Criptografía

Proposed by Fernando Chamizo

Summary

Title. A COURSE ON MODULAR FORMS.

Description and justification of the course. This is a first course focused on the classic theory of modular forms. My favorite references are [CS17] and [DS05], in this order. Although I intend to teach an algebra oriented course, it is important to emphasize the multidisciplinary nature of the topic, as reflected in the contents. Thus, for instance, some topics in complex analysis and number theory will show up naturally. No prerequisites are assumed, though.

As far as I know, the theory of modular forms has not been treated before in our Master courses and, in my opinion, it constitutes a gap in the education of our students. This topic has become crucial in modern number theory and it has broad connections with several subjects appearing in the basic education of any graduate student.

Assessment. Several homework handouts will be proposed along the course. There will also be a non-mandatory final exam.

Language. Although this proposal is written in English, the lectures will be in Spanish if no foreign student request it otherwise.

Contents

1. **Algebra and geometry of the modular group**
   1. The full modular group and the theta group.
   2. Fundamental domains and cusps.
   3. Fuchsian groups, Riemann surfaces and elliptic curves.
   4. Matrix groups and Hill ciphers.
   5. Cryptography of elliptic curves.
2. **Modular forms**
   1. Definition of modular forms and functions.
   2. Dimension formulas.
   3. Eisenstein series and their expansions.
   4. More examples of modular forms and functions.
   5. Algebraic-geometric codes.
3. **Theta functions**
   1. The Jacobi theta function.
   2. Sums of squares.
   3. Representation by quadratic forms.
   4. Remarks on sphere packing after Viazovska.
   5. Cryptosystems and lattices.

4. Hecke operators

1. Definition and basic properties.
2. The Hecke algebra.
3. Summary of the Atkin-Lehner theory.

5. Introduction to the Eichler-Shimura theory

1. L-functions and functional equations.
2. Hecke and Weil inverse theorems.
3. Considerations about Eichler cohomology.

Note: The proposed contents are quite ambitious for a one semester course. Some of the topics could be treated very lightly or diverted to exercises according to the student interests.

References

[CS17] H. Cohen and F. Strömberg. *Modular forms*, volume 179 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2017. A classical approach.

[DS05] F. Diamond and J. Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[Hel02] Y. Hellegouarch. *Invitation to the mathematics of Fermat-Wiles*. Academic Press, Inc., San Diego, CA, 2002. Translated from the second (2001) French edition by L. Schneps.

[Kna92] A. W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.

[Shi94] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[Zag08] D. Zagier. Elliptic modular forms and their applications. In *The 1-2-3 of modular forms*, Universitext, pages 1–103. Springer, Berlin, 2008.