PHD School on
Groebner Bases, Curves, Codes and Cryptography
30 luglio 2012 – 10 agosto 2012

Le lezioni avranno luogo dal lunedì al venerdì dalle 9 alle 13 e dalle 14.30 alle 16.30 in Aula Seminari di Matematica.

Programma previsto per le lezioni tenute dal
Prof. Massimiliano Sala (Università di Trento)

1. Linear codes and Cyclic codes;
2. Groebner Bases and Multivariate Division;
3. Semigroup ideals;
4. Groebner Bases for zero-dimensional ideals;
5. Numerical Semi-groups;
6. Codes from Affine Varieties: Reed-Solomon, generalized Reed-Muller codes, hyperbolic codes, codes from Norm-Trace curves;
7. Order Domains and Algebras: the structure of Order Domain and underlying algebra-morphisms, codes over OD, relation between Goppa codes and OD;
8. n-th root codes: definition, general locator polynomial, stratified ideals, advanced algebraic decoding of cyclic codes.

Programma previsto per le lezioni tenute dal
Prof. Michele Elia (Politecnico di Torino)

1. Diophantine Equations;
2. The additive point group of elliptic curves:
3. Structure and properties over the complex number field.
4. Structure and properties over the rational number field (Mordell's Theorem).
5. The additive point group of elliptic curves:
6. Structure and properties over the finite fields
7. The arithmetic of elliptic curves over finite fields:
8. Iterated sums and duplications over elliptic curves in finite fields
9. Complexity of sums, multiplications, and powers using affine and homogeneous co-ordinates.
10. Discrete logarithms with elliptic curves and Cryptographic applications:
11. Diffie-Hellman and El Gamal public-key schemes via elliptic curves
12. Public and secret parameters, comparison with classic public-key systems.
13. Computational complexity
14. Schoof's algorithm and its applications in
15. Number theory and Diophantine equations
16. Cryptography.
17. Complex multiplication and lattices
18. Factoring

Programma previsto per le lezioni tenute dal
Prof. Ferdinando Mora (Università di Genova)

1. Moeller Algorithm and Auzinger-Stetter matrices;
2. Cerlienco-Mureddu and Variations;
3. Groebner bases for polynomials over a ring;
4. Solving zero-dimensional equations: Trinks algorithm;
5. Lazard characterization of G-bases in R[Y], R a domain (PIR); Gianni-Kalkbrener Theorem;
6. Multiplicity and Macaualay's representation;
7. Solving zero-dimensional equations: Gianni Radical Algorithm, Auzinger-Stetter;
8. Cardinal Conjecture;
9. Macaulay's Trick and Axis-of-Evil Theorem;
10. Le Degré zéro de Moeller

Programma previsto per le lezioni tenute dal
Prof. Massimo Giulietti (Università di Perugia)

1. Preliminaries on Algebraic Curves and Algebraic Geometric Codes. Places and branches of an algebraic curve. Zeros and poles. Divisors. The Genus of an algebraic curve. The Riemann-Roch Theorem. Weierstrass semigroups. Asymptotic bounds for linear codes. Constructions of AG codes. Parameters of AG codes.
2. Automorphisms. Automorphisms of curves. Galois coverings and quotient curves. Hurwitz’s Theorem and Hurwitz’s bound. The different. Automorphisms of AG codes from automorphisms of curves.
3. Stoehr-Voloch Theory. Hermitian invariants and order sequence. Ramification divisor. The Stoehr-Voloch approach to the Hasse-Weil bound.
4. Maximal curves. The Natural Embedding Theorem. Classification results. The spectrum of genera of maximal curves. Serre’s covering result. Maximal curves that are not covered by the Hermitian curve. AG-codes from maximal curves.
5. Applications of Algebraic Curves to Coding Theory and Cryptography through Galois Geometries. Arcs in finite projective spaces and MDS codes. Segre’s Theorem. Plane arcs with small defect and secret sharing schemes. Saturating sets in finite projecitive spaces and covering codes. Complete caps in finite projective spaces and quasi-perfect codes. Complete caps from elliptic curves.

Nel pomeriggio del 9 agosto avrà luogo un seminario tenuto dal
dott. Claudio Fontanari (Università di Trento) con titolo

"A brief introduction to complex algebraic curves"

L'orario per questa lezione è: 14:30-17:30

Programma:

1. A crash course in algebraic geometry.
2. Moduli spaces of curves.
3. Brill-Noether theory.
4. Irreducibility of the Hilbert scheme.

Orari e docenti:

- **Lunedì 30 luglio**
  - 9:00-13:00 Prof. Sala
  - 14:30-16:30 Prof. Elia
- **Martedì 31 luglio**
  - 9:00-11:00 Prof. Sala
  - 11:00-13:00 Prof. Mora
  - 14:30-16:30 Prof. Elia
- **Mercoledì 1 agosto**
  - 9:00-11:00 Prof. Sala
  - 11:00-13:00 Prof. Mora
  - 14:30-16:30 Prof. Elia
- **Giovedì 2 agosto**
  - 9:00-12:00 Prof. Sala
  - 12:00-13:00 Prof. Mora
  - 14:30-16:30 Prof. Elia
- **Venerdì 3 agosto**
  - 9:00-11:00 Prof. Sala
  - 11:00-13:00 Prof. Mora
  - 14:30-16:30 Prof. Elia

- **Lunedì 6 agosto**
    - 9:00-11:00 Prof. Giulietti
    - 11:00-13:00 Prof. Mora
    - 14:30-16:30 Prof. Elia
- **Martedì 7 agosto**
    - 9:00-12:00 Prof. Giulietti
    - 12:00-13:00 Prof. Mora
    - 14:30-16:30 Prof. Elia
- **Mercoledì 8 agosto**
    - 9:00-13:00 Prof. Giulietti
    - 14:30-16:30 Prof. Elia
- **Giovedì 9 agosto**
    - 9:00-13:00 Prof. Giulietti
    - 14:30-17:30 Dott. Fontanari
- **Venerdì 10 agosto**
    - Mini-workshop