kolyconj: 389a demo
heegner_points(389)

```
Set of all Heegner points on X_0(389)
```

time H = heegner_points(389).reduce_mod(5)

H

```
Heegner points on X_0(389) over F_5
```

Using ternary quadratic forms we find all reductions $\overline{x}_1$, for the choices of ideal I with $O_K/I = \mathbf{Z}/N\mathbf{Z}$.

time hd = H.heegner_divisor(-7)

```
Time: CPU 3.56 s, Wall: 3.65 s
```

hd

```
(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)
```

hd.element().nonzero_positions()

```
[104, 118]
```

The following "big linear algebra computation" computes data that defines the Hecke equivariant map from

$$\mathrm{Div}(X_0(N)_{\mathbf{F}_5}) \otimes (\mathbf{Z}/3\mathbf{Z}) \to E(\mathbf{F}_{5^2}) \otimes (\mathbf{Z}/3\mathbf{Z}),$$

up to scalar.
time V = H.modp_dual_elliptic_curve_factor(EllipticCurve('389a'), 3, 5)

```
Time: CPU 2.01 s, Wall: 2.17 s
```

V.basis()

```
[
(1, 0, 1, 0, 1, 0, 1, 0, 2, 2, 1, 0, 2, 1, 1, 2, 1, 1, 0, 1, 2, 0,
2, 1, 2, 1, 1, 1, 1, 1, 1, 1, 0, 1, 2, 0, 2, 2, 2, 1, 1, 0, 1, 1, 1,
0, 1, 1, 0, 0, 1, 2, 1, 0, 0, 0, 0, 0, 2, 1, 0, 0, 0, 2, 2, 2, 2, 0,
2, 1, 1, 0, 1, 2, 0, 2, 2, 2, 2, 0, 2, 1, 0, 1, 2, 0, 2, 2, 2, 2, 2,
0, 0, 1, 0, 2, 2, 1, 1, 0, 2, 0, 2, 0, 0, 2, 2, 0, 1, 2, 2, 0, 2, 0,
1, 0, 0, 1, 0, 0, 1, 1, 2, 2, 2, 0, 0, 1, 0, 2),
```

```
(0, 1, 2, 0, 2, 1, 2, 2, 2, 1, 1, 1, 0, 0, 1, 0, 1, 0, 2, 0, 0, 2,
0, 0, 1, 2, 0, 1, 2, 2, 0, 2, 1, 1, 2, 1, 0, 0, 0, 1, 2, 1, 2, 1, 1,
2, 0, 2, 2, 2, 1, 2, 0, 1, 1, 1, 0, 0, 2, 1, 2, 0, 2, 1, 0, 2, 1, 1,
1, 1, 1, 2, 1, 2, 2, 2, 1, 2, 1, 0, 0, 2, 0, 2, 2, 1, 2, 2, 0, 2, 0,
1, 2, 0, 1, 2, 1, 0, 2, 2, 2, 2, 1, 0, 0, 0, 0, 2, 1, 2, 1, 2, 1, 1,
0, 2, 0, 0, 0, 2, 1, 1, 1, 2, 1, 1, 1, 1, 1, 2)
]
```

Compute the two choices of derived Kolyvagin divisor $\sum i\overline{\sigma^i(x_n)}$ associated to $n = 17$ on the modular curve:

k104 = H.kolyvagin_sigma_operator(-7, 17, 104); k104

```
(3, 1, 0, 0, 0, 0, 17, 0, 0, 0, 0, 5, 0, 0, 10, 12, 0, 7, 0, 0, 8,
0, 0, 0, 0, 15, 13, 14, 16, 0, 0, 0, 0, 0, 9, 0, 0, 0, 0, 11, 0, 0,
0, 0, 0, 0, 0, 0, 0, 6, 0, 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)
```

k118 = H.kolyvagin_sigma_operator(-7, 17, 118); k118

```
(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0,
0, 0, 13, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 6, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 5, 0, 0, 0, 0, 0, 0, 4, 0, 0, 8, 0, 0, 2, 0,
0, 0, 0, 0, 0, 0, 0, 0, 17, 15, 3, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 10,
0, 0, 7, 9, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
12, 14, 0, 11, 0, 0, 0, 0, 0, 0, 0, 16, 0, 0, 0, 0, 0, 0, 0)
```

Map them to $E(\mathbf{F}_{5^2})/3E(\mathbf{F}_{5^2})$.

[b.dot_product(k104.element().change_ring(GF(3))) for b in V.basis()]

```
[0, 0]
```

[b.dot_product(k118.element().change_ring(GF(3))) for b in V.basis()]

```
[0, 0]
```

Drat, we got 0, so we didn't verify Kolyvagin's conjecture yet! So try the next inert prime with $3 \mid \gcd(a_p, p+1)$, which is $p = 41$.

k104 = H.kolyvagin_sigma_operator(-7, 41, 104); k104

k118 = H.kolyvagin_sigma_operator(-7, 41, 118); k118

```
(2, 36, 28, 0, 0, 0, 0, 0, 0, 0, 10, 0, 0, 0, 0, 12, 18, 0, 0, 0, 0,
0, 0, 0, 0, 34, 6, 20, 0, 22, 0, 0, 0, 0, 0, 0, 26, 0, 0, 40, 32, 0,
(0, 19, 11, 0, 0, 0, 27, 35, 29, 36, 0, 0, 0, 0, 0, 0, 0, 0, 14, 6,
0, 0, 0, 0, 0, 0, 3, 0, 0, 0, 0, 4, 16, 38, 0, 0, 0, 0, 0, 0, 0, 29,
0, 22, 30, 0, 38, 0, 0, 3, 37, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
30, 0, 0, 37, 27, 19, 0, 0, 0, 0, 0, 15, 23, 0, 7, 0, 22, 0, 0, 0,
1, 0, 0, 0, 0, 48, 31, 23, 0, 0, 8, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
11, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 30, 24, 0, 0, 0, 0, 0, 0, 0,
0, 0, 20, 0, 15, 0, 7, 21, 0, 0, 0, 0, 40, 0, 0, 32, 0, 0, 0, 0, 33,
0, 0, 0, 0, 0, 41, 33, 25, 0, 17, 14, 40, 0, 0, 31, 0, 0, 0, 0, 0,
41, 0, 0, 0, 16, 0, 0, 0, 2, 34, 0, 0, 0, 0, 0, 0, 0, 0, 28, 22, 0,
0, 0, 0, 39)
30, 38, 0, 0, 0, 0, 24, 0, 0, 14, 0, 0, 0, 0, 0, 0, 0, 26, 0, 0, 0,
```

```
0, 0, 0, 0)
```

This works, and shows that $[P_{41}] \neq 0$:

[b.dot_product(k104.element().change_ring(GF(3))) for b in V.basis()]

```
[1, 0]
```

[b.dot_product(k118.element().change_ring(GF(3))) for b in V.basis()]

```
[1, 0]
```