MAGMA SOURCE FOR N SQUARE-FREE TO COMPUTE $X_0^*(N)(\mathbb{F}_{p^n})$, AND IF $Aut(X_0^*(N)_{\mathbb{F}_p})$ IS TRIVIAL OR NOT

FRANCESC BARS

Programme in Magma V2-23.9 (and working in Magma Calculator Online in October 2018) to compute the number of elements of the set $X_0^*(N)(\mathbb{F}_{p^n})$, obtain $Q_p(k)$ with k odd in [1], and given E an elliptic curve over $\mathbb{Q}$ with conductor $M|N$ to compute two times the number of $\mathbb{F}_{p^n}$-points of E, always $p \nmid N$ prime. Here always N is square-free integer.

To compute $Q_p(k)$ is needed to compute $P_p(k) \in \{0,1\}$, see also the details of such elements in the paper "Bielliptic modular curves $X_0^*(N)$ with N square-free levels by Francesc Bars and Josep González.

Input: Introduce in the first line N a square-free level, p a prime with $p \nmid N$, and the a_p-coefficient of the q-expansion of an elliptic curve E over $\mathbb{Q}$ of conductor M with $M|N$ such that at level M all the Atkin-Lehner involution acts as $+1$ (this elliptic curve appears as a 1-dimensional factor in the Jacobian decomposition of Jac($X_0^*(N)$) over $\mathbb{Q}$).

Output:

(1) PointsOfXzerostarGFp:=[$\#X_0^*(N)(\mathbb{F}_p), \dots, \#X_0^*(N)(\mathbb{F}_{p^{20}})$],
(2) N,
(3) `ValueofP_p`
  :=[$P_p(1), P_p(2), \dots, P_p(20)$],
(4) k, (is the biggest odd integer ≤ 20 such that $P_p(k) = 1 \in \{0,1\}$),
(5) $Q_p(k)$.
(6) DoubleNumberPointsofEprimep:=[$2 \cdot \#E(\mathbb{F}_p), \dots, 2 \cdot \#E(\mathbb{F}_{p^{20}})$].

If one wish to replace 20 for another integer, one can modify 20 in the next programme source with a positive integer where he expects that $Q_p(M)$ will increase, or $2 \cdot \#E(\mathbb{F}_{p^n})$ will be smaller than $\#X_0^*(N)(\mathbb{F}_{p^n})$.

Remember that Aut($X_0^*(N)$) is trivial if $Q_p(k)$ for some k odd and p prime with $p \nmid N$ the quantity $Q_p(k) > 2g_N^* + 2$ following [1], where g_N^* denotes de genus of $X_0^*(N)$.

Magma code:

We use level $N = 555$, $p = 2$ and $E = 185a$ (where $a_2(185a) = -2$, from Cremona tables).

```
N:=555;

p:=2;

a_p_E:=-2;
```

F.Bars supported by MTM2016-75980-P.

```
invariant_eigenforms := [* *]; number_fields:=[* *];

for conductor in Divisors(N) do
  for decomposition_factor in
          NewformDecomposition(CuspidalSubspace(ModularSymbols(conductor,2,1))) do
    eigenform := Eigenform(decomposition_factor, 20);
    number_field_of_eigenform := Parent(Coefficient(eigenform, 3));

    all_atkin_lehners_act_as_identity := true;
    for prime_dividing_conductor in PrimeDivisors(conductor) do
      if AtkinLehner(decomposition_factor, prime_dividing_conductor) ne
                 IdentityMatrix(Rationals(), Dimension(decomposition_factor)) then
        all_atkin_lehners_act_as_identity := false;
      end if;
    end for;

    if all_atkin_lehners_act_as_identity then
      invariant_eigenforms:= Append(invariant_eigenforms, eigenform);
      number_fields:= Append(number_fields, number_field_of_eigenform);
    end if;
  end for;
end for;


C:=ComplexField(100);

R<x>:=PolynomialRing(C);

FrobpolynJacobian:=0*x+1;

RootsFrobactJacob:=[* *];

for j in [1 .. #number_fields] do
   if Degree(number_fields[j]) eq 1 then
       Rootsellipticfactor:=Roots(x^2-Coefficient(invariant_eigenforms[j],p)*x+p,C);
       RootsFrobactJacob:=Append(RootsFrobactJacob,Rootsellipticfactor);
       FrobpolynJacobian:=FrobpolynJacobian*(x^2-Coefficient(invariant_eigenforms[j],p)*x+p);
   else
      dd:=Degree(number_fields[j]);
      u:=Roots(DefiningPolynomial(number_fields[j]),C);
      for m in [1 .. #u] do
         f := hom< number_fields[j] -> C | u[m][1]>;
         cc2:=Roots(x^2-f(Coefficient(invariant_eigenforms[j],p))*x+p,C);
         RootsFrobactJacob:=Append(RootsFrobactJacob,cc2);
         FrobpolynJacobian:=FrobpolynJacobian*(x^2-f(Coefficient(invariant_eigenforms[j],p))*x+p);
      end for;
  end if;
end for;

PointsOfXzerostarGFp:=[* *];
```

```
for nn in [1 .. 20] do
   SumofpowerofFrobpolyn:=0;
   for i in [1 .. # RootsFrobactJacob] do
      for j in [1..2] do
        if RootsFrobactJacob[i][j][2] gt 0 then
         SumofpowerofFrobpolyn:=
         SumofpowerofFrobpolyn+(RootsFrobactJacob[i][j][2])*(RootsFrobactJacob[i][j][1])^(nn) ;
        else
          SumofpowerofFrobpolyn:=SumofpowerofFrobpolyn;
        end if;
      end for;
   end for;

  PointsXzerostarpnn:=Round(1+p^(nn)-SumofpowerofFrobpolyn);

  PointsOfXzerostarGFp:=Append(PointsOfXzerostarGFp,PointsXzerostarpnn);
end for;

PointsOfXzerostarGFp;

N;

ValueofP_p:=[* *];

for aaa in [1..20] do
 sumdivisorsMUbyPointszerostar:=0;
    for kk in Divisors(aaa) do
       vv:=aaa/kk;
       vv:=Numerator(vv);
       sumdivisorsMUbyPointszerostar:=
       sumdivisorsMUbyPointszerostar+(MoebiusMu(vv))*(PointsOfXzerostarGFp[kk]);
     end for;

  vvv:=sumdivisorsMUbyPointszerostar/aaa;
  Rr:=Integers(2);
  P_p_aaa:=Rr!vvv;
  ValueofP_p:=Append(ValueofP_p,P_p_aaa);
end for;

ValueofP_p;




Q_p_odd:=0;

odd_number:=0;

for t in [1..#ValueofP_p] do
```

```
  if ValueofP_p[t] eq 1 then
     tred:=Rr!t;
     if tred eq 1 then
     Q_p_odd:=Q_p_odd+t;
     odd_number:=t;
     else
     Q_p_odd:=Q_p_odd;
     end if;
  else
     Q_p_odd:=Q_p_odd;
  end if;
end for;

odd_number;

Q_p_odd;



DoubleNumberPointsofEprimep:=[* *];

RootsofFrobactE:=Roots(x^2-a_p_E*x+p,C);

for i in [1..20] do
    Twotimesp_i_points_E:=
                         2*(p^i+1-Round(RootsofFrobactE[1][1]^i+ p^i/RootsofFrobactE[1][1]^i));
    DoubleNumberPointsofEprimep:=Append(DoubleNumberPointsofEprimep,Twotimesp_i_points_E);
end for;

DoubleNumberPointsofEprimep;
```

Acknowledgements. We thank referees for their comments, especially those that have contributed to improve the presentation of the Magma source presented here. I am grateful to Josep González for his constant enthusiasm in the study of modular curves and their computational aspects

References

[1] J. González. Constraints on the automorphism group of a curve. *J. Théor. Nombres Bordeaux*, 29(2):535–548, 2017.

• Francesc Bars Cortina

Departament Matemàtiques, Edif. C, Universitat Autònoma de Barcelona, 08193 Bellaterra, Catalonia
E-mail address: francesc@mat.uab.cat