THE MODULAR APPROACH TO DIOPHANTINE EQUATIONS

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.

Contents

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.

Date: October 3, 2007.

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 [32], 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 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 [34], and do the programming in any available computer package (`GP` [1] is highly recommended). It is hoped that eventually it will also be possible to use the computer package `SAGE` [35] 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 am indebted to 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 $K = \mathbb{Q}(c_2, c_3, \ldots)$ 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 [36], [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

$$f_1 = q - q^2 + q^3 + q^4 - q^5 - q^6 + 5q^7 + \cdots,$$
$$f_2 = q + q^2 + q^3 + q^4 - q^5 + q^6 - q^7 + \cdots,$$
$$f_3 = q + q^2 - q^3 + q^4 + q^5 - q^6 + 3q^7 + \cdots,$$
$$f_4 = q - q^2 + \theta q^3 + q^4 + q^5 - \theta q^6 - \theta q^7 + \cdots,$$

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 [38], [37]. 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).

5. Level-Lowering

5.1. 'arises from'.

Definition. *Let E be an elliptic curve over the rationals of conductor N, and suppose that f is a newform (of weight 2 as always) and level N' with q-expansion as in (1), and coefficients c_i generating the number field $K/\mathbb{Q}$. We shall say* [2] *that the curve E arises modulo p from the newform f (and write $E \sim_p f$) if there is some prime ideal $\mathfrak{P} \mid p$ of K such that for almost all primes l, we have $a_l(E) \equiv c_l \pmod{\mathfrak{P}}$.*

In fact we can be a little more precise.

Proposition 5.1. *Suppose $E \sim_p f$. Then there is some prime ideal $\mathfrak{P} \mid p$ of K such that for all primes l*

[2] Rather that saying that E arises modulo p from the newform f, it is usual here to say that the Galois representation

$$\rho_p^E : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[p])$$

arises from the newform f.

(i) *if* $l \nmid pNN'$ *then* $a_l(E) \equiv c_l \pmod{\mathfrak{P}}$, *and*
(ii) *if* $l \nmid pN'$ *and* $l \,||\, N$ *then* $l+1 \equiv \pm c_l \pmod{\mathfrak{P}}$.

If f is a rational newform, then we know that f corresponds to some elliptic curve F say (this is E_f in the notation of Theorem 2). If E arises modulo p from f then we shall also say that E arises modulo p from F (and write $E \sim_p F$).

Proposition 5.2. *Suppose that E, F are elliptic curves over $\mathbb{Q}$ with conductors N and N' respectively. Suppose that E arises modulo p from F. Then for all primes l*

(i) *if* $l \nmid NN'$ *then* $a_l(E) \equiv a_l(F) \pmod{p}$, *and*
(ii) *if* $l \nmid N'$ *and* $l \,||\, N$ *then* $l+1 \equiv \pm a_l(F) \pmod{p}$.

It does seem that this Proposition is merely a restatement of Proposition 5.1 in this special case. However it does represent a slight but very important strengthening (due to Kraus and Oesterlé [19]); namely the assumption that $l \neq p$ is removed. This is important because later on p will be an unknown prime exponent in some equation that we would like to solve. It is thus awkward to have conditions that depend on p.

We note in passing that the condition $l \nmid NN'$ is equivalent to saying that the two elliptic curves E and F have good reduction at l. The condition $l \nmid N'$ and $l \,||\, N$ means that E has multiplicative reduction at l, whilst F has good reduction at l.

5.2. **Ribet's Level-Lowering Theorem.** Let E be an elliptic curve over $\mathbb{Q}$. Let $\Delta = \Delta_{\min}$ be the discriminant for a minimal model of E, and N be the conductor of E. Suppose p is a prime, and let [3]

$$N_p = N \Big/ \prod_{\substack{q \,||\, N, \\ p \,|\, \mathrm{ord}_q(\Delta)}} q. \tag{2}$$

We emphasize that the Δ appearing in the definition of N_p must be the minimal discriminant.

Theorem 3. *(A simplified special case of Ribet's Level-Lowering Theorem) Suppose E is an elliptic curve over $\mathbb{Q}$ and $p \geq 5$ is prime. Suppose further that E does not have any p-isogenies. Let N_p be as defined above. Then there exists a newform f of level N_p such that $E \sim_p f$.*

Ribet's Theorem is much more general than this, but this is the only case that we need. Ribet's Theorem has a modularity assumption, but since we are restricting ourselves to elliptic curves, this follows from Theorem 2 (the Modularity Theorem).

Example 5.1. Consider the elliptic curve

$$E \; : \quad y^2 = x^3 - x^2 - 77x + 330$$

[3] **A highbrow remark that should be omitted on first reading:** This N_p is not always the same as the Serre conductor. If we denote the Serre conductor by N_p' then $N_p' \mid N_p$ and the two can only differ by a power of p. In fact Ribet's Theorem allows us to get a newform at level N_p' and weight $k_p \geq 2$ (k_p is the Serre weight). However in these notes we have restricted ourselves to newforms of weight 2, and it turns out that we obtain a newform at level N_p and not at N_p'. In my experience, for purposes of practical computation, this is a bonus and not a hindrance.

with Cremona reference 132B1. The minimal discriminant and conductor are respectively

$$\Delta_{\min} = 2^4 \times 3^{10} \times 11, \qquad N = 2^2 \times 3 \times 11.$$

The only isogeny the curve E has is a 2-isogeny. Hence we may apply Ribet's Theorem with $p = 5$. From the above recipe (2) for the level we find that $N_p = 44$. However, there is only one newform at level 44 which corresponds to the elliptic curve

$$F \ : \quad y^2 = x^3 + x^2 + 3x - 1$$

with Cremona reference $44A1$. Thus $E \sim_5 F$. We record here the traces for E and F for primes $2 \leq l \leq 19$.

l	2	3	5	7	11	13	17	19
$a_l(E)$	0	-1	2	2	-1	6	-4	-2
$a_l(F)$	0	1	-3	2	-1	-4	6	8

The reader is invited to compare this table with what is expected from Proposition 5.2.

Exercise 5.2. Let

$$E \ : \quad y^2 + xy = x^3 - x^2 - 47808x + 4476064.$$

(i) Calculate the minimal discriminant and the conductor of E, and their factorisations.
(ii) Show that E does not have 5-isogenies. One way of doing this is to ask `MAGMA` for the 5-th division polynomial of E and its factorisation: `Factorisation(DivisionPolynomial(E));`
(iii) Apply Ribet's Theorem to E with $p = 5$. Show that $E \sim_5 f$ where f is a newform of level $N_5 = 171$.
(iv) Compute all the newforms at level 171. Determine which one does E arise from modulo 5 (warning: there is no reason to suppose that this newform f is one of the rational ones—be sure to consider both the rational and the irrational newforms).

6. Absence of Isogenies

To be able to apply Ribet's Theorem we must know that our elliptic curve E does not have a p-isogeny. In Exercise 5.2 we did this by writing down the p-th division polynomial of E and testing it for irreducibility. We will shortly apply Ribet's Theorem to Frey elliptic curves. We will explain what Frey curves are later, but for now let us just say that these are elliptic curves that depend on some unknown solution to a Diophantine equation that we would like to solve. Therefore the coefficients of E are not known exactly. Even if p is fixed it is not usually easy to decide if the p-th division polynomial is irreducible. However, the situation is normally much more difficult than that. Normally, p is some unknown exponent in the Diophantine equation that we would like to solve (think of the exponent in Fermat's Last Theorem). We need some way of saying that infinitely many division polynomials are irreducible. What is in fact needed is the following beautiful and powerful theorem of Mazur.

Theorem 4. *(Mazur* [24]*) Suppose $E/\mathbb{Q}$ is an elliptic curve and that* **at least one** *of the following conditions holds.*

- $p \geq 17$ *and* $j(E) \notin \mathbb{Z}[\frac{1}{2}]$,
- *or* $p \geq 11$ *and* E *is a semi-stable elliptic curve,*
- *or* $p \geq 5$, $\#E(\mathbb{Q})[2] = 4$, *and* E *is a semi-stable elliptic curve,*

Then E *does not have any* p*-isogenies.*

Theorem 5. *(Diamond and Kramer* [16]*) Suppose that* $E/\mathbb{Q}$ *is an elliptic curve with conductor* N*. If* $\mathrm{ord}_2(N) = 3$, 5, 7 *then* E *does not have any isogenies of odd degree.*

Example 6.1. Let E be a semi-stable elliptic curve and Δ be its minimal discriminant. Brumer and Kramer conjectured [7] that if $|\Delta|$ is a perfect p-th power for some prime p, then $p \leq 7$ and E has a point of order p. Serre gave a proof of this in [29] that was dependent at the time on what is known as Serre's conjectures. This dependency has now been removed thanks to the work of Ribet and Wiles. Let us follow some of the steps of Serre's proof.

It is easy to see that $N_p = 1$. Suppose that $p \geq 11$. By Theorem 4 the curve E, being semi-stable, does not have p-isogenies. Thus Ribet's Theorem implies that $E \sim_p f$ where f is a newform of level 1. But there are no newforms of level 1. This contradiction shows that $p \leq 7$. With some extra work, Serre proves not only that $p \leq 7$ but that the curve E has non-trivial p-torsion.

Example 6.2. If E has no p-isogenies then we know from Ribet's Theorem that $E \sim_p f$ for some newform f at level N_p. At level N_p there may be rational and non-rational newforms, and some of the non-rational ones can be defined over number fields of rather large degree. There is no reason to suppose that f is rational, or even that the degree of the number field over which f is defined is small as we will show in this example.

Let p be a prime and let $L = 2^{p+4} + 1$; here we do not assume that L is prime. Write

$$E \; : \quad Y^2 = X(X+1)(X - 2^{p+4})$$

The minimal discriminant and conductor are respectively given by

$$\Delta_{\min} = 2^{2p} L^2, \qquad N = 2\,\mathrm{Rad}(L).$$

From Mazur's Theorem E has no p-isogenies, and so applying Ribet's Theorem we see that $E \sim_p f$ for some newform at level N_p, defined over some number field K. We cannot calculate N_p exactly since we do not know if L has any p-th powers in its prime–power decomposition, but we observe that $2 \nmid N_p$. Moreover $2 \,||\, N$. Applying Proposition 5.1 we see that

$$p \mid \mathrm{Norm}_{K/\mathbb{Q}}(3 \pm c_2),$$

where c_i are the coefficients of the q expansion of f. From the facts we have stated about newforms we know that all the conjugates of c_2 are bounded by $2\sqrt{2} < 3$. Hence

$$p < 6^{[K:\mathbb{Q}]}$$

or in other words

$$[K : \mathbb{Q}] > \frac{\log p}{\log 6},$$

showing indeed that an elliptic curve can arise from a newform whose degree (of field of definition) is arbitrarily large.

7. Frey Curves or 'How to use Ribet's Theorem?'

How do we use Ribet's Theorem to solve Diophantine equations. Well, given a Diophantine equation, we shall suppose that it has a solution and associate the solution somehow to an elliptic curve E called a *Frey curve*, **if possible**. The key properties of a 'Frey curve' are that

- the coefficients of E depend on the solution to the Diophantine equation,
- The minimal discriminant of the elliptic curve can be written in the form $\Delta = C \cdot D^p$ where D is an expression that depends on the solution of the Diophantine equation. The factor C **does not depend on the solutions but only on the equation itself**.
- E has multiplicative reduction at primes dividing D.

The conductor N of E will be divisible by the primes dividing C and D, and those dividing D will be removed when we write down N_p. In other words we can make a finite list of possibilities for N_p that depend on the equation. Thus we are able to list a finite set of newforms f such that $E \sim_p f$. From knowing the newforms we deduce local information about E, and since the model for E has coefficients that depend on solutions of our original Diophantine equation, we get information about these solutions.

The rest of these notes is devoted to giving concrete examples of how Ribet's Theorem is used in getting information about solutions to Diophantine equations and occasionally solving them.

8. Fermat's Last Theorem

In this section we prove Fermat's Last Theorem. In fact we solve a more general equation.

Theorem 6. *Suppose $p \geq 5$ is prime. The equation*

$$x^p + 2^r y^p + z^p = 0 \tag{3}$$

has no solutions with $xyz \neq 0$, and x, y, z pairwise coprime except $r = 1$ and $(x, y, z) = \pm(-1, 1, -1)$.

Proof. This Theorem is due to Wiles [38] for $r = 0$, Ribet [27] for $r \geq 2$, and Darmon and Merel [13] for $r = 1$. Suppose that x, y, z is a solution to (3) that is non-trivial (meaning $xyz \neq 0$) and primitive (meaning x, y, z are pairwise coprime). We may assume without loss of generality that

$$x^p \equiv -1 \pmod 4, \qquad 2^r y^p \equiv 0 \pmod 2, \qquad 0 \leq r < p.$$

Associate to this solution the elliptic curve (called a Frey curve)

$$E \ : \quad Y^2 = X(X - x^p)(X + 2^r y^p). \tag{4}$$

We write the associated invariants

$$c_4 = 16(z^{2p} - 2^r x^p y^p), \qquad \Delta = 2^{2r+4}(xyz)^{2p}, \qquad j = \frac{(z^{2p} - 2^r x^p y^p)^3}{2^{2r-8}(xyz)^{2p}}.$$

Applying Tate's algorithm [33, pages 364–369] we compute the minimal discriminant and conductor:

$$\Delta_{\min} = \begin{cases} 2^{2r+4}(xyz)^{2p} & \text{if } 16 \nmid 2^r y^p \\ 2^{2r-8}(xyz)^{2p} & \text{if } 16 \mid 2^r y^p, \end{cases}$$

$$N = \begin{cases} 2\,\mathrm{Rad}_2(xyz) & r \geq 5 \text{ or } y \text{ is even} \\ \mathrm{Rad}_2(xyz) & r = 4 \text{ and } y \text{ is odd} \\ 8\,\mathrm{Rad}_2(xyz) & r = 2,\ 3 \text{ and } y \text{ is odd} \\ 32\,\mathrm{Rad}_2(xyz) & r = 1 \text{ and } y \text{ is odd,} \end{cases} \tag{5}$$

where for positive integer R and prime q we let

$$\mathrm{Rad}_q(R) = \prod_{\substack{l \mid R \text{ prime,} \\ l \neq q}} l.$$

Applying the recipe in (2) we find that

$$N_p = \begin{cases} 2 & r = 0 \text{ or } r \geq 5 \\ 1 & r = 4 \\ 2 & 1 \leq r \leq 3 \text{ and } y \text{ is even} \\ 8 & r = 2,\ 3 \text{ and } y \text{ is odd} \\ 32 & r = 1 \text{ and } y \text{ is odd.} \end{cases}$$

Before applying Ribet's Theorem (Theorem 3) we must ensure that E does not have p-isogenies. Now we know that $E(\mathbb{Q})[2] = 4$. Thus by Mazur's Theorem (Theorem 4), if the conductor N is squarefree then E does not have p-isogenies (recall that $p \geq 5$ and is prime). Examining the formulae for N in (5) we see that if N is not squarefree then $\mathrm{ord}_2(N) = 3$ or 5. In this case it follows from Theorem 5 that E has not p-isogenies.

Now Ribet's Theorem tells us that there is a newform f of level N_p such that $E \sim_p f$. Theorem 1 tells us that there are no newforms of levels 1, 2, 8. Thus we deduce that $r = 1$ and y is odd. We cannot yet eliminate this last possibility since there are newforms at level 32. In fact there is precisely one newform at level 32 corresponding to the elliptic curve

$$F \ : \quad Y^2 = X(X+1)(X+2) \tag{6}$$

with Cremona reference $32A2$. Notice that we can get the elliptic curve F by letting $x = -1$, $y = 1$, $r = 1$, in the model for E given in (4). That is, we are substituting a solution to the equation (3) that satisfies the additional constraints placed above. At this point all that we can conclude is that E arises modulo p from F. The curve F is unusual in that it has complex multiplication. This fact enabled Darmon and Merel to solve the equation (3). The proof will be completed later after we take a closer look at the consequence for an elliptic curve to arise modulo p from another curve with complex multiplication. □

8.1. E **arises from a curve having complex multiplication.** To solve the equation $x^p + 2y^p + z^p = 0$ we shall use the following theorem. For other Diophantine applications of this theorem see [13], [22], [18].

Theorem 7. *Suppose that E and F are elliptic curves over $\mathbb{Q}$, and F has complex multiplication by an order in a number field L. Suppose that $E \sim_p F$ for some prime p.*

(i) *(Halberstadt and Kraus [17]) If $p = 11$ or $p \geq 17$, and p splits in L then the conductors of E and F are equal.*

(ii) *(Darmon and Merel* [13]*) If $p \geq 5$ and p is inert in L, and E has a $\mathbb{Q}$-rational subgroup of order 2 or 3, then $j(E) \in \mathbb{Z}[\frac{1}{p}]$.*

Remark. In part (ii) of the theorem, if we assume that $p^2 \nmid N$ and $p \nmid N'$ where N, N' are respectively the conductor of E, F then we can deduce that $j(E) \in \mathbb{Z}$. To see this suppose that $j(E) \in \mathbb{Z}[\frac{1}{p}]\backslash\mathbb{Z}$. Then $p \,||\, N$, and so by Proposition 5.2

$$p + 1 \equiv \pm a_p(F) \pmod{p}.$$

But since p is inert in L, and F has complex multiplication by an order in L we see that $a_p(F) = 0$. This immediately gives a contradiction.

Completion of the Proof of Theorem 6. We now return to complete the proof of Theorem 6. We have shown that $r = 1$, that y is odd and $E \sim_p F$ where E and F are as in (4) and (6). To simplify we assume that $p \neq 5$, 13. However we note that Dénes [14] has solved the equation $x^p + 2y^p + z^p = 0$ for $p \leq 31$ by classical means.

Now F has complex multiplication by $\mathbb{Z}[i]$. By Theorem 7, if $p \equiv 1 \pmod 4$ (p splits in $\mathbb{Q}(i)$), then the conductor of E is 32. From the formula for the conductor in (5) we know that x, y and z are not divisible by any odd primes. But x, y, z are odd, and it follows $(x, y, z) = \pm(-1, 1, -1)$.

Suppose now that $p \equiv 3 \pmod 4$ (p is inert in $\mathbb{Q}(i)$). Note also that E has a point of order 2. Then $j(E) \in \mathbb{Z}$. From the formula for the j-invariant above and the pairwise coprimality of x, y, z above, we see again that x, y, z is not divisible by odd primes and so $(x, y, z) = \pm(-1, 1, -1)$. □

Exercise 8.1. Use the Theorem 1 and the recipes in Section 13 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?

Exercise 8.2. Consider the Diophantine equation

$$x^2 = y^p + 2^m z^p, \qquad x, y, z \text{ are non-zero, odd and coprime,} \tag{7}$$

where p is prime, and $m \geq 2$. Without loss of generality, assume that $x \equiv 3 \pmod 4$ and associate a solution of this equation to the Frey curve

$$E \;:\quad Y^2 = X(X^2 + 2xX + y^p).$$

Mimic the proof of Theorem 6 to show, assuming that p is suitably large, that the only solutions to (7) are $m = 3$, $x = \pm 3$, $y = z = 1$ and p arbitrary. Where does the proof break down for $m = 1$? [If you get stuck, then this equation is solved in [18] and [30]. You might find the paper of Papadopoulos [25] useful for calculating the conductor.]

9. An Occasional Bound for the Exponent

The proof of Theorem 6 is somewhat miraculous. In general, we expect to find newforms at the level predicted by Ribet's Theorem. Moreover, complex multiplication is rather rare. In general what we will probably find is a collection of newforms, some rational, and some irrational. It is however often possible to obtain a bound for the exponent p via the following Proposition.

Proposition 9.1. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, and suppose that $t \mid \#E(\mathbb{Q})_{\mathrm{tors}}$. Suppose that f is a newform of level N'. Let l be a prime such that $l \nmid N'$ and $l^2 \nmid N$. Let*

$$S_l = \left\{ a \in \mathbb{Z} \ : \quad -2\sqrt{l} \leq a \leq 2\sqrt{l}, \quad a \equiv l+1 \pmod{t} \right\}.$$

Let c_l be the l-th coefficient of f and define

$$B_l'(f) = \mathrm{Norm}_{K/\mathbb{Q}}((l+1)^2 - c_l^2) \prod_{a \in S_l} \mathrm{Norm}_{K/\mathbb{Q}}(a - c_l)$$

and

$$B_l(f) = \begin{cases} l \cdot B_l'(f) & \text{if } f \text{ is } \textbf{not} \text{ rational,} \\ B_l'(f) & \text{if } f \text{ is rational.} \end{cases}$$

If $E \sim_p f$ then $p \mid B_l(f)$.

Proof. This follows easily from Propositions 5.1, 5.2 and the fact the if l is a prime of good reduction for E then $l + 1 - a_l(E) = \#E(\mathbb{F}_l) \equiv 0 \pmod{t}$. □

Notice that this Proposition allows us to bound p provided we can find l such that $B_l(f) \neq 0$. We are guaranteed to succeed in two cases:

(a) Suppose that f is irrational. Then for infinitely many primes l we have $B_l(f) \neq 0$. This is true since $c_l \notin \mathbb{Q}$ for infinitely many of the coefficients c_l.
(b) Suppose that f is rational and that t is prime or $t = 4$. Suppose that for every elliptic curve F in the isogeny class corresponding to f we have $t \nmid \#F(\mathbb{Q})_{\mathrm{tors}}$. Then there are infinitely many primes l such that $B_l(f) \neq 0$.

Exercise 9.1. Let $L = 2^m - 1$ be a Mersenne prime with $m \geq 5$. Show that there is some newform f having level $2L$ such that $B_l(f) = 0$ for all primes $l \neq 2$, L. [**Hint:** Show that the elliptic curve

$$F \ : \quad Y^2 = X(X+1)(X+2^m)$$

has conductor $2L$. Now let f be the newform corresponding to F.]

10. An Example of Serre-Mazur-Kraus

Let L be an odd prime number. In this section we take a close look at the equation

$$x^p + L^r y^p + z^p = 0, \qquad xyz \neq 0, \quad p \geq 5 \text{ is prime,} \tag{8}$$

studied by Serre in [29] and Kraus in [20] – the connection of this equation with Mazur will become apparent. We assume that

$$x,\ y,\ z \text{ are pairwise coprime}, \qquad 0 < r < p. \tag{9}$$

Let A, B, C be some permutation of x^p, $L^r y^p$ and z^p such that $A \equiv -1 \pmod 4$ and $2 \mid B$, and let E be the elliptic curve

$$E \ : \quad Y^2 = X(X - A)(X + B). \tag{10}$$

The minimal discriminant and conductor of E are

$$\Delta_{\min} = 2^{-8} L^{2r} (xyz)^{2p}, \qquad N = \mathrm{Rad}(Lxyz).$$

The recipe for N_p in (2) shows that

$$N_p = 2L.$$

Notice that the elliptic curve E is semi-stable (squarefree conductor N) and that $\#E(\mathbb{Q})[2] = 4$. By Theorem 4, E does not have p-isogenies. Applying Ribet's Theorem we see that E arises modulo p from some newform f at level $N_p = 2L$.

The following result appears in Serre's paper [29].

Theorem 8. *(Mazur) Suppose that L is an odd prime that is neither a Mersenne prime nor a Fermat prime (hence L cannot be written in the form $2^m \pm 1$). Then there is a constant C_L such that if (x, y, p) is a solution to equation (8) satisfying condition (9) then $p \leq C_l$.*

Proof. The point of the proof is that for primes L that are neither Mersenne nor Fermat primes, there are no elliptic curves having full 2-torsion and conductor $2L$. The theorem then follows from the remarks made after Proposition 9.1.

We briefly sketch why there are no elliptic curves having full 2-torsion and conductor $2L$ unless L is a Mersenne or Fermat prime [4]. Suppose F is a curve with conductor $2L$ and full 2-torsion. It is possible to construct a model for F of the form

$$Y^2 = X(X - a)(X + b)$$

which is minimal away from 2, where a, b are integers. Now the discriminant of this model must be of the form $2^u L^v$. However the discriminant of this model is

$$16a^2b^2(a + b)^2.$$

As the model is minimal but has bad reduction at L, we find that precisely one of a, b, $a + b$ is divisible by L. We quickly obtain a relation of the form

$$\pm 2^\alpha \pm 2^\beta \pm 2^\gamma L^\delta = 0$$

where $\delta \geq 1$. From this it is easy to deduce that L is a Fermat or Mersenne prime. □

In fact Kraus [20] went even further proving the following:

Theorem 9. *(Kraus) Suppose that L is an odd prime number that is neither a Mersenne prime nor a Fermat prime. Suppose that (x, y, p) is a solution to equation (8) satisfying conditions (9). Then*

$$p \leq \left(\sqrt{\frac{L+1}{2}} + 1 \right)^{\frac{L+11}{6}}$$

The bound is rather large. However, in practice we obtain a very tiny bound since we can, for any given newform f, compute $B_l(f)$ for many primes l and take the greatest common divisor of them.

Theorem 10. *Suppose $3 \leq L < 100$ is prime. Then the equation (8) has no solutions satisfying conditions (9) unless $L = 31$, in which case $E \sim_p F$ where F is the curve $62A1$.*

Proof. The proof of this result depends on Proposition 9.1, the method of Kraus (Proposition 11.2 below), and the method of predicting exponents (Section 12). See Exercise 11.1 and Exercise 12.1.

[4] There is no proof given of this in [29]. Here we follow [20, Lemme 7].

For illustration we treat the case $L = 19$. From the above we know that $E \sim_p f$ for some newform at level $N_p = 38$. There are two newforms at level 38:

$$f_1 = q - q^2 + q^3 + q^4 - q^6 - q^7 + \cdots$$
$$f_2 = q + q^2 - q^3 + q^4 - 4q^5 - q^6 + 3q^7 + \cdots$$

We apply Proposition 9.1 with $t = 4$ and compute $B_3(f_1) = -15$ and $B_5(f_1) = -144$. By Proposition (9.1), if $E \sim_p f_1$ then p must divide both. But this is impossible as we are assuming that $p \geq 5$.

Also

$$B_3(f_2) = 15, \quad B_5(f_2) = 240, \quad B_7(f_2) = 1155, \quad B_{11}(f_2) = 3360.$$

Thus if $E \sim_p f_2$ then $p = 5$. It turns out that all of the $B_l(f_2)$ are divisible by 5. To see why let F be the elliptic curve $38B1$; this is the elliptic curve that corresponds to f_2. Now looking at Cremona's tables [12] we see that this curve has a point of order 5. Hence $5 \mid \#F(\mathbb{F}_l)$ for all primes $l \nmid 38$. In other words $5 \mid (l + 1 - a_l(F))$ for all primes $l \nmid 38$. Now we see from the definition of $B_l(f_2)$ that $5 \mid B_l(f_2)$ for all primes $l \nmid 38$. Thus we are unable to eliminate the possibility that $p = 5$ using Proposition 9.1. However we can turn the situation to our advantage as follows: suppose that $E \sim_5 f_2$ or equivalently $E \sim_5 F$. Then $a_l(E) \equiv a_l(F) \pmod 5$ for all but finitely many primes l. Hence $5 \mid (l+1-a_l(E))$ for all but finitely many primes l. It follows from the Čebotarev Density Theorem that E has a 5-isogeny (do this as an exercise, or see [28, IV-6]). But E is semi-stable and has full 2-torsion; by Mazur's Theorem (Theorem 4) we have reached a contradiction. Thus we know that equation (8) does not have any solutions with $L = 19$ and $p \geq 5$ satisfying conditions (9). For the analogue of this trick when the newform is irrational see [20, pages 1155–1156]. □

Exercise 10.1. Let A, B, C be non-zero integers such that $A + B + C = 0$. Let E be the elliptic curve

$$E \; : \quad Y^2 = X(X - A)(X + B).$$

Show that any permutation of A, B, C will give a curve that is isomorphic to E or to its quadratic twist by -1.

11. The Method of Kraus

Proposition 9.1 is often capable of bounding p when our (hypothetical Frey) elliptic curve arises modulo p from a newform f. There is another rather interesting method, due to Kraus [21], that can often be used to derive a contradiction **for a fixed value of** p. Kraus used this method to prove that the equation

$$a^3 + b^3 = c^p, \qquad a, b, c \text{ non-zero and coprime},$$

has no solutions for $11 \leq p \leq 10000$. A combination of Proposition 9.1, the method of Kraus and classical techniques for Diophantine equations recently lead to the complete solutions of equations $x^2 + D = y^n$ for $n \geq 3$ and $1 \leq D \leq 100$ (see [9], [31]). In this section we adapt the method of Kraus for equation (8).

We continue with the notation of the previous section. Recall that E is the curve (10) where A, B, C is some permutation of x^p, $L^r y^p$, z^p such that $A \equiv -1 \pmod 4$

and $2 \mid B$. It is somewhat awkward to work with the curve E since there are six possibilities for the triple A, B, C. However, letting

$$E' \quad : \quad Y^2 = X(X - x^p)(X + z^p),$$

we see (from Exercise 10.1) that E and E' are either isomorphic, or quadratic twists of each other by -1. Now E' depends on two variables x, z. However if we write $\delta = (z/x)^p$ then we see that E' is the quadratic twist of

$$E_\delta : \quad Y^2 = X(X-1)(X+\delta),$$

by x^p. For prime $l \nmid x$ it follows that $a_l(E) = \pm a_l(E_\delta)$. From this and Proposition 5.2 we deduce the following.

Lemma 11.1. *With notation as above, suppose that $E \sim_p f$ for some newform f with level $2L$. Suppose that l is a prime distinct from 2, L, p. Write c_l for the l-th coefficient of f as in (1).*

- *If $l \mid xyz$ then $p \mid \mathrm{Norm}((l+1)^2 - c_l^2)$.*
- *If $l \nmid xyz$ then $p \mid \mathrm{Norm}(a_l(E_\delta)^2 - c_l^2)$.*

Suppose $l = np + 1$ is prime. Let

$$\mu_n(\mathbb{F}_l) = \left\{\zeta \in \mathbb{F}_l \quad : \quad \zeta^n = \overline{1}\right\}. \tag{11}$$

Note that if $l \nmid xyz$ then the reduction of $\delta = (x/z)^p$ modulo l belongs to $\mu_n(\mathbb{F}_l)$. The following proposition is now obvious.

Proposition 11.2. *Suppose that $p \geq 5$ is a fixed prime and E is as above. Suppose that for each newform f at level $2L$ there exists a positive integer n satisfying the following four conditions:*

- *$l = np + 1$ is prime.*
- *$l \neq L$.*
- *$p \nmid \mathrm{Norm}((l+1)^2 - c_l^2)$. (Here c_l is the l-th coefficient of f).*
- *For all $\delta \in \mu_n(\mathbb{F}_l)$, $\delta \neq -1$ we have*

$$p \nmid \mathrm{Norm}(a_l(E_\delta)^2 - c_l^2).$$

Then the equation (8) does not have any solutions satisfying conditions (9).

Theorem 11. *Suppose $L = 31$. Then equation (8) does not have any solutions satisfying condition (9) for $11 \leq p \leq 10^6$.*

Proof. Suppose $L = 31$. By Theorem 10 we know that $E \sim_p F$ where F is the elliptic curve $62A1$ with equation

$$y^2 + xy + y = x^3 - x^2 - x + 1.$$

We wrote a very short `GP` [1] script which, for a given prime p, searches for a prime l satisfying the conditions (i), (ii), (iii) of Proposition 11.2. This took about 18 minutes for p in the above range. Our program failed to find a suitable value of $n \leq 1000$ for $p = 5$ and $p = 7$. The case $p = 7$ is dealt with in Exercise 12.1. □

Exercise 11.1. Using a combination of Proposition 9.1 and Proposition 11.2, show that the equation (8) has no solutions for $L = 23$.

12. 'Predicting Exponents of Constants'

The title is in quotes because it is rather vague. For various Diophantine equations the modular approach is very effective at predicting exponents of terms with constant base. This method is central to the recent determination of all perfect powers in the Fibonacci and Lucas sequences [8]. We would like to illustrate this method by studying the Diophantine equation

$$x^2 - 2 = y^p, \qquad p \geq 5 \text{ prime}. \tag{12}$$

The exponent that we would like to predict will become known shortly. As a motivation for studying this equation let us note that the more general equation

$$x^2 - 2^m = y^p$$

has been solved for all $m \geq 2$ (if you did not do Exercise 8.2 then see [18], [30]). Besides, equation (12) is now considered to be one of the most difficult exponential Diophantine equations. This section presents a partial attempt at solving this equation by Bugeaud, Mignotte and myself.

Equation (12) is a special case of the more general equation $Ax^n + By^n = Cz^2$ and so applying the recipes in Section 13 we may associate any solution (x, y) of (12) to the Frey curve

$$E \; : \quad Y^2 = X^3 + 2xX^2 + 2X.$$

We find that

$$\Delta_{\min} = 2^8 y^p, \qquad N = 2^7 \operatorname{Rad}(y), \qquad N_p = 128.$$

From Theorem 5 we know that the curve E does not have p-isogenies. We deduce that E arises from a newform of level 128. There are four newforms at level 128—all rational—corresponding to the four elliptic curves

$$F_1 = 128A1, \quad F_2 = 128B1, \quad F_3 = 128C1, \quad F_4 = 128D1.$$

Hence $E \sim_p F_i$ for some i. Notice that the equation (12) has the solutions $(x, y) = (\pm 1, -1)$ for all exponents p. Hence any attempt to prove that p is bounded by some result similar to Proposition 9.1 will fail. So will mimicking Kraus's method. However we can still use the modular approach to derive non-trivial information about (12).

The classical line of attack for an equation such as (12) is to factorize the left-hand side and deduce that

$$x + \sqrt{2} = (1 + \sqrt{2})^r (U + V\sqrt{2})^p \tag{13}$$

for some U, $V \in \mathbb{Z}$ and

$$\frac{-(p-1)}{2} < r \leq \frac{p-1}{2}. \tag{14}$$

We deduce that

$$\frac{1}{2\sqrt{2}} \left((1 + \sqrt{2})^r (U + V\sqrt{2})^p - (1 - \sqrt{2})^r (U - V\sqrt{2})^p \right) = 1. \tag{15}$$

Notice that the polynomial on the left-hand side is homogeneous of degree p in U, V with coefficients in $\mathbb{Z}$. Thus to solve equation (12) for any particular exponent p we are forced to solve p Thue equations (15), one for each value of r in the range (14). As p gets larger, the coefficients of these equations become very unpleasant, making it difficult to solve them. However, we believe, based on a short search,

that the only solutions are $x = \pm 1$, $y = -1$. Thus from (13) we suspect the only values of r that should correspond to solutions are $r = \pm 1$. We prove this using the modular approach together with a result proved by classical means.

Proposition 12.1. *With notation as above, $r = \pm 1$.*

Proof. Fix F to be one of the four elliptic curves $F_1, \ldots, F_4$ above, and suppose that $E \sim_p F$. Now let l be a prime satisfying the following conditions:

(a) $l = np + 1$ for some integer n,
(b) $\left(\frac{2}{l}\right) = 1$,
(c) $l + 1 \not\equiv \pm a_l(F) \pmod{p}$,

Let $\theta \in \mathbb{F}_l$ be some fixed choice of $\sqrt{2}$ modulo l. We impose on l yet one more condition, namely:

(d) $(1 + \theta)^n \not\equiv 1 \pmod{l}$.

We note that if $l \mid y$ then l will be a prime of multiplicative reduction for E and so condition (a) contradicts Proposition 5.2. We deduce that $l \nmid y$. Hence $\overline{y}^p \in \mu_n(\mathbb{F}_l)$ where $\mu_n(\mathbb{F}_l)$ is given in (11). Let

$$\mathfrak{X}_l' = \left\{\delta \in \mathbb{F}_l \quad : \quad \delta^2 - \overline{2} \in \mu_n(\mathbb{F}_l)\right\}.$$

We see that $\overline{x} \in \mathfrak{X}_l'$. Notice that $\mathfrak{X}_l'$ has cardinality at most $2n$. We would like to refine $\mathfrak{X}_l'$ to obtain better information on the value of x modulo l. For $\delta \in \mathfrak{X}_l'$, let E_δ be the elliptic curve over $\mathbb{F}_l$

$$E_\delta \ : \quad Y^2 = X^3 + 2\delta X^2 + 2X.$$

We let

$$\mathfrak{X}_l = \{\delta \in \mathfrak{X}_l' \quad : \quad a_l(E_\delta) \equiv a_l(F) \pmod{p}\}.$$

It is clear from Proposition 5.2 that $\overline{x} \in \mathfrak{X}_l$ where $\mathfrak{X}_l$ is now a set that we hope is much smaller than $\mathfrak{X}_l'$. Now we want to obtain information about r from knowing that $\overline{x} \in \mathfrak{X}_l$. It follows from (13) that, for some $\delta \in \mathfrak{X}_l$,

$$\delta + \theta \equiv (1 + \theta)^r (U + V\theta)^p \pmod{l}; \tag{16}$$

We note that $U + V\theta \not\equiv 0 \pmod{l}$ since $U^2 - 2V^2 = \pm y$ and we know that $l \nmid y$. To get information about r we need to use the discrete logarithm modulo l. Fix once and for all some primitive root g of $\mathbb{F}_l$. The discrete logarithm with respect to g is the isomorphism $\mathbb{F}_l^* \to \mathbb{Z}/(l-1)$ given by $g^k \mapsto k \pmod{(l-1)}$. Write Φ for the composite of the discrete logarithm with the natural projection $\mathbb{Z}/(l-1) \to \mathbb{Z}/p$. We apply L to both sides of (16) and deduce that,

$$\Phi(\delta + \theta) \equiv r\Phi(1 + \theta) \pmod{p}.$$

It follows from (d) that $\Phi(1 + \theta) \not\equiv 0 \pmod{l}$. Hence

$$r \pmod{p} \in \mathcal{R}_l(F) := \left\{\frac{\Phi(\delta + \theta)}{\Phi(1 + \theta)} \quad : \quad \delta \in \mathfrak{X}_l\right\}.$$

Now we would like to show that $r = \pm 1$. Since r lies in the interval (14), it is enough to show that $r \equiv \pm 1 \pmod{p}$. Thus we look for primes $l_1, \ldots, l_k$ satisfying conditions (a)–(d) so that

$$\cap_{j=1}^{k} \mathcal{R}_{l_j}(F) \subseteq \{\pm 1 \pmod{p}\}.$$

If we can do this for each of the $F = F_1, \ldots, F_4$ we will have proved that $r = \pm 1$. We wrote a short GP script to carry out the above proof for all $5 \leq p < 10^6$. The proof for this range took about 3 hours.

Going up to $p < 10^6$ is indeed overkill, since a careful application of linear forms in logarithms [23] to this problem shows that $p < 8200$ if $y \neq -1$. Thus we know for any p that is not in our range (and indeed for $p > 8200$) that $y = -1$ and we easily see that $r = \pm 1$ in all cases. □

It is possible to improve the estimate $p < 8200$ mentioned in the proof above now that we know that $r = \pm 1$ and using another interesting piece of information given below.

Lemma 12.2. *Suppose $y \neq -1$. Then $y \geq (\sqrt{p} - 1)^2$.*

Proof. It is clear that if $y \neq -1$ then $y > 1$. Clearly y is odd. Hence there is some odd prime $l \mid y$. By Proposition 5.2 we see that

$$l + 1 \equiv \pm a_l(F) \pmod{p},$$

where F is one of $F_1, \ldots, F_4$. However $|a_l(F)| < 2\sqrt{l}$. Thus we see that

$$p \leq l + 1 + 2\sqrt{l} \leq y + 1 + 2\sqrt{y} = (1 + \sqrt{y})^2.$$

The Lemma follows. □

Using this information, another careful application of linear forms in logarithms [23] shows that $p < 1237$.

We can also try to solve the Thue equations with $r = \pm 1$. In fact if we let $F_r(U, V)$ be the polynomial on the left-hand side of equation (15), we see that $F_{-1}(U, V) = F_1(U, -V)$. Hence it is sufficient to solve the Thue equation $F_1(U, V) = 1$. Solving this with GP for $5 \leq p \leq 37$ we get that $(U, V) = (1, 0)$ is the only solution. Thus we have proved the following modest result.

Lemma 12.3. *If $5 \leq p \leq 37$ then $(x, y) = (\pm 1, -1)$ are the only solutions to (12).*

Exercise 12.1. In this exercise we adapt the method of predicting exponents to equation (8). So suppose that (x, y, z) is a solution to equation (8) and that we would like to predict the exponent r. We follow the notation of Sections 10 and 11. Suppose that $E \sim_p f$ for some newform f of level $2L$. Fix a prime $p \geq 7$.

(i) Let $l = np + 1$ be a prime such that $l \neq L$ and $p \nmid \mathrm{Norm}((l+1)^2 - c_l^2)$. Define

$$\mathfrak{X}_l = \left\{ \delta \in \mu_n(\mathbb{F}_l) \setminus \left\{ \overline{-1} \right\} \quad : \quad p \mid \mathrm{Norm}(a_l(E_\delta)^2 - c_l^2) \right\}.$$

Prove that $z^p/x^p \equiv \delta \pmod{l}$ for some $\delta \in \mathfrak{X}_l$. [**Hint:** Use Lemma 11.1. To see why $z^p/x^p \not\equiv -1 \pmod{l}$ use equation (8).]

(ii) Let $\Phi : \mathbb{F}_l^* \to \mathbb{Z}/p$ be a surjective homomorphism as in the proof of Proposition 12.1. Let

$$\mathcal{R}_l = \left\{ \frac{\Phi(-1 - \delta)}{\Phi(L)} \quad : \quad \delta \in \mathfrak{X}_l \right\}.$$

Show that

$$r \pmod{p} \in \mathcal{R}_l.$$

(iii) Use this to prove that equation (8) has no solutions with $p = 7$ and $L = 31$.

13. Recipes for Ternary Diophantine Equations

By ternary Diophantine equations we mean equations of the form $Ax^l + By^m = Cz^n$; the triple of exponents (l, m, n) is called the signature of the equation. How to associate such an equation to a Frey curve is detailed for three important signatures (p, p, p), $(p, p, 2)$ and $(p, p, 3)$ respectively by Kraus [20], by Bennett and Skinner [2], and by Bennett, Vatsal and Yazdani [3]. For convenience of the reader we reproduce the recipes appearing in these papers for the Frey curves and levels. We must however point out that there is much more in these papers than just the recipes and the reader is particularly urged to pursue them. This section is influenced heavily by Bennett's paper [4].

13.1. **Recipes for signature** (p, p, p)**.** Suppose that A, B, C are non-zero pairwise coprime integers, and $p \geq 5$ is prime. Let

$$R = ABC,$$

and suppose that

$$\mathrm{ord}_q(R) < p$$

for every prime number q. Consider the equation

$$Ax^p + By^p + Cz^p = 0, \tag{17}$$

where we assume that

$$Ax,\ By,\ Cz \text{ are non-zero and pairwise coprime.}$$

Without loss of generality we also suppose that

$$Ax^p \equiv -1 \pmod 4, \qquad By^p \equiv 0 \pmod 2.$$

The Frey curve is

$$E\ :\quad Y^2 = X(X - Ax^p)(X + By^p).$$

The minimal discriminant is

$$\Delta_{\min} = \begin{cases} 2^4 R^2 (xyz)^{2p} & \text{if } 16 \nmid By^p, \\ 2^{-8} R^2 (xyz)^{2p} & \text{if } 16 \mid By^p, \end{cases}$$

and the conductor N is given by

$$N = \begin{cases} 2\,\mathrm{Rad}_2(Rxyz) & \text{if } \mathrm{ord}_2(R) = 0 \text{ or } \mathrm{ord}_2(R) \geq 5, \\ 2\,\mathrm{Rad}_2(Rxyz) & \text{if } 1 \leq \mathrm{ord}_2(R) \leq 4 \text{ and } y \text{ is even}, \\ \mathrm{Rad}_2(Rxyz) & \text{if } \mathrm{ord}_2(R) = 4 \text{ and } y \text{ is odd}, \\ 2^3\,\mathrm{Rad}_2(Rxyz) & \text{if } \mathrm{ord}_2(R) = 2 \text{ or } 3 \text{ and } y \text{ is odd}, \\ 2^5\,\mathrm{Rad}_2(Rxyz) & \text{if } \mathrm{ord}_2(R) = 1 \text{ and } y \text{ is even}. \end{cases}$$

Theorem 12. *(Kraus* [20]*) Under the above assumptions, $E \sim_p f$ for some newform f of level N_p where*

$$N_p = \begin{cases} 2\,\mathrm{Rad}_2(R) & \textit{if } \mathrm{ord}_2(R) = 0 \textit{ or } \mathrm{ord}_2(R) \geq 5, \\ \mathrm{Rad}_2(R) & \textit{if } \mathrm{ord}_2(R) = 4, \\ 2\,\mathrm{Rad}_2(R) & \textit{if } 1 \leq \mathrm{ord}_2(R) \leq 3 \textit{ and } y \textit{ is even}, \\ 2^3\,\mathrm{Rad}_2(R) & \textit{if } \mathrm{ord}_2(R) = 2 \textit{ or } 3 \textit{ and } y \textit{ is odd}, \\ 2^5\,\mathrm{Rad}_2(R) & \textit{if } \mathrm{ord}_2(R) = 1 \textit{ and } y \textit{ is odd}. \end{cases}$$

The proof is left as an exercise to the reader. Note that you must show that E does not have any p-isogenies.

13.2. **Recipes for signature** $(p, p, 2)$**.** Consider the equation

$$Ax^p + By^p = Cz^2, \qquad p \geq 7 \text{ is prime},$$

where we assume that

$$Ax,\ By,\ Cz \text{ are non-zero and pairwise coprime.}$$

We moreover suppose that

$$\mathrm{ord}_q(A) < p, \qquad \mathrm{ord}_q(B) < p, \qquad \text{for all primes } q$$

and

$$C \text{ is squarefree.}$$

Without loss of generality we may suppose that we are in one of the following situations:

(i) $ABCxy \equiv 1 \pmod 2$ and $y \equiv -BC \pmod 4$.
(ii) $xy \equiv 1 \pmod 2$ and either $\mathrm{ord}_2(B) = 1$ or $\mathrm{ord}_2(C) = 1$.
(iii) $xy \equiv 1 \pmod 2$, $\mathrm{ord}_2(B) = 2$ and $z \equiv -By/4 \pmod 4$.
(iv) $xy \equiv 1 \pmod 2$, $\mathrm{ord}_2(B) \in \{3, 4, 5\}$ and $z \equiv C \pmod 4$.
(v) $\mathrm{ord}_2(By^p) \geq 6$ and $z \equiv C \pmod 4$.

In cases (i) and (ii) we consider the curve

$$E_1 \ : \quad Y^2 = X^3 + 2CzX^2 + BCy^pX.$$

In cases (iii) and (iv) we consider

$$E_2 \ : \quad Y^2 = X^3 + CzX^2 + \frac{BCy^p}{4}X,$$

and in case (v) we consider

$$E_3 \ : \quad Y^2 + XY = X^3 + \frac{Cz - 1}{4}X^2 + \frac{BCy^p}{64}X.$$

Theorem 13. *(Bennett and Skinner* [2]*) With assumptions and notation as above, we have:*

(a) *The minimal discriminant of E_i is given by*

$$\Delta_i = 2^{\delta_i} C^3 B^2 A (xy^2)^p,$$

where

$$\delta_1 = 6, \qquad \delta_2 = 0, \qquad \delta_3 = -12.$$

(b) *The conductor of the curve E_i is given by*

$$N = 2^{\alpha} C^2 \,\mathrm{Rad}(ABxy),$$

where

$$\alpha = \begin{cases} 5 & \text{if } i=1, \text{ case (i)} \\ 6 & \text{if } i=1, \text{ case (ii)} \\ 1 & \text{if } i=2, \text{ case (iii)}, \ \mathrm{ord}_2(B)=2 \text{ and } y \equiv -BC/4 \pmod 4 \\ 2 & \text{if } i=2, \text{ case (iii)}, \ \mathrm{ord}_2(B)=2 \text{ and } y \equiv BC/4 \pmod 4 \\ 4 & \text{if } i=2, \text{ case (iv) and } \mathrm{ord}_2(B)=3 \\ 2 & \text{if } i=2, \text{ case (iv) and } \mathrm{ord}_2(B)=4 \text{ or } 5 \\ -1 & \text{if } i=3, \text{ case (v) and } \mathrm{ord}_2(By^7)=6 \\ 0 & \text{if } i=3, \text{ case (v) and } \mathrm{ord}_2(By^7)\geq 7. \end{cases}$$

(c) *suppose that E_i does not have complex multiplication (This would follow if we assume that $xy \neq \pm 1$). Then $E_i \sim_p f$ for some newform f of level*

$$N_p = 2^\beta C^2 \,\mathrm{Rad}(AB)$$

where

$$\beta = \begin{cases} \alpha & \text{cases (i)–(iv)}, \\ 0 & \text{case (v) and } \mathrm{ord}_2(B) \neq 0,\ 6, \\ 1 & \text{case (v) and } \mathrm{ord}_2(B)=0, \\ -1 & \text{case (v) and } \mathrm{ord}_2(B)=6. \end{cases}$$

(d) *The curves E_i have non-trivial 2-torsion.*

(e) *Suppose $E = E_i$ is a curve associated to some solution (x, y, z) satisfying the above conditions. Suppose that F is another curve defined over $\mathbb{Q}$ such that $E \sim_p F$. Then the denominator of the j-invariant $j(F)$ is not divisible by any odd prime $q \neq p$ dividing C.*

Part (d) is included to help with the application of Proposition 9.1. Part (e) is often very useful in eliminating rational newforms (which correspond to elliptic curves). See for example Exercise 13.2.

Exercise 13.1. Determine all the solutions of the equation

$$x^p + 2^r y^p = 3z^2, \qquad r \geq 2, \quad p \geq 7 \text{ prime}$$

in coprime integers x, y, z.

Exercise 13.2. The Fibonacci and Lucas sequences F_n, L_n are defined by

$$F_0 = 0,\ F_1 = 1, \qquad F_{n+2} = F_n + F_{n+1} \text{ for all } n \geq 0,$$
$$L_0 = 2,\ L_1 = 1, \qquad L_{n+2} = L_n + L_{n+1} \text{ for all } n \geq 0.$$

(a) Show that $5F_n^2 + 4(-1)^n = L_n^2$.

(b) Prove that the equation $L_n = y^p$ has no solution with n even.

[**Hint for (b)**: You should follow the recipes above and use part (e) of Theorem 13 to deduce a contradiction.]

Exercise 13.3. In this exercise we look at the equation $F_n = y^p$ where F_n is the Fibonacci sequence defined above. This is a very difficult Diophantine problem, whose solution [8] required just about all the tools described in these lecture notes plus a highly non-trivial application of Baker's Theory and the methods of Diophantine approximation. Our aim in this exercise is to show how congruences for

n can be obtained by the modular approach. This is really an exercise about predicting the exponents of constants in the style of Section 12; note that the index n is an exponent in the familiar expressions for the Fibonacci and Lucas sequences:

$$F_n = \frac{\lambda^n - \mu^n}{\sqrt{5}}, \qquad L_n = \lambda^n + \mu^n,$$

where $\lambda = (1+\sqrt{5})/2$ and $\mu = (1-\sqrt{5})/2$.

To simplify, suppose $p = 7$ and $n \equiv 1 \pmod 6$.

(a) Show that $F_n \equiv L_n \equiv 1 \pmod 4$ (for $n \equiv 1 \pmod 6$).
(b) Show that $F_n = y^7$ implies that
$$5y^{14} - 4 = L_n^2.$$
(c) Apply the recipes above to this equation (with $p = 7$). This means that we take the Frey curve to be
$$E_n \; : \quad Y^2 = X^3 + L_n X^2 - X.$$
Deduce from the recipes that $E_n \sim_7 E$ where E is the unique elliptic curve of conductor 20. One model for E is
$$E \; : \quad Y^2 = X^3 + X^2 - X.$$
Note that $E_1 = E$ which is not a coincidence since $F_1 = 1 = 1^7$ is a solution to the Diophantine equation that we are trying to solve.
(d) Use Proposition 5.2 with $l = 3$ to show that $L_n \equiv 1 \pmod 3$.
(e) By writing down the sequence L_n modulo 3 for sufficiently many n (until it starts repeating), deduce from $L_n \equiv 1 \pmod 3$ that $n \equiv 1, 3, 4 \pmod 8$. However, we are assuming that $n \equiv 1 \pmod 6$, so that $n \equiv 1$ or $19 \pmod{24}$.
(f) Repeat steps (d) and (e) with $l = 7$ to deduce that $n \equiv 1$ or $43 \pmod{48}$. Deduce that if $n \neq 1$ then $n \geq 43$.

One step in the solution of $F_n = y^p$ for $n \equiv 1 \pmod 6$ and $p = 7$ is to show that either $n = 1$ or $n > 2.639 \times 10^{46}$. This was shown By repeating the above argument (using a suitable computer program) with thousands of primes l.

13.3. **Recipes for signature** $(p, p, 3)$**.** Consider the equation

$$Ax^p + By^p = Cz^3, \qquad p \geq 5 \text{ is prime},$$

where we suppose that

$$Ax,\ By,\ Cz \text{ are non-zero and pairwise coprime.}$$

We suppose without loss of generality that

$$\mathrm{ord}_q(A) < p, \quad \mathrm{ord}_q(B) < p, \quad \mathrm{ord}_q(C) < 3,$$

for all primes q, and that

$$Ax \not\equiv 0 \pmod 3, \quad By^p \not\equiv 2 \pmod 3.$$

Let

$$E \; : \quad Y^2 + 3CzXY + C^2By^pY = X^3.$$

Theorem 14. *(Bennett, Vatsal and Yazdani* [3]*) With notation and assumptions as above:*

(a) *The conductor N of the curve E is given by*

$$N = \mathrm{Rad}_3(ABxy)\,\mathrm{Rad}_3(C)^2\epsilon_3$$

where

$$\epsilon_3 = \begin{cases} 3^2 & \text{if } 9 \mid (2 + C^2By^p - 3Cz), \\ 3^3 & \text{if } 3 \mid\mid (2 + C^2By^p - 3Cz), \\ 3^4 & \text{if } \mathrm{ord}_3(By^p) = 1, \\ 3^3 & \text{if } \mathrm{ord}_3(By^p) = 2, \\ 1 & \text{if } \mathrm{ord}_3(By^p) = 3, \\ 3 & \text{if } \mathrm{ord}_3(By^p) > 3, \\ 3^5 & \text{if } 3 \mid C. \end{cases}$$

(b) *Suppose that $xy \neq 1$ and the curve E does not correspond to one of the equations*

$$1 \cdot 2^5 + 27 \cdot (-1)^5 = 5 \cdot 1^3, \qquad 1 \cdot 2^7 + 3 \cdot (-1)^7 = 1 \cdot 5^3.$$

Then $E \sim_p f$ for some newform f of level

$$N_p = \mathrm{Rad}_3(AB)\,\mathrm{Rad}_3(C)^2\epsilon_3',$$

where

$$\epsilon_3' = \begin{cases} 3^2 & \text{if } 9 \mid (2 + C^2By^p - 3Cz), \\ 3^3 & \text{if } 3 \mid\mid (2 + C^2By^p - 3Cz), \\ 3^4 & \text{if } \mathrm{ord}_3(By^p) = 1, \\ 3^3 & \text{if } \mathrm{ord}_3(By^p) = 2, \\ 1 & \text{if } \mathrm{ord}_3(B) = 3, \\ 3 & \text{if } \mathrm{ord}_3(By^p) > 3 \text{ and } \mathrm{ord}_3(B) \neq 3, \\ 3^5 & \text{if } 3 \mid C. \end{cases}$$

(c) *The curve E has a point of order 3, namely the point $(0, 0)$.*

(d) *Suppose F is an elliptic curve defined over $\mathbb{Q}$ such that $E \sim_p F$. Then the denominator of the j-invariant $j(F)$ is not divisible by any odd prime $q \neq p$ dividing C.*

References

[1] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, *User's guide to PARI-GP*, version 2.3.2. (See also `http://pari.math.u-bordeaux.fr/`)

[2] M. A. Bennett and C. M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), no. 1, 23–54.

[3] M. A. Bennett, V. Vatsal and S. Yazdani, *Ternary Diophantine Equations of Signature* $(p, p, 3)$, Compositio Mathematica **140** (2004), 1399-1416.

[4] M. A. Bennett, *Recipes for ternary Diophantine equations of signature* (p, p, k), Proc. RIMS Kokyuroku (Kyoto) **1319** (2003), 51–55

[5] W. Bosma, J. Cannon and C. Playoust, *The Magma Algebra System I: The User Language*, J. Symb. Comp. **24** (1997), 235–265. (See also `http://magma.maths.usyd.edu.au/magma/`)

[6] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14 No.4** (2001), 843–939.

[7] A. Brumer and K. Kramer, *The rank of elliptic curves*, Duke Math. J. **44** (1977), 715–742.

[8] Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers*, Annals of Mathematics **163** (2006), 969–1018.

[9] Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential Diophantine equations II. The Lebesgue–Nagell Equation*, Compositio Mathematica **142** (2006), 31–62.
[10] H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM **138**, Springer-Verlag, 1993.
[11] B. Conrad, F. Diamond, R. Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, J. Amer. Math. Soc. **12** (1999), no. 2, 521–567.
[12] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd edition, Cambridge University Press, 1996.
[13] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*, J. reine angew. Math. **490** (1997), 81–100.
[14] P. Dénes, *Über die Diophantische Gleichung* $x^l + y^l = cz^l$, Acta Math. **88** (1952), 241–251.
[15] F. Diamond, *On deformation rings and Hecke rings*, Ann. of Math. **144** (1996), no. 1, 137–166.
[16] F. Diamond and K. Kramer, *Modularity of a family of elliptic curves*, Math. Res. Lett. **2** (1995), No. 3, 299–304.
[17] E. Halberstadt and A. Kraus, *Sur les modules de torsion des courbes elliptiques*, Math. Ann. **310** (1998), 47–54.
[18] W. Ivorra, *Sur les équations* $x^p + 2^\beta y^p = z^2$ *et* $x^p + 2^\beta y^p = 2z^2$, Acta Arith. **108** (2003), 327–338.
[19] A. Kraus and J. Oesterlé, *Sur une question de B. Mazur*, Math. Ann. **293** (1992), 259–275.
[20] A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée*, Can. J. Math. **49** (1997), 1139–1161.
[21] A. Kraus, *Sur l'équation* $a^3 + b^3 = c^p$, Experimental Mathematics **7** (1998), No. 1, 1–13.
[22] A. Kraus, *On the Equation* $x^p + y^q = z^r$*: A Survey*, The Ramanujan Journal **3** (1999), 315–333.
[23] M. Laurent, M. Mignotte and Yu. Nesterenko, *Formes linéaires en deux logarithmes et déterminants d'interpolation*, J. Number Theory **55** (1995), 255–265.
[24] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.
[25] I. Papadopoulos, *Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle* 2 *et* 2, J. Number Theory **44** (1993), 119–152.
[26] K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476.
[27] K. Ribet, *On the equation* $a^p + 2b^p + c^p = 0$, Acta Arith. **LXXIX.1** (1997), 7–15.
[28] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, W. A. Benjamin, New York, 1968.
[29] J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230.
[30] S. Siksek, *On the Diophantine equation* $x^2 = y^p + 2^k z^p$, Journal de Théorie des Nombres de Bordeaux **15** (2003), 839–846.
[31] S. Siksek and J. E. Cremona, *On the Diophantine equation* $x^2 + 7 = y^m$, Acta Arith. **109.2** (2003), 143–149.
[32] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, GTM 106, 1985.
[33] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, GTM 151, 1994.
[34] W. A. Stein, *Modular Forms Database*, `http://modular.fas.harvard.edu/Tables`
[35] W. A. Stein, *SAGE: Software for Algebra and Geometry Experimentation*, `http://www.sagemath.org/sage/`, `http://sage.scipy.org/`
[36] W. A. Stein, *Modular Forms: A Computational Approach*, American Mathematical Society, Graduate Studies in Mathematics 79, 2007.
[37] R. L. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Math. **141** (1995), 553–572.
[38] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. **141** (1995), 443–551.

Samir Siksek, Mathematics Institute, University of Warwick, Coventry, CV4 7AL, United Kingdom

E-mail address: `s.siksek@warwick.ac.uk`