UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
INTERNATIONAL ATOMIC ENERGY AGENCY
INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS
I.C.T.P., P.O. BOX 586, 34100 TRIESTE, ITALY, CABLE: CENTRATOM TRIESTE

SMR.1004/2

SUMMER SCHOOL ON ELLIPTIC CURVES

(11- 29 August 1997)

On the equation $x^p + y^q = z^r$

A. Kraus
Université de Paris VI
Institut de Mathématiques, Case 247
4, Place Jussieu
F-75252 Paris Cedex 05
France

These are preliminary lecture notes, intended only for distribution to participants

Conference Trieste, August 24-29, 1997

On the equation $x^p + y^q = z^r$

Alain Kraus

Introduction

Let p, q and r be three integers ≥ 2. In this text we shall survey the main lines on works which have been done on the diophantine equation

$$x^p + y^q = z^r. \tag{1}$$

It has a long history in relation with Fermat's Last Theorem. Of course there are in general plenty of solutions to this kind of equations. For instance, let p be an odd number and a, b be two integers. Then taking $c = a^p + b^p$, we have the equality

$$(ac)^p + (bc)^p = (c^{\frac{p+1}{2}})^2.$$

From an arithmetic point of view, these solutions are not very interesting. That is the reason why we introduce the following definition : given an integral solution (a, b, c) to the above equation, we shall say that this solution is proper if a, b, and c are pairwise coprime and that it is non trivial if abc is non zero. Let us denote by $S(p, q, r)$ the set of the proper non trivial integral solutions of the equation (1).

The main problem related to this equation is the following :

Problem. *Describe the set $S(p, q, r)$.*

Let us define the *characteristic* of the equation (1) to be

$$\chi(p,q,r) := \frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1.$$

The study of the equation (1) depends on the fact whether $\chi(p, q, r)$ is > 0 (the spherical case), is zero (the euclidean case) or is < 0 (the hyperbolic case). In light of the *abc* conjecture, one might expect $S(p, q, r)$ to be empty if the exponents p, q and r are large enough. In this way it is tempting to make the following conjecture, which we may call the Asymptotic Generalized Fermat Conjecture (see for instance [7], p. 515 or [10], p. 2) :

Conjecture 1. *The set of triples coprime integers (a^p, b^q, c^r), such that $a^p + b^q = c^r$ and $\chi(p, q, r) < 0$, is finite.*

There are only ten known solutions satisfying a generalized Fermat equation of the above type, with the condition $\chi(p, q, r) < 0$:

$$1^p + 2^3 = 3^2, \quad 2^5 + 7^2 = 3^4, \quad 7^3 + 13^2 = 2^9, \quad 2^7 + 17^3 = 71^2, \quad 3^5 + 11^4 = 122^2,$$
$$17^7 + 76271^3 = 21063928^2, \quad 1414^3 + 2213459^2 = 65^7, \quad 9262^3 + 15312283^2 = 113^7,$$
$$43^8 + 96222^3 = 30042907^2, \quad 33^8 + 1549034^2 = 15613^3.$$

The five larger solutions in this list were found by a computer search by F. Beukers and D. Zagier at Utrecht in 1993 (cf. [3]). In each solution an exponent 2 occurs. This has led Tijdeman and Zagier to raise the following question :

Question. *Do there exist integers p, q and $r \geq 3$ such that $S(p, q, r)$ is non empty ?*

D. Bernardi in 1997, by a computer search as well, has not found any proper non trivial solution (a, b, c) to the equation (1) if the maximum in absolute value of a^p, b^q and c^r is $< 2^{63}$ and if p, q and r are ≥ 3.

A. The spherical case

The possible sets $\{p, q, r\}$ are $\{2, 2, r\}$ with $r \geq 2$, $\{2, 3, 3\}$, $\{2, 3, 4\}$ and $\{2, 3, 5\}$. In that case, the proper solutions to the equation (1) correspond to rational points on certain curves of genus zero (see [7], 7, p. 536). The first result which has long been known is the following :

Theorem 1. *Suppose $\chi(p, q, r) > 0$. The set $S(p, q, r)$ is infinite.*

There is in fact the presence of *parametrised* solutions which do not exist in the non-spherical cases :

Definition 1. *A parametrised solution of the equation (1) is a triple (X, Y, Z) of homogeneous polynomials in $\mathbf{Q}[s, t]$, with $gcd(X, Y, Z) = 1$ and $XYZ \neq 0$, such that $X^p + Y^q = Z^r$. Two parametrised solutions (X, Y, Z) and (X', Y', Z') are said to be equivalent if there exists a matrix A in $\mathbf{GL}_2(\mathbf{Q})$ such that*

$$X(A(s,t)) = X'(s,t), \quad Y(A(s,t)) = Y'(s,t) \quad \text{and} \quad Z(A(s,t)) = Z'(s,t).$$

F. Beukers has shown in 1995, in a more general setting, the following result ([3], th. 1.2) :

Theorem 2. *Suppose $\chi(p, q, r) > 0$. There exists a finite number of parametrised solutions classes, from which all solutions of the equation (1) can be obtained by specialisation of the variables s and t to rational integral values.*

For argument's sake, let us consider the equation

$$x^3 + y^3 = z^2.$$

In 1993 D. Zagier found three classes of parametrised solutions which yield all integral solutions to this equation (cf. *loc. cit.*, 7) :

$$X = s^4 + 6s^2t^2 - 3t^4, \quad Y = -s^4 + 6s^2t^2 + 3t^4, \quad Z = 6st(s^4 + 3t^4).$$
$$X = (1/4)(s^4 + 6s^2t^2 - 3t^4), \quad Y = (1/4)(-s^4 + 6s^2t^2 + 3t^4), \quad Z = (3/4)st(s^4 + 3t^4).$$
$$X = s^4 + 8st^3, \quad Y = -4s^3t + 4t^4, \quad Z = s^6 - 20s^3t^3 - 8t^6.$$

D. Zagier has also found the classes of parametrised solutions which yield all integral solutions to the equations :

$$x^4 + y^3 = z^2 \quad \text{and} \quad x^4 + y^2 = z^3.$$

A complete set of parametrised solutions, that is $\mathbf{GL}_2(\mathbf{Q})$-inequivalent, of the equation $x^5 + y^3 = z^2$, which would yield to all integral proper non trivial solutions, is still unknown. We only know fifteen of them (cf. *loc. cit.*, 5).

B. The euclidean case

The list of possible sets $\{p, q, r\}$ are $\{3,3,3\}$, $\{2,4,4\}$, $\{2,3,6\}$. In this case the set $S(p,q,r)$ corresponds to rational points on certain curves of genus one (see for instance [7], 6, p. 534). The situation in this case has long been known, thanks to Fermat, Leibniz, Bachet and Euler :

Theorem 3. *The only proper non trivial solution in the euclidean case corresponds to the equality* $1 + 2^3 = 3^2$.

For instance, one can finds the proofs that the sets $S(3,3,3)$ and $S(4,4,2)$ are empty in [17], p. 37-45, by mean of arguments using infinite descent.

C. The hyperbolic case

In this case the first fondamental known result is due to H. Darmon and A. Granville in 1993 (cf. [7], 3, p. 524).

I. Darmon and Granville's Theorem

This theorem is the following :

Theorem 4. *Suppose* $\chi(p,q,r) < 0$. *The set* $S(p,q,r)$ *is finite.*

Let $\bar{\mathbf{Q}}$ be an algebraic closure of $\mathbf{Q}$. The proof of this theorem uses the result below which is based on the Riemann Existence Theorem :

Theorem 5. *Let p, q and r be three integers ≥ 2 such that $\chi(p,q,r) < 0$. There exists an irreducible smooth curve X defined over $\bar{\mathbf{Q}}$, whose genus is ≥ 2, and a finite Galois covering $\pi : X \to \mathbf{P}_1$ such that :*

(i) the covering π in unramified outside $\{0, 1, \infty\}$;

(ii) the ramification indices of the points 0, 1 *and* ∞ *are p, q and r respectively.*

Since the map π is defined over $\bar{\mathbf{Q}}$, it can be defined over some finite extension K of $\mathbf{Q}$. Let d the degree of π. Define V the set of finite places of K at which the covering π has bad reduction : say that a finite place v belongs to V if the graph of π has bad reduction at v. The set V is finite.

Suppose from now on that we are given a model of X over the ring of integers of K. Given a point t in $\mathbf{P}_1(K) - \{0,1,\infty\}$, we define L_t to be the field extension of K generated by the coordonnates of the points P in $X(\bar{\mathbf{Q}})$ which belong to the fiber $\pi^{-1}(t)$. Since π is defined over K, the extension L_t of K is Galois. In other respects the degree of L_t over K is at most d; in fact it divides d.

We need some information about the ramification of the extension L_t/K. Let v a non archimedian place of K. We define arithmetic intersection numbers

$$(t.0)_v := \mathrm{Max}(v(t), 0), \quad (t.1)_v := \mathrm{Max}(v(t-1), 0) \quad \text{and} \quad (t.\infty)_v := \mathrm{Max}(v(1/t), 0).$$

The following result describes the ramification of the extension L_t/K (cf. [2]and [7]) :

Theorem 6. *(Beckmann, Darmon, Granville) Let t be a point in $\mathbf{P}_1(K) - \{0,1,\infty\}$ and v a finite place of K which is not in V. If the following congruences are satisfied*

$$(2) \qquad (t.0)_v \equiv 0 \text{ mod. } p, \quad (t.1)_v \equiv 0 \text{ mod. } q \quad \textit{and} \quad (t.\infty)_v \equiv 0 \text{ mod. } r,$$

the extension L_t/K is unramified at v.

Let us now see how these results imply Darmon and Granville 's theorem. Let us consider (a,b,c) a proper non trivial solution to the equation (1). Let us take

$$(3) \qquad t = \frac{a^p}{c^r}.$$

Evidently t is distinct from 0, 1 and ∞, and the congruences (2) are satisfied. The theorem 6 implies that the extension L_t/K is unramified at the finite places which are not in V. On the other hand the degree of L_t over K is $\leq d$. We then deduce from the Minkowski's theorem that there are only finitely many such fields L_t which may arise from a proper solution of the equation (1). So the compositum L of all such fields L_t is a finite extension of K and in particular of $\mathbf{Q}$.

Suppose now that the set $S(p,q,r)$ is infinite. In this case, there would exist infinitely many elements t of K of the form (3). Those elements would then lead to infinitely many points of the curve X rational over L. But since the genus of X is ≥ 2, the set $X(L)$ is finite by Falting's theorem. We so get a contradiction and then obtain the theorem.

Remark. It is in general very difficult to find an explicit covering $\pi : X \rightarrow \mathbf{P}_1$ as above. Anyway the proof of the previous theorem shows that we may deduce the description of the set $S(p,q,r)$, by analysing the set of the rational points of an algebraic curve defined over some number field (which is not easy at all). H. Darmon gave another formulation of this fact in terms of, what he calls, the M-curves (see [10]).

II. The known results towards the Asymptotic Generalized Fermat Conjecture

They all use the known results on the Taniyama-Weil conjecture (cf. [12], [23]and [21]) : an elliptic curve defined over $\mathbf{Q}$ which is semi-stable at 2 and 3 is *modular*. Moreover, it seems that recently, Conrad, Diamond and Taylor have extended this result : an elliptic curve defined over $\mathbf{Q}$ whose conductor is not divisible by 27 is modular.

The first result in the direction of the Asymptotic Generalized Fermat Conjecture is the Last Fermat's Theorem proved by Wiles and Ribet (cf. [18]and [23]) :

Theorem 7. *Let n be an integer ≥ 3. The set $S(n,n,n)$ is empty.*

The next theorem has been proved by H. Darmon and L. Merel in 1996 (cf. [6], [9]), at least if n is prime ≥ 7. The cases of various small exponents $n \leq 9$ have been treated by Poonen :

Theorem 8. *a) Let n be an integer ≥ 4. The set $S(n,n,2)$ is empty.*
b) Let n be an integer ≥ 3. If the Taniyama-Weil conjecture is true, $S(n,n,3)$ is empty.

The theorem below is a consequence of the results obtained in [5]and [9] :

Theorem 9. *Let n be an integer ≥ 2. The set $S(4,n,4)$ is empty.*

I proved in 1997 the following result at least if p is prime ≥ 17 (cf. [14]) ; the case $3 \leq p \leq 13$ can in fact be treated by ad hoc arguments :

Theorem 10. *a) Let p be a prime number such that $3 \leq p < 10^4$. The set $S(3,3,p)$ is empty.*
b) Let n and m be two integers ≥ 2 and p be a prime number ≥ 3. The sets $S(3n,3m,p)$ and $S(3n,p,3m)$ are empty.

For the proof of the theorem 10, we assumed in [14] that the Taniyama-Weil conjecture is true. Thanks to the recent result of Conrad, Diamond and Taylor this statement is now unconditional.

Actually, if p is explicitly given, we dispose of an algorithm, which allows one often in practice to prove that the set $S(3,3,p)$ is empty (cf. *loc. cit.)*. This is for instance the case if $p = 479909$, which is the forty thousandth prime number.

III. The key ingredients to obtain such results

All the arguments used to prove these results are of modular type. The nature of these arguments can be divided into three parts :

a) the recent results obtained on the Taniyama-Weil conjecture ;
b) the construction of, what we usually call, Frey curves ;
c) Galois properties of the division points of elliptic curves.

From now on, for the sake of simplicity, we will suppose that $n = p$ is a prime number which is ≥ 7. Let $\bar{\mathbf{Q}}$ be an algebraic closure of $\mathbf{Q}$, say the one which is contained in $\mathbf{C}$.

Let us now explain the general method which was used to prove the above theorems for the exponent p. At first, we consider a proper non trivial solution (a,b,c) to one of the equations below :

$$x^p + y^p = z^p, \quad x^p + y^p = z^2, \quad x^p + y^p = z^3, \quad x^4 - y^4 = z^p, \quad x^3 + y^3 = z^p.$$

Then we construct an elliptic curve $F = F(a,b,c)$ defined over $\mathbf{Q}$ such that the following conditions are satisfied :

(i) the curve F has semi-stable reduction at p, and the exponent at p in its minimal discriminant is divisible by p ;
(ii) the representation $\rho_p^F : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \rightarrow \mathrm{Aut}(F[p])$, of the Galois group $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ in the p-division points of F is irreducible ; moreover ρ_p^F is unramified outside a set $T \cup \{p\}$, T being contained in $\{2,3\}$;
(iii) there exists a prime number at which F has multiplicative reduction.

Definition 2. *We shall call such a curve F a Frey curve associated to (a,b,c).*

Let us denote by

$$s \mapsto \sum_{n \geq 1} \frac{a_n(F)}{n^s},$$

the Hasse-Weil L function of F. To such a representation ρ_p^F, J.-P. Serre associates two integers : a weight k which is ≥ 2 and a conductor $N = N(\rho_p^F)$ which is prime to p (cf. [20]). These invariants measure the ramification of ρ_p^F. In our cases we have $k = 2$ (condition (i)) and the prime numbers which may divide N are 2 or 3. If F is *modular*, which is known to be always the case, except perhaps if (a,b,c) belongs to $S(p,p,3)$, it is now proved that the following condition holds (cf. [21], 2.2, *Remarques* 2)) :

there exists a newform in $S_2^{new}(N)$, that is a cusp newform of weight 2 and of trivial character for the congruence subgroup $\Gamma_0(N)$, in the sense of [1], whose the q-expansion at infinity is

$$f = q + \sum_{n\geq 2} a_n q^n \qquad (q = \exp(2\pi i\tau)),$$

and a prime ideal $\mathcal{P}$ above p of the ring of the algebraic integers, such that, for almost all prime l, we have the congruence :

$$a_l(F) \equiv a_l \text{ mod. } \mathcal{P}.$$

In our situation, we are in one of the following cases :

(c_1) the dimension over $\mathbb{C}$ of $S_2^{new}(N)$ is zero, so that f, and then (a,b,c), cannot exist;
(c_2) the Fourier coefficients a_n of f are rational integers.

In the case (c_2), there exists an elliptic modular curve E defined over $\mathbb{Q}$, of conductor N, whose Galois representation in its p division points is isomorphic to ρ_p^F. In fact, in this case, if (a,b,c) belongs to one of the sets $S(p,p,2)$, $S(p,p,3)$ or $S(4,p,4)$, the elliptic curve E has *complex multiplications* and has a point of order two or three rational over $\mathbb{Q}$. Then by mean of arguments concerning the Galois properties of the division points of elliptic curves (see below IV.1), we are then led to a contradiction for the existence of the solution (a,b,c).

We have to notice the important fact that in all the above treated cases, it has been possible to construct a Frey curve for each proper solution of the equations considered. This has been done by H. Darmon. It is nowdays really a crucial step in the direction of proving that a generalized Fermat equation $x^p + y^q = z^r$ has no proper non trivial integer solution.

IV. The main arguments of the demonstrations

Let us begin by stating the Galois properties of the p-division points of elliptic curves over $\mathbb{Q}$ we need for the proofs. Let us recall that, from now on, the letter p, if there is no supplementary precision, refers to a prime number ≥ 7.

IV.1. Two results on the division points of elliptic curves

Let E be an elliptic defined over $\mathbb{Q}$. Let

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

the representation given by its p-division points. In [19], J.-P. Serre has described all the possibilities for the image of ρ_p. For our purpose, we are essentially faced with the problem of knowing if there exists an elliptic E' over $\mathbb{Q}$, non isogenous over $\mathbb{Q}$ to E, such that the Galois representations given by the p-division points of E and $E'$are isomorphic : this problem addresses a question raised by B. Mazur in 1978 (cf. [15], p. 133).

IV.1.1. The case of a normalizer of a split Cartan subgroup

Let us suppose that the image of ρ_p is contained in the normalizer of a split Cartan subgroup (cf. [19], p. 278-283). For instance, this is such the case if E has complex multiplications by an order of a quadratic field K and if p splits in K. In 1984 F. Momose has proved the following theorem ([16], prop. (3.1)) :

Theorem 11. *Suppose p is ≥ 11 and distinct from 13. Let l be an odd prime number. Then E has potentially good reduction at l.*

As a consequence of this theorem, in the direction of the above question raised by Mazur, we have the result below ([13], th. 1) :

Theorem 12. *Suppose p is ≥ 11 and distinct from 13. Let E' be an elliptic curve over $\mathbb{Q}$ such that the Galois representations given by the p-division points of E and E' are isomorphic. Then the conductors of E and E' are equal.*

We would like of course to conclude that E and E' are isogenous. This is actually true if E has complex multiplications, at least if its modular invariant is distinct from 0 and 1728 (cf. *loc. cit.*).

IV.1.2. The case of a normalizer of a non split Cartan subgroup

Let us suppose now that the image of ρ_p is contained in the normalizer of a non split Cartan subgroup (cf. [19], p. 278-283). This is for instance the situation if E has complex multiplications by an order of a quadratic field K and if p remains prime in K. The theorem below is crucial for the above results ([9], th. 8.1) :

Theorem 13. *Suppose $p \geq 5$, and that the following conditions are satisfied :*
a) the curve E has a $\mathbb{Q}$-rational subgroup of order two or three ;
b) the image of ρ_p is a normalizer of a non split Cartan subgroup.
Then the modular invariant of E belongs to $\mathbb{Z}[\frac{1}{p}]$.

The assumption a) is essential : let E be the elliptic curve of equation

$$y^2 = x^3 + 27786\,x + 30624566 \qquad \text{(cf. [7], p. 531).}$$

This curve has no Q-rational subgroup of order two or three. The image of the Galois representation in the 7-division points of E is a normalizer of a non split Cartan subgroup, and the modular invariant j of E is

$$j = \frac{2^9.3^3.11^3.421^3}{113^7}.$$

IV.2. Last Fermat's Theorem

Let us be given an element (a, b, c) belonging to the set $S(p, p, p)$. Then it is now a classical fact that the elliptic curve of equation

$$y^2 = x(x - a^p)(x + b^p),$$

is a Frey modular curve. The conductor of its mod p representation is 2. This contradicts the existence of (a, b, c) because the dimension of the vector space $S_2^{new}(2)$ is zero.

IV.3. The equation $x^p + y^p = z^2$

Let us be given a triple of integers (a, b, c) belonging to the set $S(p, p, 2)$. At first we are faced to the problem of constructing a Frey curve associated to (a, b, c). In accordance with the definition of a Frey curve (def. 2), we have to search for an elliptic curve over Q with the most possible pth powers in its minimal discriminant. For this aim, let us consider two indeterminates u and v and the elliptic curve over the field $\mathbf{Q}(u, v)$ of equation

$$y^2 = x^3 + u\,x^2 + v\,x.$$

It arises from the universal family over the modular curve $X_0(2)$, which parametrises the elliptic curves with a rational point of order two. The standard invariants associated to this equation are (cf. [22]) :

$$c_4 = 16(u^2 - 3v) \quad \text{et} \quad \Delta = 16v^2(u^2 - 4v).$$

Thanks to the equality $a^p + b^p = c^2$, we then can hope to construct a Frey curve associated to (a, b, c). This is such the case : let F be the elliptic curve of equation

$$F: \quad y^2 = x^3 + 2c\,x^2 + a^p\,x.$$

Let $\Delta(F)$ its discriminant. We have

$$\Delta(F) = 2^6.a^{2p}.b^p.$$

This curve is a Frey modular curve with $T = \{2\}$. Actually, we can normalize (a, b, c) such that the conductor N defined by Serre of the mod p representation ρ_p^F divides 32. Since the dimension of the vector spaces $S_2^{new}(2^k)$ is zero if $0 \leq k \leq 4$, we can actually suppose that we have $N = 32$. But there is just one normalized newform of weight 2 and level 32 : it corresponds to the elliptic curve E of conductor 32, noted 32A in Cremona's tables ([4], p. 91), of equation

$$E: \quad y^2 = x^3 - x.$$

The curve E has complex multiplications by the ring of Gaussian integers $\mathbf{Z}[i]$. Let ρ_p^E its mod p representation. The representations ρ_p^E and ρ_p^F are isomorphic. The image of of ρ_p^E is a normalizer of a *split* Cartan subgroup if $p \equiv 1$ mod. 4, and is a normalizer of a *non split* Cartan subgroup if $p \equiv 3$ mod. 4. We then obtain a contradiction to the existence of (a, b, c) in the following way :

1) suppose $p \equiv 1$ mod. 4 and $p \geq 17$. Using the theorem 12, we see that the conductor of the curve F must necessarily be 32, contradicting the fact that F is a Frey curve (condition (iii)). Let us mention that we can also tackle this case using a result of Kamienny on Eisenstein quotients over imaginary quadratic fields (see [6], prop. 1.6). The case $p = 13$ can be treated by mean of ad hoc arguments.

2) Suppose $p \equiv 3$ mod. 4. In this case it is easy to obtain a contradiction for the existence of (a, b, c) from the theorem 13, by showing that p cannot divide ab.

IV.4. The equation $x^p + y^p = z^3$

To construct a Frey curve associated to a proper non trivial solution (a, b, c) of this equation, one may think about the modular curve $X_1(3)$, which parametrises the elliptic curves with a rational point of order three. To be more precise, if u and v are two indeterminates, we can consider the elliptic curve over the field $\mathbf{Q}(u, v)$ of equation

$$y^2 + u\,xy + v\,y = x^3.$$

It has a rational point of order 3 : the point $(0, 0)$.The standard invariants associated to this equation are

$$c_4 = u(u^3 - 24v) \quad \text{and} \quad \Delta = v^3(u^3 - 27v).$$

Then one can consider the elliptic curve F of equation

$$F: \quad y^2 + 3c\,xy + b^p\,y = x^3.$$

The discriminant $\Delta(F)$ of this equation is

$$\Delta(F) = 3^3.a^p.b^{3p}.$$

The elliptic curve F is a Frey curve with $T = \{3\}$, and the conductor of its mod p representation divides 27. Since the dimension of the vector spaces $S_2^{new}(3^k)$ is zero if $0 \leq k \leq 2$, we can actually suppose that we have $N = 27$. The dimension of the vector space $S_2^{new}(27)$ is one, and the normalized basis corresponds to the elliptic curve E of conductor 27, noted 27A in Cremona's tables ([4], p. 91), of equation

$$E: \quad y^2 + y = x^3.$$

The curve E has complex multiplications by the ring $\mathbf{Z}[\zeta]$, ζ being a cubic root of unity. Next, if we assume that F is modular, which is not known to be true in this case, we contradict the existence of (a, b, c) by modular arguments in the same way of those used in the section IV.3.

IV.5. The equation $x^4 - y^4 = z^p$

Let (a, b, c) be an element belonging to $S(4, p, 4)$. In this case, to construct a Frey curve, we use the identity

$$(a + b)(a - b)(a^2 + b^2) = c^p.$$

Let us put

$$A = (a + b)^2, \quad B = (a - b)^2 \quad \text{and} \quad C = a^2 + b^2.$$

We notice that $A + B - 2C = 0$. The elliptic curve of equation $y^2 = x(x + A)(x - B)$, that is

$$y^2 = x^3 + 4ab\, x^2 - (a^2 - b^2)^2\, x,$$

is then a Frey modular curve with $T = \{2\}$. We can normalize (a, b, c) such that the conductor of its mod p representation divides 32, and we are led again to a contradiction (cf. section IV.2).

IV.6. The equation $x^3 + y^3 = z^p$

From now on, we consider an element (a, b, c) of the set $S(3, 3, p)$.

IV.6.1. The Frey curve

Let ξ be a cubic root of unity. In order to find a Frey curve associated to (a, b, c) we use the identity

$$(a + b)(a + \xi b)(a + \xi^2 b) = c^p.$$

We then notice that putting

$$A = \xi(a + \xi b) \quad \text{and} \quad B = \xi^2(a + \xi^2 b),$$

we have the equality $A + B + (a + b) = 0$. Next, we consider the elliptic curve over $\mathbf{Q}(\sqrt{-3})$ given by the equation

$$y^2 = x(x - A)(x + B).$$

After twisting that equation over $\mathbf{Q}(\sqrt{-3})$ by $(-3)^{\frac{1}{4}}$, we obtain the ellipic curve defined over $\mathbf{Q}$ of equation

$$y^2 = x^3 + 3ab\, x + b^3 - a^3.$$

It is a Frey modular curve with the set $T = \{2, 3\}$ (cf. [7], p. 530 and [14]). In fact we can normalize (a, b, c) such that the conductor of its mod p representation divides 72.

The assertion b) of the theorem 10 is a direct consequence of the following proposition, which can be obtained by modular arguments, applied with the Frey curve above, analogue to those already mentioned (cf. [14], th. 6.1) :

Proposition 1. *The number c is odd and ab is not divisible by 4, so that the 2-adic valuation of ab is 1.*

IV.6.2. The algorithm

Let us describe now an algorithm which allow one often in practice to prove that the set $S(3, 3, p)$ is empty.

We have to consider the elliptic curve E over $\mathbf{Q}$ of equation

$$y^2 = x^3 + 6x - 7.$$

It is the curve numbered 72A in Cremona's tables. Its conductor is 72. If l is a prime number ≥ 5, let us denote by $n_l(E)$ the number of points rational over the field $\mathbf{F}_l$, of the curve $\tilde{E}$ deduced from E by mod l reduction. Let us then put

$$a_l(E) = 1 + l - n_l(E).$$

The first two conditions that must be fulfilled in our algorithm is to find an integer $n \geq 1$ such that $q = np + 1$ is prime and that p does not divide $a_q(E)^2 - 4$. Suppose we get such an integer (which is very easy to get), then we have to consider the subset $A(n, q)$ of the nth roots of unity in $\mathbf{F}_q$ of the elements ζ such that the following condition is satisfied :

$$\text{the element } -\frac{1}{3} + 36\zeta \text{ is a square in } \mathbf{F}_q.$$

If ζ is an element in $A(n, q)$, let δ_ζ be the least integer ≥ 0 such that

$$\delta_\zeta^2 \text{ mod. } q = -\frac{1}{3} + 36\zeta.$$

We associate to ζ the Weierstrass affine equation over $\mathbf{F}_q$:

$$(W_\zeta) \qquad Y^2 = X^3 + \frac{1 - 27\zeta}{9}\, X + \delta_\zeta \left(\frac{2 + 27\zeta}{81}\right).$$

The discriminant of (W_ζ) is $-2^4.3^3.\zeta^2$. It is in particular non zero, and (W_ζ) is an elliptic curve defined over $\mathbf{F}_q$; let $n_q(\zeta)$ its number of rational points over $\mathbf{F}_q$. We put

$$a_q(\zeta) = q + 1 - n_q(\zeta).$$

Then the statement of the algorithm is the following :

Theorem 14. *Let p be a prime number ≥ 5. Suppose there exists an integer $n \geq 1$ such that the following conditions are satisfied :*

a) the number $q = np + 1$ is prime ;

b) we have $a_q(E)^2 \not\equiv 4$ mod. p ;

c) for all element ζ belonging to $A(n, q)$, we have $a_q(\zeta)^2 \not\equiv a_q(E)^2$ mod. p.

Then the set $S(3, 3, p)$ is empty.

We deduce from this result the assertion a) of the theorem 10 with the software calculus PARI. For instance we see that the set $S(3, 3, 479909)$ is empty by applying the above theorem with $n = 14$ (it is the least possible integer n).

V. Connection with another conjecture on elliptic curves

Let us *fix* two *prime numbers* which I shall note l and q such that $lq \geq 6$. Let us consider the set $F(l, q)$ of the prime numbers p such that $S(l, q, p)$ is not empty. Of course we would like to prove the following conjecture :

Conjecture 2. *The set $F(l, q)$ is finite.*

There does not exist any example of pair (l, q) for which $F(l, q)$ is known to be finite (or infinite). As we noticed, we just dispose of some fragments of information in the case $(l, q) = (3, 3)$.

It would be interesting to connect the conjecture above with other more structured conjectures. For this aim, it is tempting to evoke the following one which I shall call the Frey-Mazur conjecture :

Conjecture 3. *Let E be an elliptic curve defined over $\mathbf{Q}$. Let A_E be the set of the prime numbers p such that the condition below is realised :*

there exists an elliptic curve $E^{(p)}$ over $\mathbf{Q}$, non isogenous to E, such that the Galois modules of the p-division points of E and $E^{(p)}$ are isomorphic.

Then the set A_E is finite.

In fact we can prove that this conjecture is a consequence of a Szpiro's conjecture on elliptic curves over $\mathbf{Q}$. We do not know any elliptic curve E satisfying (or not) this conjecture. Using the theorem 12, we just dispose of some partials results when E has complex multiplications. For instance let us take for E the curve of equation $y^2 = x^3 - x$: if a prime $p \geq 17$ belongs to A_E then 4 divides $p + 1$ (cf. th. 12). We have the following result :

Proposition 2. *If the Frey-Mazur conjecture is true, the sets $F(3, 3)$, $F(5, 5)$ and $F(7, 7)$ are finite ; if furthermore we suppose the Taniyama-Weil conjecture is true, the set $F(2, 3)$ is also finite.*

The reason of this implication is the following : let us be given a prime $p \geq 11$ belonging to one of the sets $F(l, q)$ in the statement of the above proposition. Let (a, b, c) be an element of $S(l, q, p)$. Then there exists a Frey curve $F = F(a, b, c)$ over $\mathbf{Q}$ associated to (a, b, c) (def. 2) apart from the fact that the mod p representation ρ_p^F is unramified outside a set $T \cup \{p\}$, T being contained in $\{2, 3, 5, 7\}$ (and not necessarily in $\{2, 3\}$). The construction of F has been done recently by H. Darmon (cf. [10]).

The Frey-Mazur conjecture is of course very difficult to prove. But it is not hopeless that in a more or less future, someone succeeds to prove it. For that reason it would be very interesting to be able to construct Frey curves for many pairs (l, q). Unfortunately, in a certain sense to be precised, it seems not very promising (cf. [11]). Perhaps then one would have to replace the base field $\mathbf{Q}$ by other numbers fields, that is to construct "Frey curves" over numbers fields other than $\mathbf{Q}$. We dispose of one example in this direction in the section 4 below, although one of the exponents (l, q) is not prime.

We are now giving the equations of the Frey curves which allow one to prove the above proposition. Below the letter p refers to a prime number ≥ 11.

Frey Curves

1. The equation $x^2 + y^3 = z^p$

Let (a, b, c) be an element of $S(2, 3, p)$. Let F be the elliptic curve of equation

$$y^2 = x^3 + 3b\ x + 2a.$$

The discriminant of F is

$$\Delta = -3^3.2^6.c^p.$$

It is a Frey curve with $T = \{2, 3\}$ (cf. [7], p. 530).

1.1. How was found that Frey curve ?

It is fairly easy if we think about the elliptic curve, defined over the two indeterminates field $\mathbf{Q}(u, v)$, of equation

$$y^2 = x^3 + u\ x + v,$$

for which the discriminant is $-16(4u^3 + 27v^2)$.

2. The equation $x^5+y^5=z^p$

Let (a,b,c) be an element of $S(5,5,p)$. Let F be the elliptic curve of equation

$$y^2=x^3+5(a^2+b^2)\,x^2+5\left(\frac{a^5+b^5}{a+b}\right)\,x.$$

Its discriminant is

$$\Delta=2^4.5^3.(a+b)^2c^{2p}.$$

It is a Frey modular curve with $T=\{2,5\}$.

2.1. How was found that Frey curve ?

let us choose $\sqrt{5}$ a square root of 5 and define

$$\omega=\frac{-1+\sqrt{5}}{2}\quad\text{and}\quad\bar{\omega}=\frac{-1-\sqrt{5}}{2}.$$

We have

$$a^5+b^5=(a+b)(a^2+\omega ab+b^2)(a^2+\bar{\omega}ab+b^2).$$

We then wish to derive from this factorisation two numbers A and B in $\mathbb{Q}(\sqrt{5})$ such that the product $AB(A+B)$ is a pth power. For that we can choose the numbers

$$A=\bar{\omega}\big(a^2+\omega ab+b^2\big)\quad\text{and}\quad B=\omega\big(a^2+\bar{\omega}ab+b^2\big).$$

We then have the equality

$$A+B+(a+b)^2=0.$$

Now we consider the "usual" Frey curve $\mathcal{F}$ of equation

$$Y^2=X(X-A)(X+B).$$

We verify that the equation of $\mathcal{F}$ is

$$Y^2=X^3+\sqrt{5}(a^2+b^2)\;X^2+\left(\frac{a^5+b^5}{a+b}\right)\,X.$$

Its twist over $\mathbb{Q}(\sqrt{5})$ by $5^{1/4}$ is then the curve F.

3. The equation $x^7+y^7=z^p$

Let (a,b,c) be an element of $S(7,7,p)$. Let F be the elliptic curve of equation

$$y^2=x^3+a_2\,x^2+a_4\,x+a_6,$$

with

$$a_2=-(a-b)^2,\quad a_4=-2a^4+ba^3-5b^2a^2+b^3a-2b^4,$$
$$a_6=a^6-6ba^5+8b^2a^4-13b^3a^3+8b^4a^2-6b^5a+b^6.$$

The discriminant of F is

$$\Delta=2^4.7^2.\left(\frac{a^7+b^7}{a+b}\right)^2.$$

It is a Frey modular curve with $T=\{2,7\}$.

3.1. How was found that Frey curve ?

let ζ be a primitive 7th root of unity. Define

$$\omega_1=\zeta+\zeta^{-1}\quad\omega_2=\zeta^2+\zeta^{-2}\quad\text{and}\quad\omega_3=\zeta^3+\zeta^{-3}.$$

We have $\omega_1+\omega_2+\omega_3=-1$, $\omega_1\omega_2\omega_3=1$ and $\omega_1\omega_2+\omega_2\omega_3+\omega_3\omega_1=-2$. We verify that

$$a^7+b^7=(a+b)(a^2+\omega_1ab+b^2)(a^2+\omega_2ab+b^2)(a^2+\omega_3ab+b^2).$$

Let us define

$$A_1=(\omega_3-\omega_2)\big(a^2+\omega_1ab+b^2\big),\quad A_2=(\omega_1-\omega_3)\big(a^2+\omega_2ab+b^2\big),$$
$$A_3=(\omega_2-\omega_1)\big(a^2+\omega_3ab+b^2\big).$$

We have

$$A_1+A_2+A_3=0$$

Let $\mathbb{Q}(\mu_7)$ be the field of the 7th roots of unity. We now search for three integers u_1, u_2 and u_3 in $\mathbb{Q}(\mu_7)$, which are conjugate by the Galois group $\mathrm{Gal}(\mathbb{Q}(\mu_7)/\mathbb{Q})$, such that

$$A_1=u_3-u_2,\quad A_2=u_1-u_3\quad\text{and}\quad A_3=u_2-u_1.$$

We can choose

$$u_2=\omega_2a^2-\omega_3\omega_1ab+\omega_2b^2,\quad u_3=\omega_3a^2-\omega_2\omega_1ab+\omega_3b^2,$$
$$u_1=\omega_1a^2-\omega_3\omega_2ab+\omega_1b^2.$$

Our curve F is then the elliptic curve of equation

$$y^2=(x-u_1)(x-u_2)(x-u_3).$$

4. Some attempts for the equation $x^2+y^4=z^p$

Let (a,b,c) be an element of $S(2,4,p)$. I would like just mentioned the fact that one can associates a "Frey curve" F to (a,b,c) which is unfortunately not defined over $\mathbb{Q}$, but over $\mathbb{Q}(i)$ (cf. [8], 4). The equation of F is

$$y^2=x^3+2(1+i)b\,x^2+i(b^2+ia)\,x.$$

Its discriminant is $2^6.c^p.(a-ib^2)$. The curve F has the particularity to be a $\mathbb{Q}$-curve, that is a curve which is isogenous over $\mathbb{Q}(i)$ to its conjugate. This allows one to construct a 2-dimensional representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ in characteristic p, whose Serre's conductor is small; this leave perhaps some hope to derive this way a contradiction for the existence of (a,b,c) (cf. *loc. cit.*).

Bibliography

[1] A.O.L. Atkin et J. Lehner, Hecke operators on $\Gamma_0(N)$, *Math. Ann.* **185** (1970), 134-160.

[2] S. Beckmann, On extensions of number fields obtained by specializing branched coverings, *Crelle's Journal* 419 (1991), 27-53.

[3] F. Beukers, The diophantine equation $Ax^p + By^q = Cz^r$, preprint (1995).

[4] J. E. Cremona, Algorithm for modular elliptic curves,Cambridge University Press 1992.

[5] H. Darmon, The equation $x^4 - y^4 = z^p$, *C.R. Math. Rep. Acad. Sci. Canada* 15 (1993), 286-290.

[6] H. Darmon, The equations $x^n + y^n = z^2$ and $x^n + y^n = z^3$, *Intern. Math. Research Notices* 10 (1993), 263-274.

[7] H. Darmon and A. Granville, On the equations $z^m = F(x,y)$ and $Ax^p + By^q = Cz^r$, *Bull. London Math. Soc.* 27 (1995), 513-544.

[8] H. Darmon, Serre's Conjectures, Canadian Math. Society, Conference proceeding, Volume **17**, 1995.

[9] H. Darmon and L. Merel, Winding quotients and some variants of Fermat's Last Theorem, to appear in *Crelle's Journal* (1996).

[10] H. Darmon, Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation , preprint (1997).

[11] H. Darmon and A. Kraus, Note on the equations $x^5 + y^5 = z^p$ and $x^7 + y^7 = z^p$, in preparation.

[12] F. Diamond, On deformation rings and Hecke rings, *Ann. of Math.* 144 (1996), 137-166.

[13] E. Halberstadt and A. Kraus, Sur la comparaison galoisienne des points de torsion des courbes elliptiques, *C. R. Acad. Sci. Paris* 322 (1996), 313-316.

[14] A. Kraus, Sur l'équation $a^3 + b^3 = c^p$, to appear in *J. of Experimental Math.* (1997).

[15] B. Mazur, Rational Isogenies of prime degree, *Invent. Math.* 44 (1978) 129-162.

[16] F. Momose, Rational points on the modular curves $X_{split}(p)$, *Compositio Math.* 52 (1984), 115-137.

[17] P. Ribenboim, 13 Lectures on Fermat's Last Theorem, Springer-Verlag, 1979.

[18] K. Ribet, On modular representation of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms, *Invent. Math.* 100 (1990), 431-476.

[19] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259-331.

[20] J.-P. Serre, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, *Duke Math. J.* **54** (1987), 179-230.

[21] J.-P. Serre, Travaux de Wiles (et Taylor,...), Partie I, Sém. Bourbaki **803**, 1994-95.

[22] J. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, in Modular Functions of One Variable IV, Lecture Notes in Math. **476**, 33-52, 1975.

[23] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Ann. of Math.* **141** (1995), 443-551.

August 6, 1997

Alain KRAUS
Université de Paris VI
Institut de Mathématiques, Case 247
4 place Jussieu 75252 Paris Cedex 05
France

e-mail : kraus@math.jussieu.fr