EXERCISES FOR THE MODULAR/FREY CURVE COURSE PART I

SAMIR SIKSEK

Abstract. These are exercises for the course on Frey curves and modular methods for Diophantine equations. They complement the notes 'The Modular Approach to Diophantine Equations'. In particular you will need to refer to the notes for theorems and recipes.

Contents

1. Useful MAGMA Commands 1
2. Exercises: Part I 3

1. Useful MAGMA Commands

We look at some calculations that you will need in order to do the exercises. If you are familiar with SAGE then you are welcome to use it instead, but we will focus on MAGMA here.

Example 1. We choose an elliptic curve at random and calculate its minimal model and discriminant.

```
> E:=EllipticCurve([0,8,0,48,0]);
> E;
Elliptic Curve defined by y^2 = x^3 + 8*x^2 + 48*x over Rational Field
> F:=MinimalModel(E);
> F;
Elliptic Curve defined by y^2 = x^3 - x^2 + 2*x - 2 over Rational Field
> D:=Discriminant(F);
> D;
-1152
> Factorisation(D);

>> Factorisation(D);
                  ^
Runtime error in 'Factorisation': Bad argument types
```

We want to factorise the minimal discriminant D. The problem here is that MAGMA is thinking about D as a rational number (because it is the discriminant of an elliptic curve F defined over the rationals). MAGMA factorises integers but not rationals.

Date: March 30, 2010.

```
> D:=Integers()!D;
> Factorisation(D);
[ <2, 7>, <3, 2> ]
```

The first line tells MAGMA to think of D as an integer. Now MAGMA is happy to factor D and we know that $D = 2^7 \times 3^2$. Let us also compute the conductor and its factorisation.

```
> N:=Conductor(E);
> Factorisation(N);
[ <2, 7>, <3, 1> ]
```

Example 2. In this example we look at the newforms at level 110.

```
> NFs:=Newforms(CuspForms(110));
> NFs;
[* [*
    q - q^2 + q^3 + q^4 - q^5 - q^6 + 5*q^7 + O(q^8)
*], [*
    q + q^2 + q^3 + q^4 - q^5 + q^6 - q^7 + O(q^8)
*], [*
    q + q^2 - q^3 + q^4 + q^5 - q^6 + 3*q^7 + O(q^8)
*], [*
    q - q^2 + a*q^3 + q^4 + q^5 - a*q^6 - a*q^7 + O(q^8),
    q - q^2 + b*q^3 + q^4 + q^5 - b*q^6 - b*q^7 + O(q^8)
*]*]
```

MAGMA returns the newforms in Galois conjugacy classes. The first three classes contain one newform each. Thus each of the first three newforms is rational and so corresponds to an elliptic curve. Let us take the third one, for example, and see which elliptic curve it corresponds to.

```
> f:=NFs[3,1];
```

The $[3, 1]$ tells MAGMA to pick out the first element of the third conjugacy class.

```
> f;
q + q^2 - q^3 + q^4 + q^5 - q^6 + 3*q^7 + O(q^8)
> E:=EllipticCurve(f);
> E;
Elliptic Curve defined by y^2 + x*y + y = x^3 + x^2 + 10*x - 45 over Rational Field
> Conductor(E);
110
```

Notice that the elliptic curve corresponding to f has conductor 110 which is equal to the level of f. Now let us look instead at the fourth newform.

```
> g:=NFs[4,1];
> g;
q - q^2 + a*q^3 + q^4 + q^5 - a*q^6 - a*q^7 + O(q^8)
```

MAGMA displays only a few coefficients of g, but we can ask for any coefficient we like.

```
> Coefficient(g,17);
-a - 2
```

But what is a? The coefficients of g must live in some totally real field. We know that this field is quadratic since g has only one other conjugate in its conjugacy class.

```
> N<a>:=Parent(Coefficient(g,1));
> N;
Number Field with defining polynomial x^2 + x - 8 over the Rational Field
```

N is the number field generated by the coefficients of g, and a is a root of $x^2 + x - 8$. In other words $a = (-1 + \sqrt{33})/2$ (up to conjugacy).

2. Exercises: Part I

Exercise 1. Let

$$E \ : \quad Y^2 = X(X + 2^8)(X + 3^5).$$

(i) Calculate the minimal discriminant and the conductor of E, and their factorisations.
(ii) Apply Theorem 3 of the notes to E with $p = 5$. Show that $E \sim_5 f$ where f is a newform of level $N_5 = 208$.
(iii) Compute all the newforms at level 208. Determine which one does E arise from modulo 5.

Exercise 2. Use the Theorem 1 and the recipes in Section 10 of the notes to study the equation

$$x^p + 6^r y^p + z^p = 0$$

under the conditions: $p \geq 5$ is prime, $r \geq 1$ and x, y, z are pairwise coprime and not divisible by 2, 3. What can you deduce about r?

Samir Siksek, Mathematics Institute, University of Warwick, Coventry, CV4 7AL, United Kingdom
E-mail address: samirsiksek@yahoo.com