Annotations to document added 12.09.2016 in Warwick (Samuele Anni, Bartosz Naskręcki, Anna Medvedovsky).

1 LMFDB Workshop at AIM — May 10th, 2016 George J. Schaeffer

1.1 Labels for Dirichlet characters modulo ℓ

In order to tabulate entries for modular forms and Galois representations mod ℓ we need a commonly accepted labeling scheme for characters $(\mathbb{Z}/N\mathbb{Z})^\times \to \bar{\mathbb{F}}_\ell^\times$. Such a scheme has already been developed by Conrey (and implemented by LMFDB) for Dirichlet characters $(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$. Our aim here is to adapt the Conrey scheme to mod ℓ Dirichlet characters.

Just to get an idea of what needs to be done, here is how the Conrey scheme over $\mathbb{C}$ works for Dirichlet characters with odd prime power moduli: Let p^e be an odd prime power and let g be the least positive integer whose residue class is a generator of $\cancel{(\mathbb{Z}/p^e\mathbb{Z})^\times}$. Then

(Z/p^f Z)^x for every f >= 1
(equivalently, for f = 2)

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

where $\log_g$ is the discrete logarithm with base g modulo p^e. This definition depends on two choices: (1) The choice of the "least" primitive root g, and (2) The choice of $\varphi(p^e)$th root of unity $e^{2\pi i/\varphi(p^e)}$. It is this second choice that we need to adapt to the mod ℓ setting.

Compatible roots of unity mod ℓ

To adapt the Conrey scheme to mod ℓ Dirichlet characters, we need a *compatible* system of roots of unity in $\bar{\mathbb{F}}_\ell$. That is, for every ℓ we want a sequence $\{\zeta_{\ell,n}\}_n \subseteq \bar{\mathbb{F}}_\ell^\times$ where for each n,

a. If $\ell \nmid n$, $\zeta_{\ell,n}$ is a primitive nth root of unity;

b. $\zeta_{\ell,n}$ is an nth root of unity;

c. For all m, $\zeta_{\ell,mn}^m = \zeta_{\ell,n}$.

The Conway polynomials can be used to build a system of roots of unity with these properties (and Conway polynomials are at least partially impmlemented in SAGE and Magma). Let $\alpha_{\ell,r}$ be a root of the Conway polynomial $F_{\ell,r}$ so that $\alpha_{\ell,r}$ is a primitive (ℓ^r-1)th root of unity in $\bar{\mathbb{F}}_\ell^\times$ and $\alpha_{\ell,r}^{(\ell^r-1)/(\ell^s-1)} = \alpha_{\ell,s}$ for all $s \mid r$.

So long as our choice of ℓ is clear, let $r(n)$ be the least positive integer so that $n \mid \ell^r - 1$, let $v(n) = v_\ell(n)$, and let $\alpha_r = \alpha_{\ell,r}$. Note: r(n) only defined for n prime to ell.

Definition 1. *We define $\{\zeta_{\ell,n}\}_n \subseteq \bar{\mathbb{F}}_\ell^\times$ as follows:*

- *If $\ell \nmid n$ let $\zeta_{\ell,n} = \alpha_{r(n)}^{(\ell^{r(n)}-1)/n}$.*
- *If $\ell \mid n$, let σ be the inverse of $\beta \mapsto \beta^\ell$ and set $\zeta_{\ell,n} = \sigma^{v(n)}(\zeta_{\ell,n/\ell^{v(n)}})$.*

Proposition 2. *If $\ell \nmid n$, then $\zeta_{\ell,n} = \alpha_R^{(\ell^R-1)/n}$ for any R divisible by $r(n)$.*

Proof. This follows from the properties of the Conway roots. If $r \mid R$, we have

$$\alpha_R^{(\ell^R-1)/(\ell^r-1)} = \alpha_r$$

so $\zeta_{\ell,n} = \alpha_r^{(\ell^r-1)/n} = (\alpha_R^{(\ell^R-1)/(\ell^r-1)})^{(\ell^r-1)/n} = \alpha_R^{(\ell^R-1)/n}$ as claimed. $\square$

Proposition 3. *The system $\{\zeta_{\ell,n}\}_n$ as described in the definition above has properties (a–c).*

Proof. (a.) This follows directly from the fact that $\alpha_{\ell,r}$ is a primitive (ℓ^r-1)th root of unity.

(b.) By the first property, $\zeta_{\ell,n/\ell^{v(\ell,n)}}$ is a primitive $(n/\ell^{v(\ell,n)})$th root of unity, so it is an nth root of unity, and its image under $\sigma^{v(\ell,n)}$ is still an nth root of unity.

(c.) Suppose first that $\ell \nmid m'n'$. Let R be divisible by both $r(n')$ and $r(m'n')$. We have

$$\zeta_{\ell,m'n'}^{m'} = (\alpha_R^{(\ell^R-1)/m'n'})^{m'} = \alpha_R^{(\ell^R-1)/n'} = \zeta_{\ell,n'}$$

by the previous proposition. More generally,

$$\begin{aligned}
\zeta_{\ell,mn}^{m} &= \sigma^{v(mn)}(\zeta_{\ell,mn/\ell^{v(mn)}})^{m} \\
&= \sigma^{v(m)}(\sigma^{v(n)}(\zeta_{\ell,mn/\ell^{v(mn)}})^{(m/\ell^{v(m)})})^{\ell^{v(m)}} \\
&= \sigma^{v(n)}(\zeta_{\ell,(m/\ell^{v(m)})(n/\ell^{v(n)})}^{m/\ell^{v(m)}}) \\
&= \sigma^{v(n)}(\zeta_{\ell,n/\ell^{v(n)}}) = \zeta_{\ell,n}
\end{aligned}$$

where the last line follows from applying the $\ell \nmid m'n'$ case above to $m' = m/\ell^{v(m)}$ and $n' = n/\ell^{v(n)}$. $\square$

The label will actually be in the form
ell.p^e.m
instead (highlighting role of ell).

The mod ℓ Conrey scheme — odd prime powers

Let p^e be an odd prime power. The character with label ~~$p^e.m.\ell$~~ is defined by

Moreover, whenever ell divides (p-1), we will have multiple indices defining the same character — see Ex 2 below. We choose least m that works.

Note that [Z/(p^e Z)]^x is a cyclic group, so that it makes sense to work with zeta_{ell, phi(p^e)}.

$$\chi_{p^e}(m,n;\ell) = \zeta_{\ell,\varphi(p^e)}^{\log_g(m)\log_g(n)}$$

where g is the least positive integer that generates $(\mathbb{Z}/p^e\mathbb{Z})^\times$ and $\zeta_{\ell,\varphi(p^e)}$ is the element of $\bar{\mathbb{F}}_\ell$ described in the previous section.

- **Example 1.** There is a modular form

$$f \in \mathbf{S}_1(5^3, \chi; \mathbb{F}_{199^2})$$

that cannot be obtained by reducing a weight 1 modular form over $\mathbb{C}$ (see "Hecke stability and weight 1 modular forms" in Math Z.). The character $\chi : (\mathbb{Z}/5^3\mathbb{Z})^\times \to \mathbb{F}_{199^2}^\times$ is described as the character that maps the least primitive root of $\mathbb{Z}/5^3\mathbb{Z}$ (which is 2) to the element β of $\mathbb{F}_{199^2}$ whose trace is 79 and whose norm is 1; that is, the minimal polynomial of β is $X^2 + 120X + 1$. Note that this only determines β up to conjugacy.

Let us determine the Conrey label for this character. We have $\varphi(5^3) = 100$. Since $199^2 - 1 = 39600$, we set

$$\zeta = \zeta_{199,100} = \alpha^{396}$$

where $\alpha = \alpha_{199,2}$ is a root of the Conway polynomial $F_{199,2}(X)$. The roots of $X^2 + 120X + 1$ are

$$\beta = 157 + 193\alpha = \zeta^{39}$$

and its conjugate $121 + 6\alpha = \zeta^{61}$.

The character χ is determined by $g \mapsto \zeta^{39}$ with $g = 2$, so since $2^{39} \equiv 13 \mod 125$, we have for all $n \in (\mathbb{Z}/5^3\mathbb{Z})^\times$

$$\chi(n) = \chi(g^{\log_g(n)}) = \chi(g)^{\log_g(n)} = \zeta^{39\log_g(n)} = \zeta^{\log_g(13)\log_g(n)} = \chi_{5^3}(13, n; 199).$$

The label for this character would therefore be ~~125.13.199.~~ 199.125.13 Its conjugate would be ~~125.77.199.~~ 199.125.77

- **Example 2.** When $\ell \mid \varphi(p^e)$ a single character $\chi = \chi_{p^e}(m, -; \ell)$ may have multiple labels $m \in (\mathbb{Z}/\varphi(p^e)\mathbb{Z})^\times$. This may seem like a drawback to our scheme, possibly requiring us to make a further decision (either always take the least index or create duplicate pages for labels picking out the same character), but it actually allows for extra compatibility with reduction modulo ℓ (details later).

  Here is an example. Let $\chi : (\mathbb{Z}/43\mathbb{Z})^\times \to \mathbb{F}_7^\times$ be the character determined by $3 \mapsto 3$ ($g = 3$ is the least primitive root mod 43). We have

  $$\zeta_{7,42} = \sigma(\zeta_{7,6}) = \sigma(3) = 3$$

  See last page for field of definition of mod-ell Dirichlet characters with modulus N. In this case (N = 43) all characters are already defined over F7.

  So

  $$\chi(n) = \zeta_{7,42}^{\log_g(n)} = \chi_{43}(3, n; 7)$$

  but also

  $$\chi_{43}(37, n; 7) = \zeta_{7,42}^{\log_g(37)\log_g(n)} = (\zeta_{7,42}^{\log_g(n)})^7 = \zeta_{7,42}^{\log_g(n)} = \chi_{43}(3, n; 7)$$

  ~~So the exact same character would be labeled by 43.3.7 and 43.37.7.~~

So both m = 37 and m = 3 work. For the purpose of LMFDB labels, we choose the *least* m that gives this chi.

The mod ℓ Conrey scheme — general moduli

In this case, any m in {3, 5, 12, 19, 20, 33, 37} gives this chi, so chi = 7.43.3.

As in the characteristic zero case, if M and N are relatively prime odd moduli, we take

$$\chi_{MN}(m, n; \ell) = \chi_M(m, n; \ell) \cdot \chi_N(m, n; \ell)$$

See last page for more about determining the m in the label given a particular character, or for “reducing” a particular character from characteristic zero to characteristic ell.

Now, let

$$\chi_2(1, n; \ell) = \begin{cases} 0 & \text{if } n \text{ is even,} \\ 1 & \text{if } n \text{ is odd.} \end{cases}$$

and

$$\chi_4(1, n; \ell) = \chi_2(1, n; \ell)$$

and

$$\chi_4(3,n;\ell) = \begin{cases} 0 & \text{if } n \text{ is even, and} \\ (-1)^{(n-1)/2} & \text{if } n \text{ is odd.} \end{cases}$$

Finally, suppose $f \geq 3$. There exist a, b such that $m \equiv \epsilon_a 3^a \mod 2^f$ and $n \equiv \epsilon_b 3^b \mod 2^f$ where $1 \leq a, b \leq 2^{f-2}$ and $\epsilon_a, \epsilon_b = \pm 1$. We define

$$\chi_{2^f}(m,n;\ell) = \zeta_{\ell,8}^{(1-\epsilon_a)(1-\epsilon_b)} \zeta_{\ell,2^{f-2}}^{ab}$$

Note: we have

$$\zeta_{\ell,8}^{(1-\epsilon_a)(1-\epsilon_b)} = \begin{cases} \zeta_{\ell,2} = -1 & \text{if } \epsilon_a = \epsilon_b = -1, \text{ and} \\ 1 & \text{otherwise.} \end{cases}$$

To complete the labeling scheme, if $N = 2^f M$ with M odd, then

$$\chi_N(m,n;\ell) = \chi_{2^f}(m,n;\ell) \cdot \chi_M(m,n;\ell).$$

We now can find the character attached to a particular label.

- What is the character with label $168.19.71$? It is the product of the characters with labels $8.19.71 = 8.3.71$, $3.19.71 = 3.1.71$, and $7.5.71$.

I'll stop correcting the labels here, but you get the idea.

  We have $3 \equiv +1 \cdot 3^1 \mod 8$, so

  $$\chi_8(3,n;71) = \zeta_{71,2}^b = (-1)^b$$

  where b satisfies $n \equiv \pm 3^b \mod 8$. In SAGE this is the character with label

  ```
  DirichletGroup(8,GF(71))[2]
  ```

  The character $\chi_3(1,n;71)$ is trivial. Its SAGE label is

  ```
  DirichletGroup(3,GF(71))[0]
  ```

  For the last component,

  $$\chi_7(5,n;71) = \zeta_{71,6}^{5\log_3(n)}$$

  where the discrete log is modulo 7. Now,

  $$\zeta_{71,6} = 39 + 68\alpha$$

  where $\alpha = \alpha_{71,2}$. The character with index 1 in SAGE is given by $3 \mapsto \zeta_{71,6}$, and the character with index 5 is its 5th power, so the index of $7.5.71$ is

  ```
  DirichletGroup(7,GF(71**2,'a'))[5]
  ```

  So

  $$\chi_{168}(19,-;71) : (\mathbb{Z}/168\mathbb{Z})^\times \to \mathbb{F}_{71^2} = \mathbb{F}_{71}(\alpha)^\times : \begin{cases} 127 \mapsto 1 \\ 85 \mapsto 70 \\ 113 \mapsto 1 \\ 73 \mapsto 33 + 3\alpha \end{cases}$$

  This is the character

  ```
  DirichletGroup(168,GF(71**2,'a'))[42]
  ```

  in SAGE.

Going from SAGE index to label

When p is odd, the sage Character χ given by

```
DirichletGroup(p∧e,GF(l∧r,'a'))[1]
```

maps $g \mapsto \alpha_{\ell,r}^{(\ell^r-1)/\gcd(\varphi(p^e),\ell^r-1)}$. (Provided SAGE is using the Conway polynomial for that particular finite field. This is not guaranteed.) The character with SAGE index i in this case is χ^i. We have

$$\begin{aligned}\alpha_{\ell,r}^{(\ell^r-1)/\gcd(\varphi(p^e),\ell^r-1)} &= \zeta_{\ell,\gcd(\varphi(p^e),\ell^r-1)} \\ &= \zeta_{\ell,\varphi(p^e)}^{\varphi(p^e)/\gcd(\varphi(p^e),\ell^r-1)}\end{aligned}$$

So since

$$\chi : g \mapsto \zeta_{\ell,\varphi(p^e)}^{\varphi(p^e)/\gcd(\varphi(p^e),\ell^r-1)}$$

It is the character with Conrey label $m = g^{\varphi(p^e)/\gcd(\varphi(p^e),\ell^r-1)}$. χ^i is the character with label $g^{i\varphi(p^e)/\gcd(\varphi(p^e),\ell^r-1)}$. This is enough to retrieve the Conrey label of any mod ℓ character with odd modulus, knowing its SAGE index.

- **Example 3.** Let's check that this works for the SAGE character $(\mathbb{Z}/7\mathbb{Z})^\times \to \mathbb{F}_{71^2}$ with index 5 (from a previous example we know this is $7.5.71$).

  The SAGE character $(\mathbb{Z}/7\mathbb{Z})^\times \to \mathbb{F}_{71^2}$ with index 5 has label

  $$m = 3^{5\varphi(7)/\gcd(\varphi(7),71^2-1)} \equiv 3^5 \equiv 5 \mod 7$$

- **Example 4.** What about the SAGE character $(\mathbb{Z}/203\mathbb{Z})^\times \to \mathbb{F}_5$ with index 1—this is the quadratic character with conductor 7.

  The quadratic character $(\mathbb{Z}/7\mathbb{Z})^\times \to \mathbb{F}_5^\times$ has label

  $$m = 3^{\varphi(7)/\gcd(\varphi(7),5-1)} = 3^3 \equiv 6 \mod 7$$

  (as expected).

  The trivial character $(\mathbb{Z}/29\mathbb{Z})^\times \to \mathbb{F}_5^\times$ has SAGE index $i = 0$ so its label is

  $$m = 2^{0\varphi(29)/\gcd(\varphi(29),5-4)} \equiv 1 \mod 29$$

  So our character is

  $$\chi_7(6, -; 5) \cdot \chi_{29}(1, -; 5) = \chi_{203}(146, -; 5)$$

  with label $203.146.5$.

Going from character to label

- **Example 5.** Consider the character $\chi : (\mathbb{Z}/360\mathbb{Z})^\times \to \mathbb{F}_{43}^\times$ determined by

$$\chi : \begin{cases} 271 \mapsto 42 \\ 181 \mapsto 42 \\ 281 \mapsto 37 \\ 217 \mapsto 1 \end{cases}$$

  Restricting the character mod 8 yields the character determined by $5, 7 \mapsto -1$, which is (I think) $\chi_8(7, -; 43)$.

  Mod 9 this character is determined by $2 \mapsto 37 = \zeta_{43,6}$, so $\chi_9(2, -; 43)$.

  Mod 5 this character is trivial, so $\chi_5(1, -; 43)$.

  To find the label of the product of these characters, we CRT up to get $191 \mod 360$ as our index. This is the character $360.191.43$.

Compatibility with the characteristic 0 labeling

Let $\zeta_{0,n} = e^{2\pi i/n}$. There is a reduction map

$$\psi_\ell : \mathbb{Z}[\zeta_{0,n}] \to \mathbb{F}_\ell(\zeta_{\ell,n})$$

sending $\zeta_{0,n} \mapsto \zeta_{\ell,n}$. This reduction map can be obtained as reduction modulo a carefully chosen prime $\mathfrak{l}$ of $\mathbb{Z}[\zeta_{0,n}]$ over ℓ such that the minimal polynomial of $\zeta_{0,n} + \mathfrak{l}$ is the same as the minimal polynomial of $\zeta_{\ell,n}$.

Now, if $\chi : (\mathbb{Z}/p^e\mathbb{Z})^\times \to \mathbb{C}^\times$ is given by the Conrey label $p^e.m.0$, then $\psi_\ell \circ \chi$ is the character with label $p^e.m.\ell$.

1. Which m do we choose? For Dirichlet characters mod N, the Conrey scheme a priori allows any prime relatively prime to N. Whenever ell divides phi(N), we have multiple values of m giving the same character. We always choose the least one.
*** In particular, suppose N = p^e is an odd prime power with Conrey generator g, and z = zeta_{phi(p^e)} is in F-ell-bar. Let a be the logarithm of m base g: that is, g^a = m. Then the characteristic ell LMFDB label becomes ell.p^e.M, where
M = min { g^{a#} over all a# in (Z/N Z)* satisfying z^a = z^{a#} in F-ell-bar}.
Indeed, the character with label ell.p^e.{m#} maps g to z^{a#}, where a# is defined by g^(a#)= m#.
(Note that g^(a#) is a priori defined modulo N, but for the purposes of defining M we view it as an integer in [0..N).)
*** In general, we want M to be the minimum m in [0..N) prime to N that defines the correct character modulo ell. The definition of the correct character should be checked separately on the generators of (Z/N)* (there will be one generator for each odd prime power dividing phi(N), one generator for 2 if 4 divides phi(N) exactly, and two generators for 2 if 8 divides phi(N).

2. The field of definition of the group of Dirichlet characters modulo N to F-ell-bar.
For each p prime not equal to ell, let the p-primary component of (Z/NZ)* be
(Z/p^{e_1}) x (Z/p^{e_2}) x …. x (Z/p^{e_s}),
where the e_i are not necessarily distinct. Let e = max{e_i}. Let r be minimal such that p^e divides (ell^r - 1). At this point, we know that zeta_{p^e} is defined over F_{ell^n}.
Finally, let R = lcm of the r's that one gets over all the primes (except ell) that divide phi(N).
Then the Dirichlet characters modulo N over F-ell-bar are defined over F_{ell^R}.

Example: N = 29x43, and ell = 13.
Then (Z/(29x43)Z)* = (Z/29)* x (Z/43)* = (Z/4)x(Z/7)x(Z/2)x(Z/3)x(Z/7). We need to find the smallest power R of 13 so that 4*3*7 divides 13^R - 1. R = 2 works.