Implementation of a constructive algorithm for Deuring's correspondence

[+4] [2] Andy

[2022-01-31 14:19:05]

[algebraic-geometry elliptic-curves quaternions sagemath isogeny]

[https://math.stackexchange.com/questions/4370619/implementation-of-a-constructive-algorithm-for-deurings-correspondence]

Let E_0 be a supersingular elliptic curve. By Deuring's correspondence, $\mathrm{End}(E_0) \simeq \mathcal{O}_0$ is a maximal order in the quaternion algebra $B_{p,\infty}$ over $\mathbb{Q}$ ramified at p and ∞.

When $p = 17$, $B_{p,\infty} = (-p, -q) = (17, 3)$ and $\mathcal{O}_0 = \langle \frac{1+j}{2}, \frac{i+k}{2}, \frac{j+ck}{q}, k \rangle$ (I'm omitting what the value c is) is a maximal order. I'm trying to implement a constructive algorithm for Deuring's correspondence [Algorithm 3, EHL+18] [1], which computes a supersingular $j \in \mathbb{F}_p$ such that $\mathrm{End}(E(j)) \simeq \mathcal{O}_0$.

Let me briefly explain how the algortihm works; they constructed an isomorphism of $\mathbb{Q}$-algebras $B_{p,\infty} \to \mathrm{End}(E) \otimes \mathbb{Q}, (1, i, j, k) \mapsto (1, \pi, \phi, \pi\phi)$, where π is a pth-power Frobenius endomorphism (they presumed that $\mathcal{O}_0 \simeq \mathrm{End}(E)$ is supersingular so that π lies in $\mathrm{End}(E)$). To find ϕ with $\phi^2 = [-q]$, they first computed all j-invariants with an embedding $\mathcal{O}_K \subset \mathrm{End}(E)$ where $\mathcal{O}_K$ is the ring of integers of $K = \mathbb{Q}(\sqrt{-q})$, by finding roots of the hilbert class polynomial (modulo p) of K (by the construction of p and q, the roots are precisely the j-invariants with the embedding). Then they computed all endomorphisms of degree q for each $E(j)$ and checked if one of them satisfies $\phi^2 = [-q]$.

Now this is my implementaion on Sagemath:

```
sage: def j_with_embedding(p, q):
sage:  F = GF(p)
sage:  R.<x> = PolynomialRing(F)
sage:  K = QuadraticField(-q)
sage:  o = K.maximal_order()
sage:  d = o.discriminant()
sage:  H = hilbert_class_polynomial(d)
sage:  return R(H).roots(multiplicities=False)
```

j_with_embedding(p, q) computes all j-invariant in $\mathbb{F}_p$ with $\mathcal{O}_{\mathbb{Q}(\sqrt{-q})} \subset \mathrm{End}(E(j))$.

When $p = 17$ and $q = 3$, it returns 0.

```
 sage: j_with_embedding(17,3)
 [0]
```

Then I used 'E.isogenies_prime_degree(q)' which computes all isogenies over K of degree q from E/K. There are 4 isogenies of degree 3 from $j = 0$. The first isogeny is the only endomorphism of degree 3. You can get the endomorphism by post-composing an isomorphism of curves.

```
sage: E = EllipticCurve(j=GF(17^2)(0)); E
Elliptic Curve defined by y^2 = x^3 + 1 over Finite Field in z2 of size 17^2
sage: E.isogenies_prime_degree(3)
[Isogeny of degree 3 from Elliptic Curve defined by y^2 = x^3 + 1 to Elliptic Curve defined by y^2 = x^3 + 7,
Isogeny of degree 3 from Elliptic Curve defined by y^2 = x^3 + 1 to Elliptic Curve defined by y^2 = x^3 + 13*x + 15,
Isogeny of degree 3 from Elliptic Curve defined by y^2 = x^3 + 1 to Elliptic Curve defined by y^2 = x^3 + (3*z2+9)*x +
Isogeny of degree 3 from Elliptic Curve defined by y^2 = x^3 + 1 to Elliptic Curve defined by y^2 = x^3 + (14*z2+12)*x
sage: phi = E.isogenies_prime_degree(3)[0]
sage: phi.set_post_isomorphism(phi.codomain().isomorphism_to(E))
sage: phi
Isogeny of degree 3 from Elliptic Curve defined by y^2 = x^3 + 1 to Elliptic Curve defined by y^2 = x^3 + 1
sage: phi.rational_maps()
(((-4*z2 + 5)*x^3 + (z2 + 3))/x^2, ((3*z2 + 7)*x^3*y + (-7*z2 - 5)*y)/x^3)
```

but this endomorphism doesn't satisfy $\phi^2 = [-q]$.

```
sage: (X1, Y1) = phi.rational_maps()
```

```
sage: (X2, Y2) = phi.rational_maps()
sage: X3 = X2.subs(x=X1, y=Y1)
sage: Y3 = Y2.subs(x=X1, y=Y1)
sage: (X3, Y3) == E.multiplication_by_m(-3)
False
```

I'm not sure where it went wrong. Even if I work over an algebraic closure $\overline{\mathbb{F}}_p$, I get only one curve $j = 0$ and there is a unique endomorphism of degree q. I guess $\mathrm{End}(E(0)) \simeq \mathcal{O}_0$, but for some reason I can't construct an endomorphism of degree q.

[1] https://eprint.iacr.org/2018/371.pdf

[+4] [2022-02-01 04:28:15] djao [✔ACCEPTED]

All you need to do is define $\mathrm{GF}(17^2)$ explicitly using a concrete irreducible polynomial.

```
SageMath version 9.4, Release Date: 2021-08-22
Using Python 3.9.5. Type "help()" for help.
```

```
sage: F.<z> = GF(17^2, modulus=x^2+3)
....: E = EllipticCurve(F, [0,1])
....: ker = E(0,1)
....: phi = E.isogeny(ker)
....: phi.set_post_isomorphism(phi.codomain().isomorphism_to(E))
....: (X1, Y1) = phi.rational_maps()
....: (X2, Y2) = phi.rational_maps()
....: X3 = X2.subs(x=X1, y=Y1)
....: Y3 = Y2.subs(x=X1, y=Y1)
....: (X3, Y3) == E.multiplication_by_m(-3)
....:
True
```

Thanks a lot! It was simpler than I thought. - **Andy**

1

[+1] [2023-06-21 04:32:31] yyyyyyy

The core of the issue is that the endomorphism you've constructed is off by a nontrivial automorphism:

```
sage: E = EllipticCurve(j=GF(17^2)(0))
sage: phi = E.isogenies_prime_degree(3)[0]
sage: phi = phi.codomain().isomorphism_to(E) * phi
sage: phi^2 == E.scalar_multiplication(-3)
False
sage: [(aut*phi)^2 == E.scalar_multiplication(-3) for aut in E.automorphisms()]
[False, False, False, False, True, True]
```

This can happen because `.isogenies_prime_degree()` only returns a set of representatives of the outgoing isogenies *up to post-composition with isomorphisms*.

Thus, to solve your problem, you should identify the correct automorphism to compose with, for instance by evaluating the endomorphism ϕ on some points and checking which of the automorphisms acts in the same way. Note that this phenomenon is specific to the curves with j-invariants 1728 and 0, as all other elliptic curves only have ± 1 as automorphisms.

(The fact that the issue also goes away when defining the field using an explicit polynomial, as suggested by the other answer, is merely a coincidence coming from implementation choices within SageMath.)

A better method to solve this problem — construct a supersingular curve together with a small-degree endomorphism — is described in Section 3.1 of the "Deuring for the people" paper [1].

[1] https://ia.cr/2023/106

2
