On the Equation $x^r + y^r = z^p$

Alain Kraus

Introduction

Let r be a *fixed* prime number ≥ 3. The aim of this lecture was to survey the works which have been done on the diophantine equation

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

p being a prime number at least 5 other than r. So in the following the prime number p is allowed to vary, and typically we will be faced with the problem where p is large relative to the fixed prime r.

We will say that an integral solution (a, b, c) to the equation (1) is primitive if we have $gcd(a, b, c) = 1$, and is non trivial if abc is non zero. We will denote by $S(r, p)$ the set of the non trivial primitive solutions of the equation (1).

The main problem related to this equation is the following :

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

In light of the *abc* conjecture, it is tempting to make the following conjecture :

Conjecture 1. *The set* $S(r, p)$ *is empty if* p *is large enough.*

Let us define $F(r)$ to be the set

$$F(r) = \bigcup_{p \geq 5} S(r, p).$$

Actually H. Darmon and A. Granville have shown that $S(r, p)$ is *finite* (cf. [2], p. 515, th. 2). This implies that the previous conjecture is equivalent to the following :

Conjecture 2. *The set $F(r)$ is finite.*

In fact there is no example of pair (r,p) for which $S(r,p)$ is known to be non empty. The most optimistic conjecture would then be (why not) :

Conjecture 3. *The set $F(r)$ is empty.*

Let us see in the next section the known results in the direction of these conjectures.

I. The known results

They mainly concern the cases $r = 3$ and $r = 5$. They are all consequences of the proved results on the Taniyama-Weil conjecture (cf. [14]). The last one has been recently obtained by B. Conrad, F. Diamond and R. Taylor : they have shown that an elliptic curve defined over $\mathbb{Q}$ whose conductor is not divisible by 27 is *modular*. At first H. Darmon and A. Granville have proved in 1993 the result below (cf. [2], p. 530, prop. 4.4) :

Theorem 1. *Let p be a prime number ≥ 17. An even pth power cannot be expressed as a sum of two relatively prime cubes.*

I proved in 1997 the following results (cf. [8]) :

Theorem 2. *Let (a,b,c) be an element of $S(3,p)$. The two-adic valuation of ab is one and the three-adic valuation of c is at least one.*

Theorem 3. *a) Let p be a prime number such that $5 \leq p < 10^4$. The set $S(3,p)$ is empty.*

b) Suppose that p is a prime number ≥ 5 such that $q = 2p+1$ is prime and that q is a square modulo 107 and modulo 109. Then the set $S(3,p)$ is empty.

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

With H. Darmon we have obtained the result below when $r = 5$ (cf. [6]) :

Theorem 4. *Let p be a prime number ≥ 5. An even pth power cannot be expressed as a sum of two relatively prime fifth powers.*

II. The method used to obtain these results

Let us describe the method which was used to get these results and which perhaps could be used to obtain similar results for exponents r other than 3 and 5. At first, we consider an element (a, b, c) of $S(r, p)$. Then we construct an elliptic curve $F = F(a, b, c)$ defined over $\mathbb{Q}$, which we will call a Frey elliptic curve, 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 $\rho_p^F : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}\big(F[p]\big)$ of the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ in the p-division points of F is irreducible ; moreover ρ_p^F is unramified outside the set $\{2, r\} \cup \{p\}$;

(iii) there exists a prime number at which F has multiplicative reduction.

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. [12]). These invariants measure the ramification of ρ_p^F. In our situation we have $k = 2$ (condition (i)) and the prime numbers which may divide N are 2 or r (condition (ii)). If F is *modular*, which appears to be the case in our situation if $r = 3$ or $r = 5$, it is now proved that if p is greater than an explicit constant $C(N)$, there exists a modular elliptic E defined over $\mathbb{Q}$, whose conductor is N, such that the Galois representations in the p-division points of F and E are isomorphic. (cf. [13], 2.2, *Remarques* 2) and [7], th. 3).

Then by mean of arguments concerning the Galois properties of the division points of elliptic curves, we are led to a contradiction for the existence of the solution (a, b, c) (cf. [4], [10] and [11]).

III. Description of the algorithm in the case $r = 3$

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

We have to consider the elliptic curve E over $\mathbb{Q}$ given by the equation

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

It is the curve numbered 72A in Cremona's tables (cf. [1]). 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 $\mathbb{F}_l$ of the curve $\tilde{E}$ deduced from E by mod l reduction. Let us then put

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

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

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

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 $\mathbb{F}_q$:

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

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 $\mathbb{F}_q$; let $n_q(\zeta)$ the number of its rational points over $\mathbb{F}_q$. We put

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

Then the statement of the algorithm is the following :

Theorem 5. *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 $S(3,p)$ is empty.

For instance, with the software calculus PARI, we see that the set $S(3, 479909)$ is empty by applying the above theorem with $n = 14$ (it is the least possible integer n).

IV. The Frey-Mazur Conjecture

Actually it would be very interesting to construct Frey elliptic curves corresponding to many exponents r because of the following conjecture on elliptic curves which I will call the Frey-Mazur conjecture (cf. [9], p. 133 and [3], p. 148) :

Conjecture 4. *Let E be an elliptic curve defined over $\mathbb{Q}$. 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 $\mathbb{Q}$, 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.

It is a consequence of the *abc* conjecture. We do not know any elliptic curve E satisfying (or not) the conjecture 4. Let r be a prime number ≥ 3. Suppose that for all prime $p \geq 5$ there exists a Frey elliptic curve associated to each element (a, b, c) of $S(r, p)$ as indicated in the section II. Then if the Frey-Mazur conjecture is true, one can show that the set $F(r)$ is finite. In particular we have the following result (cf. [2], p. 530 et [6]) :

Theorem 6. *If the Frey-Mazur conjecture is true, the sets $F(3)$, $F(5)$ and $F(7)$ are finite.*

In fact the possible existence of a Frey elliptic curve corresponding to an exponent r is more or less equivalent to answer in the affirmative to the following question (cf. [6]) :

Question. *Let r be a prime number ≥ 3 and T be an indeterminate. Let $\Phi_r(T)$ be the rth cyclotomic polynomial and S be set $\Big\{T-1, \Phi_r(T)\Big\}$. Does there exist an elliptic curve defined over $\mathbb{Q}(T)$ with good reduction outside S, and with multiplicative reduction at $\Phi_r(T)$ and possibly at $T-1$?*

The answer is positive if $r = 3$, $r = 5$ and $r = 7$. In these cases we give below such an elliptic curve $E(T)$ answering positively to the above question : 1) for $r = 3$:

$$E(T): \qquad y^2 = x^3 - 3T\ x + 1 + T^3.$$

2) For $r = 5$:

$$E(T): \qquad y^2 = x^3 + 5(T^2+1)\ x^2 + 5\Phi_5(T)\ x.$$

3) For $r = 7$:

$$E(T): \quad y^2 = x^3 + a_2\ x^2 + a_4\ x + a_6,$$

with

$$a_2 = -(T+1)^2, \quad a_4 = -(2T^4 + T^3 + 5T^2 + T + 2),$$
$$a_6 = T^6 + 6T^5 + 8T^4 + 13T^3 + 8T^2 + 6T + 1.$$

When r is ≥ 11 it seems not quite promising to get such an elliptic curve $E(T)$ because of some reasons linked to the *abc* conjecture which is known to be true in the function field case. This shows in some sense the limit of the method, if we wish to stay in the setting of elliptic curves, in order to get informations towards the conjecture 2. As H. Darmon pointed out in his lecture (cf. [5]) it seems now suitable to try to introduce the notion of hyperelliptic Frey curve.

V. The hyperelliptic Frey curve

Actually for all prime number $r \geq 3$, there exists an hyperelliptic curve defined over $\mathbb{Q}$ which generalises the situation already encounted in the case $r = 3$. Let (a, b, c) be an element of $S(r, p)$. Then there exists $C = C(a, b, c)$ an hyperelliptic curve defined over $\mathbb{Q}$, of genus $(r-1)/2$, whose jacobian has real multiplications by the totally real subfield of the rth roots of unity. The receipt to get an equation of C is the following : let ζ be a primitive rth root of unity and $g(T)$ be the irreducible polynomial over $\mathbb{Q}$ of $\zeta + \zeta^{-1}$. Then an equation of C is

$$C: \quad y^2 = (ab)^{\frac{r-1}{2}}\ x\ g\left(\frac{x^2}{ab} + 2\right) + b^r - a^r.$$

The discriminant Δ of this equation is

$$\Delta = (-1)^{\frac{r-1}{2}}.2^{2(r-1)}.r^r.c^{p(r-1)}.$$

If $r = 3$ we recover the elliptic curve considered in [2] and in [8] given by the equation

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

In order to show that $S(r, p)$ is empty one can try then to adapt the arguments used in the setting of elliptics curves to the hyperelliptic situation. Of course we do not dispose of many results about Galois modular representations in dimension ≥ 2. But as H. Darmon has shown in his preprint [5], the consideration of hyperelliptic Frey curves seems really now a new direction to study generalised Fermat equations.

References

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

[2] 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.

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

[4] H. Darmon and L. Merel, Winding quotients and some variants of Fermat's Last Theorem, *J. reine angew. Math.* **490** (1997), 81-100.

[5] H. Darmon, Hyperelliptic curves, Hilbert modular forms, and Fermat's Last Theorem, Cicma reports, Concordia Laval McGill (1997).

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

[7] A. Kraus, Majorations effectives pour l'équation de Fermat généralisé, to appear in *Can. J. Math.* (1997).

[8] A. Kraus, Sur l'équation $a^3 + b^3 = c^p$, to appear in *J. of Experimental Math.* **7** no.1 (1998), 1-13.

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

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

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

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

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

[14] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Ann. of Math.* **141**

(1995), 443-551.

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