

宁波大学研究生课程教学大纲

一、课程基本信息

课程中文名称	代数曲线	课程编号			
课程英文名称	Algebraic Curves	总学时	54	学分	3
开课学院	数学与统计学院	开课学期	☐ 春季	☒ 秋季	☐ 全年
课程负责人	曹炜	教学团队成员	周贵松		
适用学科/专业	代数、数论	授课语言	☒ 中文	☐ 全英文	☐ 双语
适用学生	☐ 学术学位博士 ☐ 学术学位直博生 ☐ 学术学位直博生（留学生） ☒ 学术学位硕士 ☐ 专业学位硕士 ☐ 学术学位硕士（留学生） ☐ 专业学位硕士（留学生） ☐ 专业学位硕士（非全日制）				
课程类别	☐ 公共学位课 ☒ 专业学位课 ☐ 公共选修课 ☐ 专业选修课 ☐ 专业补修课 ☐ 必修培养环节 ☐ 其他_____				
主要教学方式 (可多选)	☒ 讲授 ☒ 讨论 ☐ 专题讲座 ☐ 文献研读 ☐ 专题研讨 ☐ 案例分析 ☐ 实验（含上机） ☐ 自学 ☐ 其他_				
考核方式	☒ 考试 ☐ 考查				

二、课程中文简介

域 K 上一条代数曲线是方程 $f(X, Y)=0$, 这里 $f(X, Y)$ 是一个多项式, 其系数在域 K 中。本课程主要讨论有限域上的阿贝尔簇, 椭圆曲线, 超椭圆曲线, 及 Cab 曲线。

三、课程英文简介

An algebraic curve over a field K is an equation $f(X,Y)=0$, where $f(X,Y)$ is a polynomial in X and Y with coefficients in K . This course mainly discusses Abelian varieties over finite fields, Elliptic curves, Hyperelliptic curves, Cab Curves.

四、教学目标

让学生了解有限域上曲线的 Jacobi 簇的点计数和显式算法, 包括 Schoof 的 1 进点计数算法、Kedlaya 和 Denef-Vercauteran 的 p 进算法、Cab 曲线和 zeta 函数的 Jacobi 簇的显式算法等等。

五、教学内容、基本要求及学时分配

1. 各章节主要内容

第一章： 代数曲线与密码概览（An Overview of Algebraic Curves and Cryptography）

主要内容： 基本范例（The basic paradigm）、Diffie-Hellman 决策问题（The Diffie-Hellman decision problem）、群上的限制（Constraints on the group）、有限域上的阿贝尔簇（Abelian varieties over finite fields）、椭圆曲线（Elliptic curves）、统计结果（Statistical results）、高维阿贝尔簇（Abelian varieties of higher dimension）.

重点： Diffie-Hellman 决策问题（The Diffie-Hellman decision problem）、群上的限制（Constraints on

the group)。

难点：有限域上的阿贝尔簇 (Abelian varieties over finite fields)、椭圆曲线 (Elliptic curves)。

课程思政融合点：了解有限域上的阿贝尔簇是如何构造的，了解其产生背景、发展历史和应用背景；理解有限域上的阿贝尔簇在整个科学发展历史中的意义，激发学习热情和追求科学真理的志向。

第二章：Denef-Vercauteren/Kedlaya 算法 (Denef-Vercauteren/Kedlaya Algorithm)

主要内容：主要策略 (Main strategy)、Monsky-Washnitzer 上同调 (Monsky-Washnitzer cohomology)、超椭圆曲线 (Hyperelliptic curves)、数据结构 (Data structures)、将曲线提升到特征 0 的算法 (Algorithm for lifting the curve to characteristic zero)、反演 (Inversion)、K 上 2-幂 Frobenius (The 2-power Frobenius on K)、Frobenius 的特征多项式 (The characteristic polynomial of Frobenius)、运行时间 (Running times)、并行运算 (Parallelization)。

重点：Monsky-Washnitzer 上同调 (Monsky-Washnitzer cohomology)、超椭圆曲线 (Hyperelliptic curves)

难点：Frobenius 的特征多项式 (The characteristic polynomial of Frobenius)。

课程思政融合点：了解 Monsky-Washnitzer 上同调是如何定义的，了解其产生背景、发展历史和应用背景；理解 Monsky-Washnitzer 上同调在整个科学发展历史中的意义，激发学习热情和追求科学真理的志向。

第三章：Cab 曲线 及其 Jacobians 算术 (Cab Curves and Arithmetic on Their Jacobians)

主要内容：Cab 曲线 (The Cab curves)、因子表示下 Jacobian 群的加法 (Addition algorithm for Jacobian group in divisor representation)、理想表示下 Jacobian 群的加法 (Addition algorithm for Jacobian group in ideal representation)。

重点：Cab 曲线 (The Cab curves)。

难点：理想表示下 Jacobian 群的加法。

课程思政融合点：了解 Cab 曲线是如何推广的，了解其产生背景、发展历史和应用背景；理解 Cab 曲线在整个科学发展历史中的意义，激发学习热情和追求科学真理的志向。

第四章：两个 Garcia-Stichtenoth 塔的 Zeta 函数 (The Zeta Functions of Two Garcia-Stichtenoth Towers)

主要内容：Zeta 函数的背景 (Background on zeta functions)、第一个 Garcia-Stichtenoth 塔 (The first Garcia-Stichtenoth tower)、第二个 Garcia-Stichtenoth 塔 (The second Garcia-Stichtenoth tower)、结论 (Conclusion)。

重点：Zeta 函数的背景 (Background on zeta functions)。

难点：第一个 Garcia-Stichtenoth 塔 (The second Garcia-Stichtenoth tower)。

课程思政融合点：了解 Zeta 函数是如何定义的，了解其产生背景、发展历史和应用背景；理解 Zeta 函数在整个科学发展历史中的意义，激发学习热情和追求科学真理的志向。

2. 学时分配表							
章节	标题	教学内容	学时分配				备注
			理论	实验	讨论	其他	
1	代数曲线与密码概览	Diffie-Hellman 决策问题、群上的限制、有限域上的阿贝尔簇、椭圆曲线、高维阿贝尔簇	10		4		
2	Denef-Vercauteren/Kedlaya	Monsky-Washnitzer 上同调、超椭圆曲线、将曲线提升到特征 0 的算法、	10		4		

	算法	K 上 2-幂 Frobenius、Frobenius 的特征多项式、并行运算					
3	Cab 曲线 及其 Jacobians 算术	Cab 曲线、因子表示下 Jacobian 群的加法、理想表示下 Jacobian 群的加法	10		4		
4	两个 Garcia-Stichtenoth 塔的 Zeta 函数	Zeta 函数的背景、第一个 Garcia-Stichtenoth 塔、 第二个 Garcia-Stichtenoth 塔、结论	10		2		
小计			40		14		

六、考核方式及成绩评定方法

- 考核方式：考试
- 成绩评定：满分 100 分，平时 50%（其中课程思政占比 10%），考试 50%
- 考核标准及要求：要求学生掌握基本概念、基本定理，及基本方法，结合平时讨论情况与期末考试成绩，评定最终成绩。

七、本课程创新点（内容、方法等）

理论与应用相结合。

八、教材及主要参考书目、文献与资料

教材至少 1 本，参考书目至少 3 本

类别	教材名称	编者	出版社	版次	出版时间
教材	Algebraic Curves and Cryptography	KUMAR MURTY	高等教育出版社	1	2019
参考书	Algebraic Curves, Algebraic manifolds and Schemes	V.I.Danilo	世界图书出版公司	1	2008
	Algebra	Lang S.	Addison-Wesley	1	1965
	Algebraic Number Theory	Neukirch J.	Springer-Verlag	1	1999

课程负责人（签名）：日期：

学位点负责人（签名）：日期：

所在学院主管领导（签名）（公章）：日期：