JOURNAL
de Théorie des Nombres
de BORDEAUX
*anciennement Séminaire de Théorie des Nombres de Bordeaux*

Samir SIKSEK

**Diophantine equations after Fermat's last theorem**

Tome 21, n° 2 (2009), p. 423-434.

<http://jtnb.cedram.org/item?id=JTNB_2009__21_2_423_0>

*Journal de Théorie des Nombres*
*de Bordeaux* **21** (2009), 423-434

# Diophantine equations after Fermat's last theorem

par Samir SIKSEK

Résumé. Cet article reprend les notes de mon exposé aux 25-ièmes Journées Arithmétiques, du 2 au 6 juillet 2007 à Edimbourg en Écosse. J'ai pour but d'apporter un peu de lumière sur les deux questions suivantes :

(i) Étant donnée une équation diophantienne, quelle information peut-on obtenir en suivant la stratégie de Wiles pour sa preuve du théorème de Fermat ?

(ii) Est-il utile de combiner cette approche avec les approches traditionnelles des équations diophantiennes : approximation diophantienne, géométrie arithmétique, ... ?

Abstract. These are expository notes that accompany my talk at the 25th Journées Arithmétiques, July 2–6, 2007, Edinburgh, Scotland. I aim to shed light on the following two questions:

(i) Given a Diophantine equation, what information can be obtained by following the strategy of Wiles' proof of Fermat's Last Theorem?

(ii) Is it useful to combine this approach with traditional approaches to Diophantine equations: Diophantine approximation, arithmetic geometry, ... ?

## 1. Introduction

These are expository notes that accompany my talk at the 25th Journées Arithmétiques, July 2–6, 2007, Edinburgh, Scotland. None of the ideas described in Sections 2 and 3 are due to myself; these are now well-known ideas for which credit goes to Hellegouarch, Frey, Serre, Ribet, Wiles, Taylor, etc. The rest of the talk is based on work done in collaboration either with Yann Bugeaud and Maurice Mignotte [6], [7], [8] or with John Cremona [18]. This work builds on the ideas of many others: Darmon, Merel, Kraus, Bennett, Skinner, Ivorra, etc.

I am foremost concerned with the **explicit resolution** of Diophantine equations. There are three competing traditions in this field.

(i) *elementary methods*; I need not explain what these are.

(ii) *Diophantine approximation*; one uses analytic techniques to derive bounds for the sizes of solutions of certain Diophantine equations.
(iii) *arithmetic geometry*; one views Diophantine equations as algebraic varieties.

The *modular approach*, used in Wiles' celebrated proof of Fermat's Last Theorem, is the most radical recent idea in the field of Diophantine equations. It is based on a surprising series of ideas 'Frey curves', 'Galois representations', 'modularity', 'level-lowering', etc and does not really fit into the traditional view-points i–iii.

My objective is to explain the kind of information that can be obtained from the modular approach and to give a sense that it is often necessary to combine this method with the traditional view-points i–iii. To maintain some coherence of exposition I will focus on the work done by myself and collaborators. It would however be unfair not to mention that there are others who have successfully combined the modular approach with traditional approaches, such as Bennett [2] or (as in the truly wonderful paper of) Poonen, Schaefer and Stoll [16].

This article is aimed at a general number theory audience, and so I will suppress the technicalities involved as much as possible.

This work is funded by an EPSRC grant and a Marie-Curie International Reintegration grant. I would like to thank my friends Yann Bugeaud and Maurice Mignotte for comments on a previous version of this paper.

## 2. Fermat's last Theorem

The quickest way to immerse oneself into the modular approach is through a summary of Wiles' proof [21], [20] of Fermat's Last Theorem. Suppose there is some $(x, y, z)$ satisfying $x^p + y^p + z^p = 0$ where $x, y, z$ are coprime integers, $xyz \neq 0$ and $p \geq 5$ is prime. Using the symmetries of the Fermat equation, there is no loss of generality in assuming that $x \equiv -1 \pmod 4$ and $2 \mid y$. Associate to this solution $(x, y, z)$ the Frey elliptic curve

$$E_{x,y,z} \ : \ Y^2 = X(X - x^p)(X + y^p).$$

This Frey curve has minimal discriminant

$$\Delta_{\min} = \frac{1}{2^8}(xyz)^{2p}.$$

Wiles proved the modularity of semi-stable elliptic curves, which includes the curve $E_{x,y,z}$. Historically this was the last step in the proof of Fermat's Last Theorem. The modularity is essential for the next step where we apply Ribet's Theorem. Before doing that observe that modularity has been established for all elliptic curves over the rationals [5]—I shall not need to mention modularity again.

We now look at the Galois representation on the $p$-torsion of $E_{x,y,z}$. Ribet's Level-lowering Theorem predicts that this Galois representation arises from a newform [1] of level 2. Later on I shall talk a little more about how Ribet's Theorem applies to Frey curves, and say a little about newforms. For now let me just quote the fact that there are no newforms of level 2 and so we have a contradiction.

Before we talk a little more about Frey curves and newforms, let us observe that the Fermat equation has solutions, for example $(-1, 0, 1)$. All the known solutions satisfy $xyz = 0$. We did not state where the assumption $xyz \neq 0$ was used. If $xyz = 0$ then the Frey curve has zero discriminant and so is not even an elliptic curve and so the rest of the proof is not applicable.

## 3. How the modular machinery is applied to Diophantine equations

Suppose we have a Diophantine equation that we are interested in solving; the Diophantine equation should have some prime exponent $p \geq 5$. Our first step is to associate a hypothetical solution of the Diophantine equation to a *Frey curve*. A Frey curve should satisfy the following conditions.

- Be an elliptic curve whose coefficients depend on the hypothetical solution of the Diophantine equation.
- Have minimal discriminant $\Delta = C \times D^p$ where
  - $C$ depends on the Diophantine equation that we would like to solve and not on the solution, and
  - $D$ depends on the solution.
- The primes dividing $D$ are primes of multiplicative reduction for the elliptic curve.

The next step is to look at the Galois representation on the $p$-torsion and apply Ribet's Theorem. To apply Ribet's Theorem we need that the Galois representation is irreducible (or some similar condition). For this we probably need to quote some theorems of Mazur. For example this is automatically satisfied if $p > 167$ and the $j$-invariant is non-integral. Ribet's Theorem then tells us that the Galois representation on the $p$-torsion arises from a newform at a certain (explicitly computable) level $N$. The main point is that the level depends only on $C$ which depends on the original Diophantine equation, and not on $D$ which depends on the solution. This is exactly the same as in the proof of Fermat's Last Theorem where $N = 2$ is independent of the solution. Now if there are no newforms of level $N$ then our original Diophantine equation has no *non-trivial* solutions. The trivial solutions are the ones that make the Frey curve singular.

[1] For those familiar with modular forms, I shall only be concerned with elliptic modular forms of weight 2. By a newform of level $N$ I mean a normalized cusp form of weight 2 belonging to the new space at level $N$, that is a simultaneous eigenfunction for the Hecke operators.

We should say that Frey curves have been constructed for only a few families of Diophantine equations. For example,

$$ax^p + by^p = cz^p, \qquad ax^p + by^p = cz^2, \qquad ax^p + by^p = cz^3, \qquad \dots.$$

What happens if there are newforms of the predicted level $N$? It is time to talk a little about newforms. Associated to any positive integer $N$ are the newforms of level $N$. There are finitely many of these and they can be determined by the modular symbols algorithm as explained in the books of Cremona [12] and Stein [19]. It is helpful to think of newforms in terms of their Fourier expansion around $\infty$:

$$f = q + \sum_{n=2}^{\infty} a_n q^n.$$

Here the coefficients $a_n$ are algebraic integers in some totally real number field. If all the $a_n \in \mathbb{Z}$ we say the newform is *rational*. Otherwise the newform is said to be *irrational*. Rational newforms correspond to elliptic curves, and irrational ones to higher dimensional modular abelian varieties.

Let us return to our problem of attacking a specific Diophantine equation using the modular approach. We obtain a list of finitely many newforms at the predicted level $N$. We want to know what information these newforms tell us about the Diophantine equation. Surprisingly, it is much easier to deal with the non-rational newforms than with the rational ones. The reason is that the higher dimensional modular abelian variety that corresponds to a non-rational newform looks nothing like our (1-dimensional) Frey elliptic curve and this helps us to obtain very stringent conditions on the solutions to the Diophantine equation. For example, we can obtain an explicit bound for the exponent $p$. This is sometimes true for rational newforms as well, but very often rational newforms are troublesome. It is now appropriate to give an example.

## 4. The generalized Ramanujan–Nagell equation

In 1913 Ramanujan asked for the solutions to the equation $x^2 + 7 = 2^m$. This was solved by Trygve Nagell in 1948, and the solution is found in several undergraduate algebraic number theory texts. The equation is highly unusual in that it has such large number of solutions $(x, m) = (\pm 1, 3)$, $(\pm 3, 4)$, $(\pm 5, 5)$, $(\pm 11, 7)$, $(\pm 181, 15)$. It is natural to wonder about the more general equation

$$x^2 + 7 = y^m, \qquad x, y, m \in \mathbb{Z}, \quad m \geq 3. \tag{4.1}$$

But for the history of this type of problem one needs to go back much earlier, to Victor Lebesgue who in 1850 showed that the only solution to the equation

$$x^2 + 1 = y^m, \qquad x, y, m \in \mathbb{Z}, \quad m \geq 3,$$

is the trivial one $(x, y) = (0, 1)$. This is significant as it is one of the earliest non-trivial *exponential Diophantine equation* to have been solved. By *exponential* I mean that one of the unknowns is an exponent. Lebesgue's trick is to factor the left hand-side over $\mathbb{Z}[i]$ and exploit the fact that the two factors $(x + i)$, $(x - i)$ are coprime Gaussian integers and so must be perfect powers (for $m$ odd). Over the next 140 years many equations of the form

$$x^2 + D = y^m, \quad x, y, m \in \mathbb{Z}, \quad m \geq 3,$$

have been solved using Lebesgue's elementary trick. In 1993 John Cohn [11] published an exhaustive survey of this equation which completes the solution for all but 23 values of $D$ in the range $1 \leq D \leq 100$. These are

(4.2)

7, 15, 18, 23, 25, 28, 31, 39, 45, 47, 60, 63, 71, 72, 79, 87, 92, 99, 100,

plus four more values which we write separately: 55, 74, 86, 95. The cases $D = 74$, $D = 86$ were dealt with a little later by Mignotte and de Weger, and $D = 55, 95$ by Bennett and Skinner. This leaves us with the values of $D$ in the range (4.2). It turns out that these are beyond elementary methods because $x + \sqrt{-D}$ and $x - \sqrt{-D}$ need not be coprime.

Let us return to $x^2+7 = y^m$ and attack it by the modular approach. This is based on joint work with Cremona [18] and joint work with Bugeaud and Mignotte [7], but in fact we are following in the footsteps of Kraus [15]. We restrict ourselves to

$$x^2 + 7 = y^p, \qquad x, y \in \mathbb{Z}, \qquad p \geq 11 \text{ prime}, \quad y \text{ even}. \tag{4.3}$$

This is the hard case that is beyond elementary methods. There is no loss of generality in supposing $x \equiv 1 \pmod 4$.

We associate to this solution the Frey curve:

$$E_x : \qquad Y^2 = X^3 + xX^2 + \frac{x^2 + 7}{4}X. \tag{4.4}$$

This has minimal discriminant and conductor

$$\Delta_x = \frac{-7y^{2p}}{2^{12}}, \qquad N_x = 14 \prod_{\substack{q \text{ prime} \\ q|y,\ q\neq 2,7}} q, \tag{4.5}$$

and so is clearly a Frey curve in the sense explained earlier. Now Ribet's Theorem predicts that the Galois representation on the $p$-torsion of $E_x$ arises from a newform of level 14. There is only one newform of level 14 and this turns out to be rational and indeed corresponds to the elliptic curve

$$E : \quad Y^2 + XY + Y = X^3 + 4X - 6,$$

of conductor 14. The elliptic curves $E_x$ and $E$ are related as follows: let $l \neq 2, 7$ be prime, then

(a) if $l \nmid y$, then $\#E_x(\mathbb{F}_l) \equiv \#E(\mathbb{F}_l) \pmod{p}$,
(b) if $l \mid y$, then $\#E(\mathbb{F}_l) \equiv 0, 2l+2 \pmod{p}$.

Here $\#E(\mathbb{F}_l)$ is the number of points on the elliptic curve $E$ over the finite field $\mathbb{F}_l$. We are not yet successful in showing that there are no solutions for all $p \geq 11$, but it is easy to give a criterion for the non-existence of solutions for a given prime exponent $p$.

**Lemma.** *Fix $p \geq 11$. Let $l \neq 2, 7$ be prime satisfying*

(i) $\#E(\mathbb{F}_l) \not\equiv 0, 2l+2 \pmod{p}$
(ii) $\#E_x(\mathbb{F}_l) \not\equiv \#E(\mathbb{F}_l) \pmod{p}$ *for all $x \in \mathbb{F}_l$ satisfying $x^2 + 7 \in \mathbb{F}_l^{*p}$.*

*Then there are no solutions to the equation $x^2 + 7 = y^p$ for the given exponent $p$.*

The lemma is simply a restatement what we said so far. If we choose $l$ in an arbitrary way then it is likely that condition (ii) will not hold. Indeed if $p \nmid (l-1)$ then $\mathbb{F}_l^{*p} = \mathbb{F}_l^*$. However, if $l = np + 1$ then $\#\mathbb{F}_l^{*p} = n$. Hence a correct choice for $l$ would be a prime of the form $np + 1$ where $n$ is small. If criteria (i), (ii) do not hold for some $l$ we choose another of the same form until we succeed. This gives a very efficient method for showing that there are no solutions for a given prime exponent $p \geq 11$; a method that is moreover straightforward to program since it involves only finite field arithmetic and point counting on elliptic curves. In fact it took four days of computations on a modest desktop computer (in 2002) to prove the following [18].

**Lemma** (Cremona-S.)**.** *Equation* (4.3) *has no solutions for* $11 \leq p \leq 10^8$.

Methods of Diophantine approximation—in particular, Baker's theory of linear forms in logarithms—do give bounds for the solutions of many families of Diophantine equations, including (4.3). For example, in 1998 Lesage showed that $p < 6.6 \times 10^{15}$. He also used an elementary method to rule out solutions for $11 \leq p < 5000$.

The story has a happy ending. In 2003, motivated by this work, Maurice Mignotte substantially improved the bounds for linear forms in three logarithms which is precisely what is needed for (4.3). In particular, the new bounds show that $p \leq 1.11 \times 10^9$. However, using information that can be obtained from the modular approach, the theory of linear forms in logarithms can be made to work better and we obtain $p \leq 2 \times 10^8$. Now re-running the old programs we obtain the following theorem [7].

**Theorem** (Bugeaud-Mignotte-S.)**.** *The only solutions to equation* (4.1) *are the following:*

| $m$ | $x$ | $y$ | $m$ | $x$ | $y$ | $m$ | $x$ | $y$ |
|---|---|---|---|---|---|---|---|---|
| 3 | $\pm 1$ | 2 | 3 | $\pm 181$ | 32 | 4 | $\pm 3$ | $\pm 2$ |
| 5 | $\pm 5$ | 2 | 5 | $\pm 181$ | 8 | 7 | $\pm 11$ | 2 |
| 15 | $\pm 181$ | 2 | | | | | | |

The same method has been used to solve $x^2 + D = y^m$ for the 19 outstanding values of $D$ mentioned above.

## 5. Perfect powers in the Fibonacci sequence

There is an important lesson to be learnt from the solution to $x^2+7 = y^m$. It is that the modular approach provides a tremendous amount of local information (i.e. congruences) on the solutions of the Diophantine equation. Progress can be made if we figure out a way of combining this with global information given by other methods (e.g. Baker's theory).

We now turn to another classical Diophantine problem: determine all perfect powers in the Fibonacci sequence. Partial results have been obtained by Ljunggren, Cohn, Wyler, London, Finkelstein, Robbins, Pethö, McLaughlin, etc. It is said that the question was first asked by Mordell in 1950s, although its first appearance in print is in a 1964 paper of John Cohn [10].

Let $\{F_n\}_{n=1}^{\infty}$ be the Fibonacci sequence, defined as usual by $F_0 = 0$, $F_1 = 1$, $F_{n+2} = F_n + F_{n+1}$. The equation we want to solve is

$$F_n = y^m, \qquad n, y, m \in \mathbb{Z}, \quad n \geq 0, \quad m \geq 2.$$

The problem is much more difficult than $x^2 + 7 = y^m$. The reason for the difficulty is that $x^2+7 = y^m$ has solutions for only finitely many values of $m$. We more-or-less solve the problem by showing that there are no solutions for large values of $m$. The Fibonacci powers problem is much more difficult because $F_1 = 1 = 1^m$ gives a solution for all values of $m$. Therefore any method which gives a contradiction for a given fixed exponent (such as one in the previous section) is bound to fail. Again we focus on the difficult case

$$F_n = y^p, \qquad p \geq 7 \text{ is prime, and } n \text{ is odd.} \tag{5.1}$$

Our objective is to show that $n = y = 1$ (the only solution for this case).

It is appropriate here to talk a little about Baker's theory of linear forms in logarithms. Recall the well-known expression for Fibonacci numbers (Binet's formula),

$$F_n = \frac{\lambda^n - \mu^n}{\sqrt{5}}, \qquad \lambda = \frac{1+\sqrt{5}}{2}, \quad \mu = \frac{-1}{\lambda}.$$

The equation $F_n = y^p$ yields

$$\left| \frac{\lambda^n}{\sqrt{5}y^p} - 1 \right| = \frac{1}{\lambda^n y^p \sqrt{5}}.$$

Suppose now that $n > 1$ and so $y > 1$. Then this is saying that $\lambda^n/(y^p\sqrt{5})$ is close to 1, which means that its logarithm is small. Quantitatively we obtain

$$|n \log \lambda - \log \sqrt{5} - p \log y| \leq \frac{2}{\lambda^n y^p \sqrt{5}}. \tag{5.2}$$

Here you see an upper bound for a linear form in logarithms of algebraic numbers. Baker's theory (and its refinements) supply lower bounds for such linear forms. The exact lower bound depends on the version quoted and is likely to be complicated. However, you can obtain a lower bound of the form

$$\frac{C_1}{y^{C_2(\log p)^{C_3}}} \leq |n \log \lambda - \log \sqrt{5} - p \log y| \leq \frac{2}{\lambda^n y^p \sqrt{5}},$$

for some positive constants $C_1$, $C_2$, $C_3$. Plainly, if $p$ is large, then the left-most term is larger than the right-most term, giving a contradiction. Thus $p$ is bounded by some bound that depends on the constants $C_i$. Mignotte's bounds for linear forms in three logarithms show that if $n > 1$ then $p \leq 2 \times 10^8$.

By a rather involved detour through Thue equations one also obtains bounds for the index $n$ in terms of $p$. This step uses ideas of Bugeaud and Győry and yields bounds that are rather complicated to state (as they involve many terms), but they very roughly say that $n$ is at most $p^{10p}$. Even with $p = 7$ we obtain $n \leq 3 \times 10^{46}$.

We would like to apply the modular approach here. We skip over all the details you have seen before (Frey curve, level-lowering, etc.). However all you need to know is the following fact which I hope you will readily believe following what you saw in the previous section.

**Fact:** Fix a prime exponent $p \geq 7$ and another prime $l \neq 2, 5$. There exists an easily computable and fairly small subset $\mathcal{S}(l, p) \subset \mathbb{F}_l$ such that if $(n, y, p)$ is a solution to (5.1) then $\overline{F_n} \in \mathcal{S}(l, p)$.

By $\overline{F_n}$ we obviously mean the reduction of $F_n$ modulo $l$. In other words, the modular approach is giving us stringent congruence conditions for the Fibonacci numbers that are perfect powers. We want congruences for $n$ and not for $F_n$. Let $M_l$ be the period of the Fibonacci sequence modulo $l$. Let

$$\mathcal{N}(l, p) = \{m \in \mathbb{Z}/M_l \ : \ \overline{F_m} \in \mathcal{S}(l, p)\}.$$

It follows that if $(n, y, p)$ is a solution to (5.1) then $\tilde{n} \in \mathcal{N}(l, p)$, where $\tilde{n}$ denotes reduction modulo $M_l$. In other words, we obtain stringent conditions on the index $n$ modulo $M_l$. Now it is easy to show that $M_l$ divides $l^2 - 1$,

and it is likely to be a composite number. In fact with a careful choice of $l$ we can ensure that $M_l$ is a 'smooth integer', which means that it is divisible only by small primes.

Let $l_1, \ldots, l_r$ be distinct primes write $M_i$ for $M_{l_i}$. We have congruence conditions for $n$ modulo each $M_i$. By the Chinese Remainder Theorem we obtain congruence conditions for $n$ modulo $M = \operatorname{lcm}(M_1, M_1, \ldots, M_r)$. Here an arbitrary choice of $l_i$ would lead to a combinatorial explosion of possibilities when we attempt to lift congruences modulo $M_i$ to congruences modulo $M$. However choosing the $l_i$ so that the $M_i$ are smooth and have many prime factors in common maximises the probability of contradictions and we get a few congruences for $n$ modulo a large $M$.

For example, fix $p = 7$. By an appropriate choice of hundreds of primes $l$ we obtain, utilising a computer,

$$\tilde{n} \in \left\{\tilde{1}, \tilde{a}, \tilde{b}, \tilde{c}\right\} \subset \mathbb{Z}/M$$

where

$$\begin{aligned} a &= 1007045988544277770241794182739444114829990027 99, \\ b &= 1007045988544277770241794182739444114829990028 01, \\ c &= 2014091977088555540483588365478888229659980055 99, \\ M &= 2^5 \times 3^3 \times 5^2 \times 7 \times 11 \times \cdots \times 109. \end{aligned}$$

Thus the index $n$ belongs to the set

$$1,\ a,\ b,\ c,\ 1+M,\ a+M,\ b+M,\ c+M,\ 1+2M, \ldots .$$

Note that $a, b, c, M > 10^{47}$ and we said previously that $n \leq 3 \times 10^{46}$. Hence $n = 1$ as desired. Notice how local information obtained from the modular approach is combined with global information obtained from Diophantine approximation.

We have solved the problem for $p = 7$. In fact this strategy is fairly realistic for primes $p \leq 1000$, but is completely incapable of dealing with much larger primes. Our bound for $p \leq 2 \times 10^8$ seems hopelessly out of reach.

However, it is possible to use the congruences from the modular approach to prove that $n \equiv \pm 1 \pmod{p}$ for all $p \leq 2 \times 10^8$. Writing $n = kp \pm 1$ we can rewrite the inequality (5.2) as

$$\left| p \log\left(\lambda^k / y\right) - \log\left(\sqrt{5}/\lambda^{\pm 1}\right) \right| \leq \frac{2}{\lambda^n y^p \sqrt{5}}.$$

Thus what was a linear form in three logarithms has miraculously transformed into a linear form in two logarithms. Baker's theory for linear forms in logarithms works much better now, and using bounds by Laurent, Mignotte and Nesterenko we obtain $p < 733$. Our bound for $n$ in

terms of $p$ now gives $n < 10^{8733}$ which is within reach of our previous arguments, and we are able to complete the proof of the following theorem [6].

**Theorem** (Bugeaud-Mignotte-S.)**.** *The only perfect powers in the Fibonacci sequence are* $F_0 = 0$, $F_1 = F_2 = 1$, $F_6 = 8$ *and* $F_{12} = 144$.

The computations needed took about 158 hours on a modest desktop computer and utilised the computer packages PARI [1] and MAGMA [4].

## 6. Multi-Frey approach

We saw how congruences obtained from the modular approach can help to solve Diophantine equations. The *multi-Frey approach* is a newly developed variant of the modular approach. It uses congruences obtained from several Frey curves simultaneously. It has been used to attack *multiply-exponential Diophantine equations*, in other words Diophantine equations involving several unknown exponents. Here is a specimen result [8].

**Theorem** (Bugeaud-Mignotte-S.)**.** *Suppose* $3 \leq q < 100$ *is prime. The only solutions to the equation*

$$q^u x^n - 2^r y^n = \pm 1, \qquad x,\ y \text{ non-zero integers}, \quad u,\ r \geq 0, \quad n \geq 3$$

*are*

$$1 - 2 = -1, \quad 3 - 2 = 1, \quad 3 - 4 = -1, \quad 9 - 8 = 1, \quad 5 - 4 = 1,$$
$$7 - 8 = -1, \quad 17 - 16 = 1, \quad 31 - 32 = -1, \quad 5 \times 2^4 - 3^4 = -1,$$
$$19 \times 3^3 - 8^3 = 1, \quad 17 \times 7^3 - 18^3 = -1, \quad 37 \times 3^3 - 10^3 = -1,$$
$$43 \times 2^3 - 7^3 = 1, \quad 53 - 2 \times 3^3 = -1.$$

The proof uses all the methods mentioned previously, together with three simultaneous Frey curves and a very deep theorem of Bennett on equations of the forms $Ax^n - By^n = \pm 1$.

Currently I am working with Szabolcs Tengely on Diophantine equations of the form $x^2 + q^u = 2^r y^n$ using the multi-Frey approach and a range of classical methods.

## 7. Some open problems

It is dishonest to give the impression that the current methods have flattened each and every problem. I would like to mention two of my favourite problems where good progress has been made using the modular and other approaches, but which are still out of reach.

The first problem is to solve

$$x^3 + y^3 = z^n, \qquad x,\ y,\ z \text{ are non-zero coprime integers}, \quad n \geq 3.$$

Bruin [3] showed, using descent and Chabauty arguments, that there are no solutions for $n = 4, 5$. Kraus [15] used the modular approach to show the same for prime exponents $n$ with $17 \leq n < 10^4$. By refining Kraus' approach, Dahmen [14] shows that there are no solutions for $n = 5, 7, 11, 13$. Thus we know that there are no solutions for $n \leq 10^4$. Although this range is easily extendible, there is no known method for bounding the exponent $n$. Recently Chen and myself [9] have shown that the set of exponents $n$ for which this equation has solutions (in non-zero coprime integers) has density 0; the proof uses a combination of the modular approach and the Brauer–Manin obstruction to points on curves.

The second problem is to solve.

$$x^2 - 2 = y^m, \qquad x, y \text{ are integers}, \quad m \geq 3.$$

This problem is similar to the Fibonacci powers problem in that there is a solution $1^2 - 2 = (-1)^m$ for all odd exponents $m$. However any bound on $x$ in terms of $m$ is likely to be something like $10^{m^m}$. For a further discussion of this problem see Henri Cohen's new book [13] (in particular, Volume II, pages 517–521). That book also contains a detailed exposition of the modular approach (Volume II, Chapter 15) and is an indispensable handbook for any lover/solver of Diophantine equations.

## 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, *Powers in recurrence sequences : Pell equations*. Trans. Amer. Math. Soc. **357** (2005), 1675–1691.

[3] N. Bruin, *On powers as sums of two cubes*. Pages 169–184 of *Algorithmic number theory* (edited by W. Bosma), Lecture Notes in Comput. Sci. **1838**, Springer, Berlin, 2000.

[4] 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/`)

[5] 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.

[6] 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.

[7] 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.

[8] Y. Bugeaud, M. Mignotte and S. Siksek, *A multi-Frey approach to some multi-parameter families of Diophantine equations*. Canadian Journal of Mathematics **60** (2008), no. 3, 491–519.

[9] I. Chen and S. Siksek, *Perfect powers expressible as sums of two cubes*. Journal of Algebra, to appear.

[10] J. H. E. Cohn, *On square Fibonacci numbers*; J. London Math. Soc. **39** (1964), 537–540.

[11] J. H. E. Cohn, *The Diophantine equation $x^2+C = y^n$*. Acta Arith. **LXV.4** (1993), 367–381.

[12] J. E. Cremona, Algorithms for Modular Elliptic Curves. 2nd edition, Cambridge University Press, 1997.

[13] H. Cohen, *Number Theory, Vol. I: Tools and Diophantine Equations* and *Vol. II: Analytic and Modern Tools*. Springer-Verlag, GTM **239, 240**, 2007.
[14] S. R. Dahmen, *Classical and modular methods applied to Diophantine equations*. University of Utrecht Ph.D. thesis, 2008.
[15] A. Kraus, *Sur l'équation* $a^3 + b^3 = c^p$. Experimental Mathematics **7** (1998), No. 1, 1–13.
[16] B. Poonen, E. F. Schaefer and M. Stoll, *Twists of* $X(7)$ *and primitive solutions to* $x^2 + y^3 = z^7$. Duke Math. J. **137** (2007), 103–158.
[17] K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*. Invent. Math. **100** (1990), 431–476.
[18] S. Siksek and J. E. Cremona, *On the Diophantine equation* $x^2 + 7 = y^m$. Acta Arith. **109.2** (2003), 143–149.
[19] W. A. Stein, *Modular Forms: A Computational Approach*. American Mathematical Society, Graduate Studies in Mathematics **79**, 2007.
[20] R. L. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*. Annals of Math. **141** (1995), 553–572.
[21] 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*: samirsiksek@yahoo.com
*URL*: http://www.warwick.ac.uk/staff/S.Siksek/