1 LMFDB Workshop at AIM — May 10th, 2016

1.1 Character naming scheme mod ℓ

Mod-l-character-naming-scheme

We need a system of naming Dirichlet characters taking values in finite fields. Ideally we want the system to be compatible with the current system being used in LMFDB, the Conrey naming scheme.

Briefly, in the characteristic zero case: Let p be an odd prime, and let g be the least positive integer which is a primitive root mod p^e. The value $\chi_{p^e}(m,n)$ is determined thusly: Let a, b satisfy $g^a \equiv m \mod p^e$ and $g^b \equiv n \mod p^e$ and let

$$\chi_{p^e}(m,n) = \exp\left(2\pi i \frac{ab}{\phi(p^e)}\right).$$

This scheme requires two choices: (1) A choice of primitive root g mod p^e and (2) a choice of $\phi(p^e)$th root of unity in $\mathbb{C}$. To translate this scheme to the mod ℓ case we need a plan for making an analogous choice for (2). To inherit the nice properties of the Conrey scheme in characteristic zero, we need a system of primitive roots $\{\zeta_N\}_N$ that have the same compatibility property, namely $\zeta_N^d = \zeta_{N/d}$ whenever $d \mid N$.

The Conway polynomials provide such a system of primitive roots in the mod ℓ setting, and this system is used by Sage as well as Magma. To be clear, let $\alpha_{\ell,r}$ be the generator chosen by Sage/Magma when the user calls $\mathbb{F}_{\ell^r}$. This $\alpha_{\ell,r}$ is a root of the Conway polynomial $F_{\ell,r}(X)$, it generates $\mathbb{F}_{\ell^r}^\times$ and the system $\{\alpha_{\ell,r}\}_r$ satisfies the relation

$$\alpha_{\ell,r}^{(\ell^r-1)/(\ell^s-1)} = \alpha_{\ell,s}$$

whenever $s \mid r$.

So here is the choice we make for the system $\{\zeta_{\ell,N}\}_N \subseteq \bar{\mathbb{F}}_\ell$:

$$\zeta_{\ell,N} = \alpha_{\ell,r}^{(\ell^r-1)/N}$$

where r is least so that $N \mid (\ell^r - 1)$.

So we define $\chi_{p^e}(m,n;\ell) = \zeta_{\ell,\phi(p^e)}^{ab}$.