EPFL and ETHZ Number Theory Days

ETH Zurich, 17–18 April 2008

Abstracts

COMPUTING THE COEFFICIENTS OF A MODULAR FORM AND RELATED DIOPHANTINE PROBLEMS

BAS EDIXHOVEN (LEIDEN, NL) (PART I)
JEAN-MARC COUVEIGNES (TOULOUSE, F) (PART II)

Let

$$\Delta = q\prod_{n\geq 1}(1-q^n)^{24} = \sum_{n\geq 1}\tau(n)q^n$$

with $q = e^{2\pi iz}$ for $z \in \mathcal{H}$ (the upper half plane). This Δ is a newform of weight 12 for $\mathrm{SL}_2(\mathbb{Z})$. If one has the factorization of n, one can easily compute $\tau(n)$ in terms of the $\tau(p)$ for primes p dividing n. The purpose of these two talks is to describe an algorithm that computes $\tau(p)$ in polynomial time in $\log p$. A first funny application is to compute efficiently the number of vectors of given norm in the Leech lattice of dimension 24.

Deligne has shown the following (in 1969) : For all primes ℓ, there is a unique continuous semisimple representation

$$\rho_\ell\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V_\ell)$$

where V_ℓ is a 2-dimensional $\mathbb{F}_\ell$-vector space, unramified outside ℓ, such that for all primes $p \neq \ell$,

$$\det(1 - x\,\mathrm{Frob}_p\,|V_\ell) = 1 - x\tau(p) + x^2p^{11}$$

in $\mathbb{F}_\ell[x]$. Later Deligne showed also that $|\tau(p)| < 2p^{11/2}$. (Hecke had proved $|\tau(p)| = O(p^6)$, with an explicit constant, and this will suffice for our purposes.) The image of ρ_ℓ is a transitive subgroup of $\mathrm{GL}(V_\ell)$ except for a few known small values of ℓ. An important property of the Galois module V_ℓ is that it can be embedded into the ℓ-torsion of the jacobian J_ℓ of $X_1(\ell)$:

$$V_\ell = \bigcap_{1\leq i\leq(\ell^2-1)/6} \ker\left(T_i - \tau(i), J_\ell(\overline{\mathbb{Q}})[\ell]\right) :$$

We will explain how to compute V_ℓ in time polynomial in ℓ. In fact, we will compute the splitting field of V_ℓ. This number field can be given as an irreducible degree ℓ^2-1 polynomial $P_\ell(x)$ with rational coefficients. This polynomial defines a degree $\ell^2 - 1$ Galois extension of $\mathbb{Q}$ with Galois group the image of ρ_ℓ, a known subgroup of $\mathrm{GL}(V_\ell)$.

A crucial and difficult point will be to give a bound B_ℓ for the logarithmic height of P_ℓ. Arakelov theory applied to modular curves produces such a bound that is a polynomial in ℓ.

Given such a polynomial $P_\ell(x)$ and a prime integer p, algorithmic algebraic number theory provides an algorithm that tells which element in the Galois group is the Frobenius at p. This algorithm runs in time polynomial in the degree ℓ^2-1 and logarithmic height B_ℓ of P_ℓ.

Since B_ℓ is bounded by a polynomial in ℓ, this results in an algorithm that computes $\tau(p)$ modulo ℓ in time polynomial in ℓ. Given a prime p, we can run this algorithm for several small primes ℓ. If the product of these ℓ is bigger than $4p^{\frac{11}{2}}$, we can recover the actual value of $\tau(p)$ thanks to Chinese remainder theorem and Deligne bound.

There remains to explain how to compute $V_\ell \subset J_1(\ell)[\ell]$. Let g_ℓ be the genus of $X_1(\ell)$. Fix a degree g_ℓ rational divisor Ω on $X_1(\ell)$. A class x in V_ℓ is represented by a divisor $D_x - \Omega$ where D_x is effective of degree d. One asks how to compute such torsion divisors.

A first method computes a complex approximation of D_x for every non-zero $x \in V_\ell$. This gives a complex approximation of the (rational) coefficients of P_ℓ. Since we have a good bound on the height of these coefficients, we deduce their exact values in the field $\mathbb{Q}$.

Another method uses q-adic approximations instead of complex approximations.

A reference for this work is

`http://arxiv.org/abs/math/0605244`

by Bas Edixhoven, Jean-Marc Couveignes, Robin de Jong, Franz Merkl, Johan Bosman.