Es gilt $\mathbb{F}_9 = \mathbb{F}_3[i]$. Setzen Sie $z = 1, x = a + bi, y = c + di$ mit $a, b, c, d \in \mathbb{F}_3$. (Der Anzahl ist 16.)

   (b) Die übliche Additions-Formel [Silverman, *The arithmetic of elliptic curves*, Abschnitt III.2] definiert eine Gruppenoperation auf E. Sei $P = (x : y : 1)$ ein Punkt von E mit Koeffizienten in $\mathbb{F}_9$. Der Duplikations-Formel [Silverman, *The arithmetic of elliptic curves*, III.2.3.(d)] impliziert dass die x-Koordinate von $2P$ gleich

   $$a(x) := \frac{x(x^3 - x) + 1}{(x^3 - x)}$$

   ist. Zeigen Sie dass $a(x) \in \mathbb{F}_3$, falls $x \notin \mathbb{F}_3$, und $a(x) = \infty$, falls $x \in \mathbb{F}_3$, ist. Tip: was sind die Möglichkeiten für $x^3 - x$?

(c) Zeigen Sie dass falls $x, y \in \mathbb{F}_3$, so hat P der Ordnung 2.

(d) Berechnen Sie die Ordnung von alle Punkten P aus Teil (a). Tip: man braucht nur (b) und (c), und muss nicht weiter rechnen.

Elliptische Kurven: Blatt 12

Abgabe: 13.7.2005 um 11:00 Uhr c.t.
Letzter Zettel! Klausur: Freitag 22.07.05, 11-13, nach vereinbarung.

1. Sei p ein Primzahl und $f \in M_k$ eine Modulform von Gewicht k. Wie auf Blatt 9, definieren wir

$$\sigma_p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_b = \begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix}, \quad \text{für } b = 0, \ldots, p-1,$$

und $\Sigma_p = \{\sigma_b \,|\, b = 0, \ldots, p\}$. Sei $T_k(p) : M_k \to M_k$ der Hecke-Operator, wie definiert in der Vorlesung.

   (a) Zeigen Sie dass

$$\begin{aligned} T_k(p)f &= p^{k-1} \sum_{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Sigma_p} d^{-k} f\left(\frac{az+b}{d}\right) \\ &= \frac{1}{p}\sum_{b=0}^{p} f\left(\frac{z+b}{p}\right) + p^{k-1} f(pz). \end{aligned}$$

   (b) Sei $b \in \{0, \ldots, p-1\}$. Zeigen Sie dass

$$\sum_{b=0}^{p-1} \exp(2\pi i m(z+b)/p) = \begin{cases} p & \text{if } m \equiv 0 \bmod p, \\ 0 & \text{if } m \not\equiv 0 \bmod p. \end{cases}$$

   (c) Sei $f(z) = \sum_{m=0}^{\infty} a_m q^m$ die q-Entwicklung von f, wobei $q = \exp(2\pi i z)$. Zeigen Sie dass

$$T_k(p)f = \sum_{m=0}^{\infty} a_{mp} q^m + p^{k-1} \sum_{m=0}^{\infty} a_m q^{mp}.$$

   (d) Sei nun G_{2k} die Eisenstein-Reihe von Gewicht $2k$. Benutzten Sie die Idee von Aufgabe 3a von Blatt 10 um zu zeigen dass für $k = 2, 3, 4$, die Eisenstein-Reihen G_{2k} Eigenformen unter $T_k(p)$ sind, also dass

$$T_{2k}(p)G_{2k} = c_{2k}(p)G_{2k}.$$

   Berechnen Sie auch die Koeffizienten c_{2k}.

   (e) Sei $\Delta := g_2^3 - 27g_3^2 \in M_{12}$ die Diskriminante. Zeigen Sie dass Δ ein Eigenform ist von $T_{12}(p)$, und berechnen Sie den Eigenwert.

2. Sei K ein Körper, und $A, B \in K$ mit $\Delta = 4A^3 + 27B^2 \neq 0$. Sei $E_{A,B}$ die elliptische Kurve definiert durch $y^2 = x^2 + Ax + B$. Die j-Invariante von $E_{A,B}$ ist definiert durch

$$j(E_{A,B}) = \frac{4A^3}{4A^3 + 27B^2} \in K.$$

Zwei elliptische Kurven $E_{A,B}$ und $E_{A',B'}$, über K, sind isomorph über K falls es Einheiten $u_1, u_2 \in K^\times = K - \{0\}$ gibt, so dass

$$\varphi(x, y) = (u_1 x, u_2 y), \qquad E_{A,B} \to E_{A',B'}$$

ein Isomorphismus ist.

(a) Zeigen Sie dass falls $\varphi(x, y) = (u_1 x, u_2 y)$, $E_{A,B} \to E_{A',B'}$ ein Isomorphismus ist, so gilt $u_1 = u^2$ und $u_2 = u^3$ für ein $u \in K^\times$. Drücken Sie (A', B') in u und (A, B) aus.

(b) Finden Sie alle $(A, B) \in \mathbb{F}_5 \times \mathbb{F}_5$ so dass $j(E_{A,B}) = 0$. Welche dieser Kurven sind isomorph über $\mathbb{F}_5$?

(c) Zeigen Sie dass es ein Element $\alpha \in \mathbb{F}_{25}$ gibt so dass $\alpha^6 = 2$.

(d) Zeigen Sie dass alle elliptische Kurven $E_{A,B}$ mit $j = 0$ isomorph sind über $\mathbb{F}_{25}$.