Polynomials for primitive extensions of $\mathbb{Q}_p$

David P. Roberts
University of Minnesota, Morris

Advance warning: I took the workshop directions *please come with some half-baked ideas to share* to heart!

Note: The topic of this talk arose in connection with joint work with Fred Diamond and Lassina Dembélé. This work relates p-adic ramification of number fields with weights of corresponding Hilbert modular forms. On the number field side, primitive p-adic fields enter prominently. It is necessary to thoroughly distinguish these primitive fields from each other, because similar-looking p-adic fields can correspond to different weights.

The Problem. Let $q = p^f$ be a prime power and $s \in \mathbb{Z}_{\geq 1}$.

Definition. *$A_{q,s}$ is the set of isomorphism classes of primitive degree q extensions of $\mathbb{Q}_p$ with discriminant p^{q-1+s}.*

Examples. (Weil, Exercises dyadiques):

$$\begin{aligned} A_{4,1} &= \{\mathbb{Q}_2[x]/(x^4+2x+2)\}, \\ A_{4,3} &= \{\mathbb{Q}_2[x]/(x^4+2x^3+2x^2+2)\}, \\ A_{4,5} &= \{\mathbb{Q}_2[x]/(x^4+4x+2), \\ &\qquad \mathbb{Q}_2[x]/(x^4+4x^2+4x+2)\}, \\ \text{else } A_{4,s} &= \emptyset. \end{aligned}$$

Problem. *Write down a complete irredundant set of polynomials for each $A_{q,s}$.*

The case $f = 1$ was solved by Amano, the primitivity condition being vacuous; we'll exclude it here.

Some context and definitions. There are totally ramified degree q extensions of $\mathbb{Q}_p$ of discriminant p^{q-1+s} exactly when s is in a certain subset of $\{1, \ldots, fp^f\}$. For $q \in \{4, 8, 9\}$, these sets are as follows:

$$q = 4: \quad \begin{array}{cccc} \boxed{1} & & \boxed{\mathit{3}} & \\ \boxed{5} & 6 & 7 & 8, \end{array}$$

$$q = 8: \quad \begin{array}{cccccccc} \boxed{1} & & \boxed{3} & & \boxed{5} & & \boxed{\mathit{7}} & \\ \boxed{9} & 10 & \boxed{11} & & \boxed{13} & 14 & 15 & \\ 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24, \end{array}$$

$$q = 9: \quad \begin{array}{ccccccccc} \boxed{1} & \boxed{2} & & \boxed{\mathit{4}} & \boxed{5} & & \boxed{7} & \boxed{\mathit{8}} & \\ \boxed{10} & \boxed{11} & 12 & 13 & 14 & 15 & 16 & 17 & 18. \end{array}$$

Primitive extensions can only exist when

$$s \leq p^f + p^{f-1} + \cdots + p$$

and $\mathrm{ord}_p(s) = 0$, as boxed. We say s is of *Type 1* or *Type 2* according to whether $s < q$ or $s > q$. We say that s is *generic* if its reduction $\overline{s}$ to $\mathbb{Z}/(q-1)$ is in an orbit under multiplication by p of full size f. To simplify, we exclude here the non-generic case, thus the s in italics above.

Conjectural solution in Case 1. Given $s < q$, define an *exponent set* $E(q,s)$ as follows. Write s as an f-digit number in base p, taking all digits from $\{0,\ldots,p-1\}$ as usual. For $j = 0$, ..., $f-1$, round down to $\lfloor s \rfloor_j$ by dropping the j least significant digits. Simultaneously, rotate the f-digit number s digitwise, j places to the right, to obtain $R_j(s)$. Then

$$E(q,s) = \{\lfloor s \rfloor_j : R_j(s) \le s\}.$$

Conjecture. *When $s < q$, a complete irredundant set of polynomials for $A_{q,s}$ is*

$$x^q + \sum_{e \in E(q,s)} p a_e x^e + p$$

with $a_e \in \{0,\ldots,p-1\}$ and $a_s \neq 0$.

Note: $pa_s x^s$ functions as a suitably leading term, ensuring that the discriminant is indeed p^{q-1+s}.

Example 1A: $(q,s) = (81, 59)$:

j	$\lfloor s \rfloor_j$			$R_j(s)$	Keep?
0	*2012*	$=$	59	*2012*	✓
1	*2010*	$=$	57	*2201*	
2	*2000*	$=$	54	*1220*	✓
3	*2000*	$=$	54	*0122*	(✓)

So polynomials for $A_{81,59}$ should be

$$x^{81} + 3ax^{59} + 3bx^{54} + 3,$$

with $a \in \{1, 2\}$ and $b \in \{0, 1, 2\}$.

Example IB: $(q,s) = (81, 73)$:

j	$\lfloor s \rfloor_j$			$R_j(s)$	Keep?
0	*2201*	$=$	73	*2201*	✓
1	*2200*	$=$	72	*1220*	✓
2	*2200*	$=$	54	*0122*	✓
3	*2000*	$=$	54	*2012*	(✓)

So polynomials for $A_{81,73}$ should be

$$x^{81} + 3ax^{73} + 3bx^{72} + 3cx^{54} + 3,$$

with $a \in \{1, 2\}$ and $b, c \in \{0, 1, 2\}$.

Conjectural solution in Case 2. Given $s > q$, now define $E(q,s)$ as follows. Again write s as an f-digit number in base p, but now requiring all digits to be in $\{1, \ldots, p\}$. For $j = 0, \ldots, f-1$, again round down to $\lfloor s \rfloor_j$ by dropping the j least significant digits. Again simultaneously rotate s digitwise j places rightwards to obtain $R_j(s)$. Let

$$\begin{aligned} \tilde{E}(q,s) &= \{s+1\} \cup \\ &\quad \{\lfloor s \rfloor_j > q : R_j(s) \leq s \text{ or } s | R_j(s)\}. \end{aligned}$$

Then $E(q,s) = \{k - q : k \in \tilde{E}(q,s)\}$.

Conjecture. *When $s > q$, a complete irredundant set of polynomials for $A_{q,s}$ is*

$$x^q + \sum_{e \in E(q,s)} p^2 a_e x^e + p,$$

with $a_e \in \{0, \ldots, p-1\}$ and $a_{s-q} \neq 0$.

Note: Now $p^2 a_{s-q} x^{s-q}$ is the term which ensures that the discriminant is p^{q-1+s}.

Example 2A. $(q, s) = (81, 97)$.

j	$\lfloor s \rfloor_j$				e	$R_j(s)$	Keep?
			98	$\to$	17		✓
0	*3121*	=	97	$\to$	16	*3121*	✓
1	*3120*	=	96	$\to$	15	*1312*	✓
2	*3100*	=	90	$\to$	9	*2131*	✓
3	*3000*	=	81	$\to$	0	*1213*	

So polynomials for $A_{81,97}$ should be

$$x^{81} + 9ax^{17} + 9bx^{16} + 9cx^{15} + 9dx^9 + 3,$$

with $b \in \{1, 2\}$ and a, c, $d \in \{0, 1, 2\}$.

Example 2B. $(q, s) = (32, 45)$.

j	$\lfloor s \rfloor_j$				e	$R_j(s)$	Keep?
			46	$\to$	14		✓
0	*12221*	=	45	$\to$	13	*12221*	✓
1	*12220*	=	44	$\to$	12	*11222*	✓
2	*12200*	=	40	$\to$	8	*21122*	✓
3	*12000*	=	32	$\to$	0	*22112*	

So polynomials for $A_{32,45}$ should be

$$x^{32} + 4ax^{14} + 4bx^{13} + 4cx^{12} + 4dx^8 + 2.$$

with $b = 1$ and a, c, $d \in \{0, 1\}$.

Concluding Remarks. 1. Decompose $A_{q,s} = \coprod_{j=1}^{p-1} A_{q,s,j}$ according to the leading coefficients $j = a_e$ in the conjectures. The spaces $A_{q,s,j}$ with $\overline{s} \in \mathbb{Z}/(q-1)$ in the same orbit under multiplication by p should fit together to form f-dimensional projective spaces:

q	s	Polys	#
4	1	$x^4 + 2x + 2$	1
	5	$x^4 + 4ax^2 + 4x + 2$	2
8	1	$x^8 + 2x + 2$	1
	9	$x^8 + 4ax^2 + 4x + 2$	2
	11	$x^8 + 4ax^4 + 4x^3 + 4bx^2 + 2$	4
8	3	$x^8 + 2x^3 + 2$	1
	5	$x^8 + 2x^5 + 2ax^4 + 2$	2
	13	$x^8 + 4ax^6 + 4x^5 + 4x^4 + 2$	4
9	1	$x^9 + 3jx + 3$	1
	11	$x^9 + 9ax^3 + 9jx^2 + 3$	3
9	2	$x^9 + 3jx^2 + 3$	1
	10	$x^9 + 9ax^2 + 9jx + 3$	3
9	5	$x^9 + 3jx^5 + 3$	1
	7	$x^9 + 3jx^7 + 3ax^6 + 3$	3

In the application with Diamond and Dembélé, the projective spaces arise naturally from certain H^1, and their pavings by $\mathrm{ord}_p(D)$ form a secondary structure.

2. The conjecture has an analog when one replaces p by any other choice of uniformizer. I think the ambiguities associated with this change are also seen on the automorphic side.

3. One should be able to describe the space of *all* Eisenstein polynomials belonging to a given field, as a suitable neighborhood of our preferred point.

4. A possible proof would involve the canonical Galois extension F of $\mathbb{Q}_p$ with inertial index f and ramification deqree $q-1$, and then abelian degree p extensions L of F. These L and the primitive K of the main talk are related by resolvent constructions.

5. Besides removing our standing genericity-of-s assumption, it would be desirable to replace $\mathbb{Q}_p$ by an arbitrary p-adic base field.