CM2powertorsion := function(E,m)

isab:=false;

a1:=aInvariants(E)[1];

a2:=aInvariants(E)[2];

a3:=aInvariants(E)[3];

a4:=aInvariants(E)[4];

a6:=aInvariants(E)[5];

if m gt 1 then

f:=ExactQuotient(DivisionPolynomial(E,2^m),DivisionPolynomial(E,2^(m-1)));

else

f:=DivisionPolynomial(E,2);

end if;

ffact:=Factorization(f);

/\*

Roots of f are x-coordinates of points of order 2^m.

In the following for loop we check whether each point is defined over an abelian extension.

\*/

for factor in ffact do

if Degree(factor[1]) eq 1 then

K:=Rationals();

x:=Roots(factor[1])[1][1];

else

K<x>:=NumberField(factor[1]);

end if;

/\*

Now x is the x-coordinate of a point of order 2^m.

We check if the y-coordinate is defined over the same field.

If not, we extend to the field of definition of the y-coord.

\*/

R<y>:=PolynomialRing(K);

g := y^2 + a1\*y\*x + a3\*y - x^3 - a2\*x^2 - a4\*x - a6;

if IsIrreducible(g) then

//y-coord defined in an extension

F:=ext<K|g>;

Fabs:=AbsoluteField(F);

else

//y-coord defined over K

Fabs:=K;

end if;

if Fabs eq Rationals() then

G:=CyclicGroup(1);

else

G:=GaloisGroup(Fabs);

end if;

if IsAbelian(G) then

isab:=true;

EF:=BaseExtend(E,Fabs);

end if;

end for;

return isab;

end function;

Es:=[\* \*];

/\*We produce a list that has the following data:

[\* Elliptic Curve, isogenies of E, largest n such that Q(E[n]) is abelian, largest power of 2 needed to be checked \*]

where the largest power of 2 to be checked is simply the sum of the largest power of 2 isogeny and the largest power of 2 dividing the full n-torsion defined over an abelian extension. \*/

//j-invariant 0 has three quad twist families:

Append(~Es, [\* EllipticCurve([0,0,0,0,1]), [1,2,3,6], 2, 2 \*]);

Append(~Es, [\* EllipticCurve([0,0,0,0,16]), [1,3,3,9], 3, 0 \*]);

Append(~Es, [\* EllipticCurve([0,0,0,0,2]), [1,3], 1, 0 \*]);

//j-invariant 2^4\*3^3\*11^3

Append(~Es, [\* EllipticCurveFromjInvariant(2^4\*3^3\*5^3), [1,2,3,6], 2, 2 \*]);

//j-invariant -2^15\*3\*5^3

Append(~Es, [\* EllipticCurveFromjInvariant(-2^15\*3\*5^3), [1,3,9,27], 1, 0 \*]);

//j-invariant 1728 has three quad twist families:

Append(~Es, [\* EllipticCurve([0,0,0,1,0]), [1,2,4,4], 4, 4 \*]);

Append(~Es, [\* EllipticCurve([0,0,0,-1,0]), [1,2,2,2], 4, 3 \*]);

Append(~Es, [\* EllipticCurve([0,0,0,2,0]), [1,2], 2, 2 \*]);

//the rest have only one quad twist family

Append(~Es, [\* EllipticCurveFromjInvariant(2^3\*3^3\*11^3), [1,2,4,4], 2, 3 \*]);

Append(~Es, [\* EllipticCurveFromjInvariant(-3^3\*5^3), [1,2,7,14], 2, 2 \*]);

Append(~Es, [\* EllipticCurveFromjInvariant(3^3\*5^3\*17^3), [1,2,7,14], 2, 2 \*]);

Append(~Es, [\* EllipticCurveFromjInvariant(2^6\*5^3), [1,2], 2, 2 \*]);

Append(~Es, [\* EllipticCurveFromjInvariant(-2^15), [1,11], 1, 0 \*]);

Append(~Es, [\* EllipticCurveFromjInvariant(-2^15\*3^3), [1,19], 1, 0 \*]);

Append(~Es, [\* EllipticCurveFromjInvariant(-2^18\*3^3\*5^3), [1,43], 1, 0 \*]);

Append(~Es, [\* EllipticCurveFromjInvariant(-2^15\*3^3\*5^3\*11^3), [1,67], 1, 0 \*]);

Append(~Es, [\* EllipticCurveFromjInvariant(-2^18\*3^3\*5^3\*23^3\*29^3), [1,163], 1, 0 \*]);

for i:=1 to #Es do

print Es[i][1];

if Es[i][4] gt 0 then

for m:=1 to Es[i][4] do

if CM2powertorsion(Es[i][1],m) then

if m eq Es[i][4] then

print "2power-Torsion over Qab is:", [Es[i][3],2^m];

end if;

else

print "2power-Torsion over Qab is:", [Es[i][3],2^(m-1)];

break m;

end if;

end for;

else

print "2power-Torsion over Qab is:", [0,0];

end if;

end for;

//this returns the largest 2^m such that E has a point of order 2^m over an abelian field.