Algebraic Geometry

1 Introduction to Algebraic Geometry

1.1 Affine varieties and polynomial rings 1.2 Projective varieties and homogeneous coordinates 1.3 Morphisms and rational maps 1.4 Dimension and degree of varieties

2 Commutative Algebra Foundations

2.1 Rings, ideals, and modules 2.2 Noetherian rings and Hilbert's basis theorem 2.3 Localization and local rings 2.4 Primary decomposition and associated primes

3 Sheaves and Schemes

3.1 Sheaves and sheaf cohomology 3.2 Schemes and their morphisms 3.3 Affine and projective schemes 3.4 Locally ringed spaces and structure sheaves

4 Divisors and Line Bundles

4.1 Weil and Cartier divisors 4.2 Picard group and line bundles 4.3 Linear systems and complete linear systems 4.4 Riemann-Roch theorem for curves and surfaces

5 Cohomology and Intersection Theory

5.1 Čech cohomology and derived functors 5.2 Serre duality and Riemann-Roch theorem 5.3 Chow rings and intersection theory 5.4 Grothendieck-Riemann-Roch theorem

6 Singularities and Resolution

6.1 Singular points and tangent cones 6.2 Blowing up and resolution of singularities 6.3 Normal and Cohen-Macaulay varieties 6.4 Canonical and terminal singularities

7 Curves and Surfaces

7.1 Algebraic curves and their geometry 7.2 Elliptic curves and abelian varieties 7.3 Algebraic surfaces and classification 7.4 Minimal models and birational geometry

8 Moduli Spaces and Invariants

8.1 Moduli spaces of curves and stable curves 8.2 Moduli spaces of vector bundles and sheaves 8.3 Geometric invariant theory (GIT) 8.4 Hilbert schemes and quot schemes

9 Toric Varieties and Polyhedra

10 Toric Varieties and Polyhedral Geometry

9.1 Toric varieties and fans 9.2 Polytopes and their duality 9.3 Toric morphisms and subdivisions 9.4 Toric resolutions and singularities

11 Algebraic Groups and Lie Algebras

10.1 Algebraic groups and group actions 10.2 Lie algebras and exponential map 10.3 Representation theory and characters 10.4 Flag varieties and Schubert calculus

12 Hodge Theory and Complex Geometry

11.1 Hodge structures and Hodge decomposition 11.2 Kähler manifolds and Hodge theory 11.3 Mixed Hodge structures and variations 11.4 Kodaira vanishing and Kodaira dimension

13 Arithmetic Geometry and Number Theory

12.1 Diophantine equations and rational points 12.2 Elliptic curves over finite fields 12.3 Zeta functions and L-functions 12.4 Weil conjectures and étale cohomology

Elliptic Curves

1 Foundations of elliptic curves

1.1 Weierstrass equations 1.2 Group law on elliptic curves 1.3 Elliptic curve point addition 1.4 Elliptic curve point doubling 1.5 Elliptic curve discriminant and j-invariant 1.6 Elliptic curves over various fields

2 Elliptic Curves in Finite Fields

2.1 Finite field arithmetic 2.2 Elliptic curves over prime fields 2.3 Elliptic curves over binary fields 2.4 Elliptic curve point counting 2.5 Hasse's theorem and the Hasse interval 2.6 Supersingular and ordinary elliptic curves

3 Elliptic curve cryptography

3.1 Elliptic curve Diffie-Hellman (ECDH) key exchange 3.2 Elliptic curve digital signature algorithm (ECDSA) 3.3 Elliptic curve integrated encryption scheme (ECIES) 3.4 Pairing-based cryptography 3.5 Security of elliptic curve cryptosystems 3.6 Quantum-resistant elliptic curve cryptography

4 Elliptic curves and number theory

4.1 Elliptic curves over the rational numbers 4.2 Mordell-Weil theorem 4.3 Elliptic curve L-functions 4.4 Birch and Swinnerton-Dyer conjecture 4.5 Elliptic curves and Diophantine equations 4.6 Elliptic curves and the ABC conjecture

5 Elliptic Curves: Complex Number Analysis

5.1 Complex tori and lattices 5.2 Elliptic functions and Weierstrass $\wp$ -function 5.3 Isomorphism between elliptic curves and complex tori 5.4 Elliptic curves and the modular lambda function 5.5 Elliptic curve uniformization 5.6 Elliptic curves and complex multiplication

6 Elliptic Curves: Algebraic Geometry Foundations

6.1 Elliptic curves as algebraic varieties 6.2 Elliptic curves and projective geometry 6.3 Elliptic curves and the Riemann-Roch theorem 6.4 Elliptic curves and the Weierstrass $\wp$ -function 6.5 Elliptic curves and the group structure of the Picard group 6.6 Elliptic curves and the Mordell-Weil theorem

7 Elliptic curves and modular forms

7.1 Modular curves and modular forms 7.2 Elliptic curves and the modular j-invariant 7.3 Elliptic curves and the Taniyama-Shimura conjecture 7.4 Elliptic curves and the Eichler-Shimura relation 7.5 Elliptic curves and the Hecke operators 7.6 Elliptic curves and the Modularity theorem

8 Algorithms for elliptic curves

8.1 Elliptic curve point multiplication algorithms 8.2 Elliptic curve factorization methods 8.3 Schoof's algorithm for point counting 8.4 SEA (Schoof-Elkies-Atkin) algorithm 8.5 Elliptic curve primality proving (ECPP) 8.6 Elliptic curve method for integer factorization

9 Elliptic Curves in Coding Theory

9.1 Goppa codes and algebraic-geometric codes 9.2 Elliptic curves and linear codes 9.3 Elliptic curves and cyclic codes 9.4 Elliptic curves and quantum error-correcting codes 9.5 Elliptic curve cryptography in coding theory 9.6 Elliptic curve-based secret sharing schemes

10 Elliptic Curves in Primality Testing & Factoring

10.1 Elliptic curve primality proving (ECPP) 10.2 Atkin-Morain ECPP 10.3 Lenstra's elliptic curve factorization method 10.4 Montgomery's elliptic curve factorization method 10.5 Elliptic curve method for discrete logarithms 10.6 Suyama's parametrization for ECM