Panoramas & Synthèses
36, 2012, p. 151–179

THE MODULAR APPROACH TO DIOPHANTINE EQUATIONS

by

Samir Siksek

Abstract. — The aim of these notes is to communicate Ribet's Level–Lowering Theorem and related ideas in an explicit and simplified (but hopefully still precise) way, and to explain how these ideas are used to derive information about solutions to Diophantine equations.

***Résumé* (L'approche modulaire des équations diophantiennes).** — Le but de cette note est de présenter le théorème de rabaissement du niveau de Ribet et autres idées relatives d'une façon explicite et simplifiée (que nous espérons être toujours aussi précise), et ensuite d'expliquer comment ces idées sont utilisées pour dériver des informations utiles sur les solutions aux équations diophantiennes.

1. Introduction

These notes are intended as a self-contained tutorial for those who would like to solve Diophantine equations using the modular approach. They were originally written to accompany a short course I gave during the trimester on *Explicit Methods in Number Theory*, held at the Institut Henri Poincaré (September–December 2004). I have since given similar short courses at the Max Planck Institute in Bonn (February 2007) and at the Lorentz Centre in Leiden (May 2007), and these have given me the opportunity to test and revise the notes.

The reader is asked to take some deep results on trust. We do not assume familiarity with modular forms. We do assume familiarity with elliptic curves, but no more than what is contained in, for example, Silverman's book [**34**], or any undergraduate course on elliptic curves.

To be able to verify the proofs, and to solve his/her own equations, the reader will need the computer package `MAGMA` [**5**] though this is not essential for understanding

2000 ***Mathematics Subject Classification.*** — 11D41.
Key words and phrases. — Diophantine equations, modularity.

the notes. The reader wishing to try MAGMA but who does not have access to a machine having MAGMA can try using the online MAGMA calculator:

`http://magma.maths.usyd.edu.au/calc/`.

The package MAGMA is needed to compute newforms. An alternative is to use the William Stein's Modular Forms Database [**36**], and do the programming in any available computer package (GP [**1**] is highly recommended). It is also possible to use the computer package SAGE [**37**] for the computation of newforms.

I am grateful to Henri Cohen, Tom Fisher and Maurice Mignotte for many corrections to these notes, and to William Stein for useful conversations. I would like to thank the referee for many helpful suggestions. I am indebted to Karim Belabas and the organisers of the trimester on *Explicit Methods in Number Theory* for inviting me to give these lectures, to CNRS/Paris XI for financial support, and the Institut Henri Poincaré for its hospitality.

2. Facts about newforms

Think about newforms[1] in terms of their q-expansions

$$f = q + \sum_{n\geq 2} c_n q^n. \tag{1}$$

Here are some facts about newforms:

(a) Associated to our newforms will be two integers: a weight k and a level N (positive integer). If we fix k and N then there are only finitely many newforms of weight k and level N. **In these notes the weight k will always be** 2.

(b) If f is a newform with coefficients c_i as in (1) and $K = \mathbb{Q}(c_2, c_3, \dots)$ then K is a totally real **finite** extension of $\mathbb{Q}$.

(c) The coefficients c_i in fact belong to the ring of integers $\mathcal{O}_K$ of the number field K.

(d) If l is a prime then

$$|c_l^\sigma| \leq 2\sqrt{l} \qquad \text{for all embeddings } \sigma : K \hookrightarrow \mathbb{R}.$$

We shall only be concerned about newforms up to Galois conjugacy. The number of newforms (up to Galois conjugacy) at a particular level depends in a very erratic way on the level N.

Theorem 1. — *There are no newforms at levels*

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60.$$

[1] For those familiar with modular forms, by a newform of level N we mean a normalized cusp form of weight 2 for the full modular group, belonging to the new space at level N, that is a simultaneous eigenfunction for the Hecke operators.

Example 2.1. — The newforms at a fixed level N can be computed using the modular symbols algorithm [**38, 12**]. Thankfully, this has been implemented in `MAGMA` [**5**] by William Stein. To compute in `MAGMA` the newforms at level N, use the command `Newforms(CuspForms(N))`. For example, the newforms at level 110 are

$$\begin{aligned}
f_1 &= q - q^2 + q^3 + q^4 - q^5 - q^6 + 5q^7 + \cdots,\\
f_2 &= q + q^2 + q^3 + q^4 - q^5 + q^6 - q^7 + \cdots,\\
f_3 &= q + q^2 - q^3 + q^4 + q^5 - q^6 + 3q^7 + \cdots,\\
f_4 &= q - q^2 + \theta q^3 + q^4 + q^5 - \theta q^6 - \theta q^7 + \cdots,
\end{aligned}$$

where the first three have coefficients in $\mathbb{Z}$ and the last one has coefficients in $\mathbb{Z}[\theta]$ where $\theta = (-1+\sqrt{33})/2$. Note that there is a fifth newform at level 110 which is the conjugate of f_4. As stated above, in these notes we will only need to worry about newforms up to Galois conjugacy.

3. Correspondence between rational newforms and elliptic curves

We call a newform *rational* if its coefficients are all in $\mathbb{Q}$, otherwise we call it *irrational.*

***Theorem 2* (The Modularity Theorem for Elliptic Curves)**. — *Associated to any* **rational** *newform f of level N is an elliptic curve $E_f/\mathbb{Q}$ of conductor N so that for all primes $l \nmid N$*

$$c_l = a_l(E_f)$$

where c_l is the l-th coefficient in the q-expansion of f and $a_l(E_f) = l + 1 - \#E_f(\mathbb{F}_l)$. For any given positive integer N, the association $f \mapsto E_f$ is a bijection between rational newforms of level N and isogeny classes of elliptic curves of conductor N.

The association $f \mapsto E_f$ is due to Shimura. The fact that this association is surjective was previously known as the Modularity Conjecture, and first proved for squarefree N (the semi-stable case) by Wiles [**40, 39**]. The proof was completed in a series of papers by Diamond [**15**], Conrad, Diamond and Taylor [**11**], and finally Breuil, Conrad, Diamond and Taylor [**6**].

4. Some Useful `MAGMA` Commands

This section is a short `MAGMA` tutorial for those who would like to carry out some of the computations described in these notes, or would like to try some of the exercises.

Example 4.1. — 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.

```
> 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 4.2. — In example 2.1 we looked at the newforms at level 110. Let us return to these and reexamine them with a view towards the Modularity Theorem (Theorem 2).

```
> 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.

We can even get the reference of E in Cremona's tables [**12**];

```
> CremonaReference(E);
110A1
```

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).