Wolfgang K. Seiler
Tel. 2515

A5, C201

26. November 2013

11. Übungsblatt Elliptische Kurven

Auswahl möglicher Prüfungsfragen

- Was ist eine elliptische Kurve?
- Wie ist der n-dimensionale projektive Raum über einem Körper k definiert?
- Was ist eine ebene algebraische Kurve?
- Was ist ein Wendepunkt von C und wie lassen sich die Wendepunkte berechnen?
- Was ist die Vielfachheit eines Punktes einer algebraischen Kurve?
- Wie viele Punkte hat $\mathbb{P}^2(\mathbb{F}_p)$?
- Welche Eigenschaften hat die Resultante zweier Polynome?
- Wie kann man sie effizient berechnen?
- Wie läßt sich mit Hilfe der Resultante die Vielfachheit eines Punktes einer ebenen algebraischen Kurve definieren?
- Wie ist die Schnittmultiplizität zweier ebener algebraischer Kurven in einem Punkt P definiert?
- Sind die Kurven $y^2 = x^3 + x$ und $y^2 = x^3 - x$ projektiv äquivalent in $\mathbb{P}^2(\mathbb{R})$?
- Sind sie es in $\mathbb{P}^2(\mathbb{C})$?
- Wie sieht es aus bei $y^2 = x^3 \pm 1$?
- Geben seien eine ebene Kurve zweiten Grades C und eine ebene Kurve dritten Grades E in $\mathbb{P}^2(k)$. Welche Möglichkeiten gibt es für die Menge $C \cap E$?
- Was besagt der Satz von Bézout?
- *Beweisidee?*
- Was ist ein Divisor in $\mathbb{P}^2(k)$?
- Welche Dimension hat das lineare System aller kubischer Kurven durch acht vorgegebene Punkte von $\mathbb{P}^2(k)$? Kann es leer sein?
- Was wissen Sie über die Schnittmenge zweier Kurven aus diesem System?
- Wann sind n Punkte der projektiven Ebene in allgemeiner Lage in Bezug auf Kurven d-ten Grades?
- Wie ist die Hessesche einer ebenen algebraischen Kurve definiert?
- Wozu ist sie gut?
- Skizzieren Sie eine singuläre ebene Kurve vom Grad zwei!
- *Dito* vom Grad drei!
- Wie ist die Gruppenstruktur auf einer elliptischen Kurve definiert?
- Warum muß bei dieser Definition das Neutralelement ein Wendepunkt sein?
- Skizzieren Sie die wesentliche Idee zum Beweis des Assoziativitätsgesetzes!
- Wie viele Punkte der Ordnung zwei kann es geben?
- Ist die Kurve durch diese Punkte eindeutig festgelegt?

- Wodurch zeichnet sich die HESSE-Form der Gleichung einer elliptischen Kurve aus?
- Wodurch unterscheiden sich die WEIERSTRASS- und die LEGENDRE-Form?
- Welche j-Invariante hat die Kurve $y^2 = x^3 + x$?
- Wie lassen sich die Punkte der Ordnung drei auf einer elliptischen Kurve geometrisch charakterisieren?
- Wie viele Punkte der Ordnung drei kann es auf einer reellen elliptischen Kurve geben?
- Zwei ebene kubische Kurven schneiden sich in einem gemeinsamen Doppelpunkt. Wie groß muß die Schnittmultiplizität mindestens sein?
- Wie funktionen Verschlüsselung und elektronische Unterschrift nach Art von ELGAMAL mit elliptischen Kurven?
- Wie läßt sich einer vorgegebenen Nachricht ein Punkt einer elliptischen Kurve zuordnen?
- Wie lassen sich die Vielfachen eines Punktes effizient berechnen?
- Wie funktioniert LENSTRAs Faktorisierungsmethode mit elliptischen Kurven?
- Welche Vor- und Nachteile hat sie gegenüber der $(p-1)$-Methode?
- Wie kann die Primalität einer natürlichen Zahl mit elliptischen Kurven bewiesen werden?
- Was ist ein Morphismus zwischen zwei elliptischen Kurven?
- Wie kann ermöglichst einfach dargestellt werden?
- Nennen Sie Beispiele von Endomorphismen elliptischer Kurven!
- Warum hat der Endomorphismenring stets einen zu $\mathbb{Z}$ isomorphen Unterring?
- Warum ist dies in positiver Charakteristik immer ein echter Unterring?

Abgabe bis zum Dienstag, dem 3. Dezember 2013, um 15.25 Uhr