2016-01-25-lecture

William A. Stein

1/25/2016

Contents

1 January 25, 2016: Explicitly computing the mod-5 representation attached to 11a

1.1 William Stein

1.2 Motivating problem: Galois representations attached to elliptic curves

As a motivating problem for explicitly computing (1) prime factorizations, (2) rings of integers, (3) p-maximal orders, and (4) maps to and from finite fields, we will compute Galois representations attached to elliptic curves.

Let E be an elliptic curve over and let ℓ be a prime of good reduction.

Consider the group $E[\ell] = E()$ of elements of order dividing ℓ. Fix a basis for $E[\ell] =_\ell \oplus_\ell$.

The mod ℓ Galois representation attached to E is the homomorphism

$$\rho_{E,\ell} : G_{\rightarrow} \mathrm{GL}(E[\ell])$$

got by letting the Galois group G act on $E[\ell]$.

The number field $K = (E[\ell])$ got by adjoining all x and y coordinates of elements of $E[\ell]$ to is the fixed field in $^{-}$for the subgroup $\ker(\rho_{E,\ell})$. The field K is ramified at most at ℓ and the primes of bad reduction for E. Note that K is a Galois extension.

Quick Exercise: Give a quick example of E and ℓ in which K is unramified at all primes?

Let p be a prime number. Let R be the ring of integers of K and let P be a prime of R over p, which means that $pR = P^e \cdots$ other prime ideals. The map $R \to R/P =_P$ induces a map from R to the finite field $_P$, of characteristic p.

Let D_P be the decomposition group of P in $\mathrm{Gal}(K/)$, i.e., the subgroup of automorphisms that send P to itself, and let I_P be the inertia group. We have an exact sequence

$$1 \to I_P \to D_P \to \mathrm{Gal}(_P/_p) \to 1$$

Let $\mathrm{Frob}_P \in D_P$ be a choice of lift of $x \mapsto x^p$. Note that Frob_P is well defined when $I_P = 1$, which is the case for all unramified primes (in particular, for $p \nmid \ell N_E$).

For a prime $p \nmid N_E$ of good reduction for E, let $a_p = p + 1 - \#E(_p)$.

Theorem: For $p \nmid \ell N_E$, the characteristic polynomial of $\rho_{E,\ell}(\mathrm{Frob}_P)$ is $X^2 - a_p X + p$.

Goal: Understand the details of how to explicitly compute the matrix $\rho_{E,\ell}(\mathrm{Frob}_P)$. Use the above theorem as a consistency check.

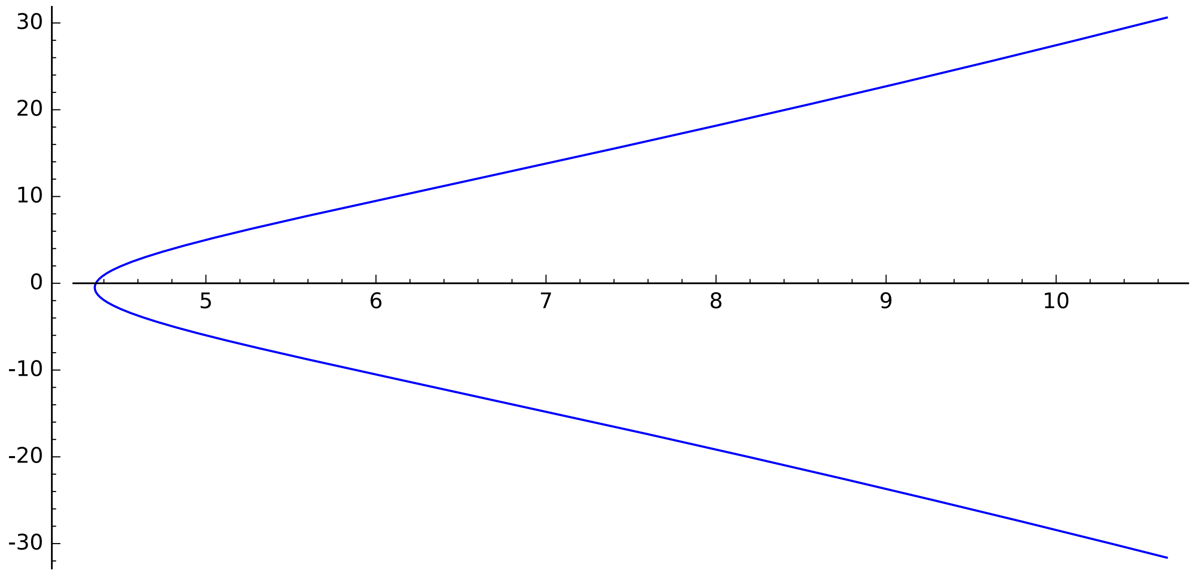
Rest of today: compute one example. Later: talk about how to factor p, compute the map $R \to R/P$ explicitly, etc.

We will compute with the mod-5 representation attached to the elliptic curve 11a (this is the one we were thinking about at lunch last week in response to Ralph Greenberg's question.)

```
E = EllipticCurve('11a')
ell = 5
p = 2
show(E)
```

$y^2 + y = x^3 - x^2 - 10x - 20$

```
plot(E)
```




```
N = N_E = E.conductor()
N
```

11

Let's compute $K = (E[5])$.

```
# Polynomial with roots the x-coordinates of the 5-torsion points
f = E.division_polynomial(5)
show(factor(f))
```

$$(5)\cdot(x-16)\cdot(x-5)\cdot(x^2+x-\frac{29}{5})\cdot(x^4+x^3+11x^2+41x+101)\cdot(x^4+15x^3+120x^2+200x+155)$$

```
# all the x-coordinates of elements of E[5]
x_coords = f.roots(ring=QQbar, multiplicities=False)
x_coords
```

```
[-2.959674775249769?, 1.959674775249769?, 5, 16, -6.545084971874737? -
7.106423590645660?*I, -6.545084971874737? + 7.106423590645660?*I, -1.927050983124843? -
1.677599044300515?*I, -1.927050983124843? + 1.677599044300515?*I, -0.9549150281252629? -
0.8652998037182486?*I, -0.9549150281252629? + 0.8652998037182486?*I, 1.427050983124843? -
3.665468789467727?*I, 1.427050983124843? + 3.665468789467727?*I]
```

```
# make E_QQbar, and construct corresponding points
Ebar = E.change_ring(QQbar)
points = [Ebar.lift_x(x) for x in x_coords]
points
```

```
[(-2.959674775249769? : -0.500000000000000000? + 4.983845452504573?*I : 1),
(1.959674775249769? : -0.500000000000000000? + 5.971707000979661?*I : 1), (5 : 5 : 1), (16
: 60 : 1), (-6.545084971874737? - 7.106423590645660?*I : 28.84345884812358? -
9.82083586381824?*I : 1), (-6.545084971874737? + 7.106423590645660?*I : 28.84345884812358?
+ 9.82083586381824?*I : 1), (-1.927050983124843? - 1.677599044300515?*I :
2.354101966249685? - 0.6407858154284560?*I : 1), (-1.927050983124843? +
1.677599044300515?*I : 2.354101966249685? + 0.6407858154284560?*I : 1),
(-0.9549150281252629? - 0.8652998037182486?*I : 0.3434588481235805? + 3.130684100311236?*I
: 1), (-0.9549150281252629? + 0.8652998037182486?*I : 0.3434588481235805? -
3.130684100311236?*I : 1), (1.427050983124843? - 3.665468789467727?*I : 3.354101966249685?
+ 9.59632187552845?*I : 1), (1.427050983124843? + 3.665468789467727?*I :
3.354101966249685? - 9.59632187552845?*I : 1)]
```

```
# this are exactly half (up to sign) of the nonzero elements of E\
    [5]:
len(points)
```

```
12
```

```
# explicitly, this is E5:
E5 = [Ebar(0)] + points0 + [-P for P in points0]
len(E5)
```

```
25
```

I don't know how in Sage, given a set of elements of QQbar, to get the number field they generate easily.

But we can just take a random linear combination and it is likely to give us that field.

Then we can do a computation to check if it worked.

```
# compute a random linear combination of the coordinates of the \
    elements of E5
set_random_seed(1)
r = 0
```

```
for P in E5:
    r += ZZ.random_element(0,5)*P[0] + ZZ.random_element(0,5)*P[1]
r
```

```
23.51497367912013? + 30.20524565041611?*I
```

```
%time r.minpoly()
```

```
x^4 + 113*x^3 + 2952/5*x^2 - 1957904/25*x + 1218275771/125
CPU time: 0.03 s, Wall time: 0.04 s
```

```
# So it appears in this case that taking one of those degree four \
   factors of the div poly will work.
K.<a> = NumberField(factor(f)[-2][0])
K
```

```
Number Field in a with defining polynomial x^4 + x^3 + 11*x^2 + 41*x + 101
```

```
# Let's double check: yep -- it works.
EK = E.change_ring(K)
EK.torsion_subgroup()
```

```
Torsion Subgroup isomorphic to Z/5 + Z/5 associated to the Elliptic Curve defined by y^2 +
y = x^3 + (-1)*x^2 + (-10)*x + (-20) over Number Field in a with defining polynomial x^4 +
x^3 + 11*x^2 + 41*x + 101
```

```
K.disc().factor()
```

```
5^3
```

```
# Compute the ring of integers:
R = K.maximal_order()
R
```

```
Maximal Order in Number Field in a with defining polynomial x^4 + x^3 + 11*x^2 + 41*x +
101
```

These are generators as a -module:

```
show(R.basis())
```

$$\left[\frac{3}{121}a^3 + \frac{62}{121}a^2 + \frac{2}{121}a + \frac{1}{121}, \frac{7}{11}a^3 + \frac{1}{11}a, a^2, a^3\right]$$

```
# Let's choose a better representation, since those 11's in the \
   denoms are ugly.
K.optimized_representation()
```

```
(Number Field in a2 with defining polynomial x^4 - x^3 + x^2 - x + 1, Ring morphism:
  From: Number Field in a2 with defining polynomial x^4 - x^3 + x^2 - x + 1
  To:   Number Field in a with defining polynomial x^4 + x^3 + 11*x^2 + 41*x + 101
  Defn: a2 |--> 1/11*a^2 + 8/11, Ring morphism:
  From: Number Field in a with defining polynomial x^4 + x^3 + 11*x^2 + 41*x + 101
  To:   Number Field in a2 with defining polynomial x^4 - x^3 + x^2 - x + 1
  Defn: a |--> a2^3 - 4*a2^2 + 2*a2 - 2)
```

```
g = K.optimized_representation()[0].defining_polynomial()
g
```

x^4 - x^3 + x^2 - x + 1

```
K.<a> = NumberField(g); K
```

Number Field in a with defining polynomial x^4 - x^3 + x^2 - x + 1

```
factor(K.disc())
```

5^3

```
# Compute the ring of integers:
R = K.maximal_order()
show(R.basis())
```

$[1, a, a^2, a^3]$

```
EK = E.change_ring(K)
T = EK.torsion_subgroup(); T
```

Torsion Subgroup isomorphic to Z/5 + Z/5 associated to the Elliptic Curve defined by y^2 + y = x^3 + (-1)*x^2 + (-10)*x + (-20) over Number Field in a with defining polynomial x^4 - x^3 + x^2 - x + 1

```
list(T)
```

[(0 : 1 : 0), (16 : 60 : 1), (5 : 5 : 1), (5 : -6 : 1), (16 : -61 : 1), (7*a^3 - 2*a^2 + 4*a - 7 : 7*a^3 - 13*a^2 - 7*a - 18 : 1), (a^3 + a^2 + 3*a - 1 : 9*a^3 - 2*a^2 + 5*a - 5 : 1), (-11/5*a^3 + 11/5*a^2 + 3/5 : 22/5*a^3 - 11/5*a^2 + 33/5*a - 19/5 : 1), (-4*a^3 + 2*a^2 - 3*a + 2 : 3*a^3 + 4*a^2 + 5*a - 1 : 1), (-2*a^3 - 3*a^2 - 4*a - 3 : -20*a^3 + 14*a^2 - 7*a + 24 : 1), (2*a^3 + a^2 - 2*a : 4*a^3 - 9*a^2 + 7*a - 5 : 1), (-3*a^3 + 7*a^2 - 5*a : 14*a^3 - 7*a^2 - 6*a + 10 : 1), (-2*a^3 - 2*a^2 + 5*a - 5 : -13*a^3 + 20*a^2 - 6*a - 5 : 1), (a^3 - 4*a^2 + 2*a - 2 : -2*a^3 - 3*a^2 + 7*a - 3 : 1), (11/5*a^3 - 11/5*a^2 - 8/5 : -11/5*a^3 - 22/5*a^2 + 11/5*a - 8/5 : 1), (2*a^3 + a^2 - 2*a : -4*a^3 + 9*a^2 - 7*a + 4 : 1), (11/5*a^3 - 11/5*a^2 - 8/5 : 11/5*a^3 + 22/5*a^2 - 11/5*a + 3/5 : 1), (a^3 - 4*a^2 + 2*a - 2 : 2*a^3 + 3*a^2 - 7*a + 2 : 1), (-2*a^3 - 2*a^2 + 5*a - 5 : 13*a^3 - 20*a^2 + 6*a + 4 : 1), (-3*a^3 + 7*a^2 - 5*a : -14*a^3 + 7*a^2 + 6*a - 11 : 1), (7*a^3 - 2*a^2 + 4*a - 7 : -7*a^3 + 13*a^2 + 7*a + 17 : 1), (-2*a^3 - 3*a^2 - 4*a - 3 : 20*a^3 - 14*a^2 + 7*a - 25 : 1), (-4*a^3 + 2*a^2 - 3*a + 2 : -3*a^3 - 4*a^2 - 5*a : 1), (-11/5*a^3 + 11/5*a^2 + 3/5 : -22/5*a^3 + 11/5*a^2 - 33/5*a + 14/5 : 1), (a^3 + a^2 + 3*a - 1 : -9*a^3 + 2*a^2 - 5*a + 4 : 1)]

Next step: let's factor the prime 2.

```
# Heh, it's just prime still.
v = K.factor(2); v
```

Fractional ideal (2)

Compute the residue class field explicitly and reduction map:

```
F2 = v[0][0].residue_field(); F2
```

```
Residue field in abar of Fractional ideal (2)
```

```
# we can coerce elements from K to F2 and back:
F2(a + 1)
```

```
abar + 1
```

```
F2.lift(F2(a+1))
```

```
a + 1
```

So we can compute the matrix of Frob_2 on $E[5]$.
We have the following (arbitrary choice of) basis P_1, P_2 for $E[5]$:

```
T.gens()
```

```
((16 : 60 : 1), (7*a^3 - 2*a^2 + 4*a - 7 : 7*a^3 - 13*a^2 - 7*a - 18 : 1))
```

```
P1, P2 = T.gens()
P1, P2
```

```
((16 : 60 : 1), (7*a^3 - 2*a^2 + 4*a - 7 : 7*a^3 - 13*a^2 - 7*a - 18 : 1))
```

```
# MASSIVE GOTCHA!!!
P1[0]
P1[1]
P2[0]
P2[1]
```

```
0
1
1
0
```

```
# move to actual points on the curve! (this is really annoying, but \
   whatever)
P1 = P1.element()
P2 = P2.element()
P1[0]
P1[1]
P2[0]
P2[1]
```

```
16
60
7*a^3 - 2*a^2 + 4*a - 7
7*a^3 - 13*a^2 - 7*a - 18
```

Clearly Frob_2 acts trivially on P_1, since P_1 is already rational, hence reduces to a point in $E(_5)$.

Reduce the points P_1 and P_2 modulo 2:

```
# P1 reduces to something fixed by Frob2
[F2(P1[0]), F2(P1[1])]
```

```
[0, 0]
```

```
# P2 reduces to something NOT fixed by frob2:
[F2(P2[0]), F2(P2[1])]
```

```
[abar^3 + 1, abar^3 + abar^2 + abar]
```

```
Frob2P2 = [F2(P2[0])^2, F2(P2[1])^2]
Frob2P2
```

```
[abar + 1, abar^3 + 1]
```

Now we need to figure out what linear combination of P1 and P2 reduces to Frob2P2. We'll just brute force it for now:

```
E2 = E.change_ring(F2)
P1bar = E2([F2(P1[0]), F2(P1[1])])
P2bar = E2([F2(P2[0]), F2(P2[1])])
Frob2P2 = E2([P2bar[0]^2, P2bar[1]^2])
for i in [0..4]:
    for j in [0..4]:
        if i*P1bar + j*P2bar == Frob2P2:
            print i, j
            break
```

```
2 2
```

Conclusion: Frob_2 sends P_1 to P_1 and P_2 to $2P_1 + 2P_2$.

```
Frob2 = matrix(GF(5), [[1,2], [0, 2]]); Frob2
```

```
[1 2]
[0 2]
```

Double check: Is $(x-1)(x-2) \equiv x^2 - a_2 x + 2 \pmod 5$?

```
E.ap(2)
```

```
-2
```

```
x = polygen(GF(5),'x')
(x-1)*(x-2)
x^2 - E.ap(2)*x + 2
```

```
x^2 + 2*x + 2
x^2 + 2*x + 2
```

YEP.

Final note: Computing Frob_p for other primes $p > 2$ is not more difficult. The difficulty is entirely a function of the original choice of ℓ.

```
def Tmodp(p):
    v = K.factor(p)
```

```
    F = K.factor(p)[0][0].residue_field()
    print F
    print "Image of P1 mod %s: %s"%(p, [ F(P1[0]), F(P1[1])])
    print "Image of P2 mod %s: %s"%(p, [ F(P2[0]), F(P2[1])])
    x = polygen(F,'x')
    print "x^2 - a_px + p - (x-1)^2=", x^2 - E.ap(p)*x + p - (x-1)^2
```

```
for p in [2,3,7]+prime_range(13,100):
    print Tmodp(p)
```

```
Residue field in abar of Fractional ideal (2)
Image of P1 mod 2: [0, 0]
Image of P2 mod 2: [abar^3 + 1, abar^3 + abar^2 + abar]
x^2 - a_px + p - (x-1)^2= 1
None
Residue field in abar of Fractional ideal (3)
Image of P1 mod 3: [1, 0]
Image of P2 mod 3: [abar^3 + abar^2 + abar + 2, abar^3 + 2*abar^2 + 2*abar]
x^2 - a_px + p - (x-1)^2= 2
None
Residue field in abar of Fractional ideal (7)
Image of P1 mod 7: [2, 4]
Image of P2 mod 7: [5*abar^2 + 4*abar, abar^2 + 3]
x^2 - a_px + p - (x-1)^2= 4*x + 6
None
Residue field in abar of Fractional ideal (13)
Image of P1 mod 13: [3, 8]
Image of P2 mod 13: [7*abar^3 + 11*abar^2 + 4*abar + 6, 7*abar^3 + 6*abar + 8]
x^2 - a_px + p - (x-1)^2= 11*x + 12
None
Residue field in abar of Fractional ideal (17)
Image of P1 mod 17: [16, 9]
Image of P2 mod 17: [7*abar^3 + 15*abar^2 + 4*abar + 10, 7*abar^3 + 4*abar^2 + 10*abar +
16]
x^2 - a_px + p - (x-1)^2= 4*x + 16
None
Residue field in abar of Fractional ideal (4*a^3 - 4*a^2 - 1)
Image of P1 mod 19: [16, 3]
Image of P2 mod 19: [3*abar + 4, 17*abar + 4]
x^2 - a_px + p - (x-1)^2= 2*x + 18
None
Residue field in abar of Fractional ideal (23)
Image of P1 mod 23: [16, 14]
Image of P2 mod 23: [7*abar^3 + 21*abar^2 + 4*abar + 16, 7*abar^3 + 10*abar^2 + 16*abar +
5]
x^2 - a_px + p - (x-1)^2= 3*x + 22
None
Residue field in abar of Fractional ideal (a^3 + 5*a^2 + a)
```

```
Image of P1 mod 29: [16, 2]
Image of P2 mod 29: [8*abar + 1, 23*abar + 1]
x^2 - a_px + p - (x-1)^2= 2*x + 28
None
Residue field of Fractional ideal (-a^3 - 2*a^2)
Image of P1 mod 31: [16, 29]
Image of P2 mod 31: [14, 12]
x^2 - a_px + p - (x-1)^2= 26*x + 30
None
Residue field in abar of Fractional ideal (37)
Image of P1 mod 37: [16, 23]
Image of P2 mod 37: [7*abar^3 + 35*abar^2 + 4*abar + 30, 7*abar^3 + 24*abar^2 + 30*abar +
19]
x^2 - a_px + p - (x-1)^2= 36*x + 36
None
Residue field of Fractional ideal (-2*a^3 + a^2 + a + 1)
Image of P1 mod 41: [16, 19]
Image of P2 mod 41: [10, 34]
x^2 - a_px + p - (x-1)^2= 10*x + 40
None
Residue field in abar of Fractional ideal (43)
Image of P1 mod 43: [16, 17]
Image of P2 mod 43: [7*abar^3 + 41*abar^2 + 4*abar + 36, 7*abar^3 + 30*abar^2 + 36*abar +
25]
x^2 - a_px + p - (x-1)^2= 8*x + 42
None
Residue field in abar of Fractional ideal (47)
Image of P1 mod 47: [16, 13]
Image of P2 mod 47: [7*abar^3 + 45*abar^2 + 4*abar + 40, 7*abar^3 + 34*abar^2 + 40*abar +
29]
x^2 - a_px + p - (x-1)^2= 41*x + 46
None
Residue field in abar of Fractional ideal (53)
Image of P1 mod 53: [16, 7]
Image of P2 mod 53: [7*abar^3 + 51*abar^2 + 4*abar + 46, 7*abar^3 + 40*abar^2 + 46*abar +
35]
x^2 - a_px + p - (x-1)^2= 8*x + 52
None
Residue field in abar of Fractional ideal (7*a^3 - 7*a^2 - 5)
Image of P1 mod 59: [16, 1]
Image of P2 mod 59: [56*abar + 52, 25*abar + 52]
x^2 - a_px + p - (x-1)^2= 56*x + 58
None
Residue field of Fractional ideal (-3*a^2 - 1)
Image of P1 mod 61: [16, 60]
Image of P2 mod 61: [60, 50]
x^2 - a_px + p - (x-1)^2= 51*x + 60
```

```
None
Residue field in abar of Fractional ideal (67)
Image of P1 mod 67: [16, 60]
Image of P2 mod 67: [7*abar^3 + 65*abar^2 + 4*abar + 60, 7*abar^3 + 54*abar^2 + 60*abar +
49]
x^2 - a_px + p - (x-1)^2= 9*x + 66
None
Residue field of Fractional ideal (3*a^3 - 2*a^2 - 1)
Image of P1 mod 71: [16, 60]
Image of P2 mod 71: [42, 24]
x^2 - a_px + p - (x-1)^2= 5*x + 70
None
Residue field in abar of Fractional ideal (73)
Image of P1 mod 73: [16, 60]
Image of P2 mod 73: [7*abar^3 + 71*abar^2 + 4*abar + 66, 7*abar^3 + 60*abar^2 + 66*abar +
55]
x^2 - a_px + p - (x-1)^2= 71*x + 72
None
Residue field in abar of Fractional ideal (-8*a^3 + 8*a^2 + 3)
Image of P1 mod 79: [16, 60]
Image of P2 mod 79: [17*abar + 40, 9*abar + 40]
x^2 - a_px + p - (x-1)^2= 12*x + 78
None
Residue field in abar of Fractional ideal (83)
Image of P1 mod 83: [16, 60]
Image of P2 mod 83: [7*abar^3 + 81*abar^2 + 4*abar + 76, 7*abar^3 + 70*abar^2 + 76*abar +
65]
x^2 - a_px + p - (x-1)^2= 8*x + 82
None
Residue field in abar of Fractional ideal (a^3 + 9*a^2 + a)
Image of P1 mod 89: [16, 60]
Image of P2 mod 89: [48*abar + 58, 47*abar + 58]
x^2 - a_px + p - (x-1)^2= 76*x + 88
None
Residue field in abar of Fractional ideal (97)
Image of P1 mod 97: [16, 60]
Image of P2 mod 97: [7*abar^3 + 95*abar^2 + 4*abar + 90, 7*abar^3 + 84*abar^2 + 90*abar +
79]
x^2 - a_px + p - (x-1)^2= 9*x + 96
None
```