DISCRETE LOGS AND FOURIER COEFFICIENTS

DAVID MIRELES AND STEVEN GALBRAITH

We present a probabilistic polynomial time reduction from the discrete logarithm problem in the multiplicative group $\mathbb{F}_q^\times$, where q denotes a prime number, to the problem of calculating the Fourier coefficients of a Hecke eigenform of level q.

This is done using the recursion formula for the coefficients of an eigenform with associated Dirichlet character χ, using the character to change the discrete log problem from $\mathbb{F}_q^\times$ to the group μ_{q-1} of complex $q-1$-th roots of unity.

It is worth mentioning that Bas Edixhoven has outlined an algorithm [Edix] that would calculate the p-th Fourier coefficient of a given modular form in polynomial time.

Another result related with the reduction presented in this note is in Dennis Charles' thesis [Char], where he proves that being able to compute the values of Ramanujan's τ-function is not more difficult that being able to factor RSA moduli, a difference between his approach and ours is that he considers the problem of calculating the n-th Fourier coefficient for arbitrary n, whereas we restrict ourselves to computing Fourier coefficients for a prime number and the square of a prime number. Charles' result supports a claim by Edixhoven, saying that in order to compute the n-th Fourier coefficient of an eigenform, one must be able to factor n.

References

[Char] Dennis X. Charles, *Computational Aspects of Modular Forms and Elliptic Curves*, PhD thesis, Department of Computer Sciences and Statistics, University of Winsconsin-Madison, 2005.

[Dia-Sh] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Springer-Verlag 2005.

[Edix] B.Edixhoven, *On the computation of coefficients of modular forms.* Notes prepared by John Voight of a talk given during the Computational Arithmetic Geometry workshop at the MSRI, December 2000.

[Lang] S. Lang, *Introduction to Modular Forms*, Springer-Verlag 1995.