

Generalized Fermat equations (d'après Halberstadt-Kraus).

Pierre Charollois

ABSTRACT. In this paper, we summarize the work of Halberstadt and Kraus on generalized Fermat equations of the shape $ax^n + by^n = cz^n$. In particular, we sketch the proof that, for fixed odd coprime integer coefficients a, b, c , there is a set of primes n of positive density for which only trivial solutions (x, y, z) occur.

CONTENTS

| | |
|---------------------------------------|----|
| 1. Introduction. | 81 |
| 2. Preliminary section. | 82 |
| 3. Proof of Theorems 1.1 and 1.2. | 83 |
| 4. Proof of the symplectic criterion. | 85 |
| 5. Limitations of the method. | 86 |
| References | 87 |

1. Introduction.

Our purpose is to publicize the statement and the proof of the following theorem [HK02, théorème 2.1]:

THEOREM 1.1 (Halberstadt-Kraus (2002)). *Let a, b, c be odd pairwise coprime integers. Then there is a set of primes $\mathcal{P} = \mathcal{P}(a, b, c)$ of positive density such that if $p \in \mathcal{P}$, then the equation*

$$(1) \quad ax^p + by^p + cz^p = 0$$

has only trivial rational solutions $(x, y, z) \in \mathbb{Q}^3$.

A solution (x, y, z) is called trivial in our context if $xyz = 0$.

One must point out that before Wiles's work, even the case $a = b = c = 1$ was unknown. Theorem 1.1 exhibits the first infinite family of generalized Fermat equations having only trivial solutions.

Note that the set of primes \mathcal{P} will be given by congruence conditions. These can be made more precise and explicit for particular choices of triples (a, b, c) . For instance, the

2000 *Mathematics Subject Classification.* Primary 11D41, Secondary 11F11, 11G05.

proof of Theorem 1.1 yields the following, providing a partial answer to a question raised by Serre [Ser87, p.204]:

THEOREM 1.2. *If $p \geq 7$ is a prime number satisfying $p \not\equiv 1 \pmod{12}$, the equation*

$$x^p + 3y^p + 5z^p = 0$$

has only trivial solutions over \mathbb{Q} . So does the equation

$$x^p + y^p + 15z^p = 0.$$

The proof of these theorems relies crucially on the modularity theorem for elliptic curves from Wiles and his followers, as well as Ribet's level-lowering theorem. Another expository paper on the application of these modular techniques to Diophantine equations can be found in [Sik07].

It is a pleasure to thank Henri Darmon and Alain Kraus for their help and their support.

2. Preliminary section.

In this section, we give some classical necessary preparation for the theorems. Namely, following the lines of the exposition in section 4 of [Dar], we attach successively three objects to a hypothetical solution (x, y, z) of (1):

1. A Frey curve E_0 whose invariants can be computed.
2. A representation ρ describing the action of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the p -division points of E_0 .
3. Corresponding to ρ is a cusp form f of weight 2 for $\Gamma_0(N)$, where N divides the conductor of E_0 . We then reduce to the case where f has integer coefficients.

After this preparation, the point is to be able to discard all such modular forms. Halberstadt and Kraus manage to do so using their so-called "symplectic criterion" which will be explained in detail in the last section.

We proceed by contradiction and start from a hypothetical non-trivial solution

$$(x, y, z) \in \mathbb{Q}^3$$

of equation (1). Adjusting p^{th} -powers and clearing denominators, we can assume without loss of generality that x, y, z are coprime integers, and that a, b and c do not contain any p^{th} -powers.

One can reorder and label the three integers ax^p, by^p and cz^p by A, B and C respectively so that B is the only even integer among them, and $A \equiv \pm 1 \pmod{4}$. By adjusting the signs of our solution, we are reduced to the case where $A \equiv -1 \pmod{4}$. To this data $A + B + C = 0$ we attach the Frey curve over \mathbb{Q}

$$E_0 : Y^2 = X(X - A)(X + B).$$

The computation of its invariants on this model using classical formulae [Sil86, p.46] leads to:

$$\tilde{c}_4 = 16(A^2 + AB + B^2) \quad \text{and} \quad \tilde{\Delta} = 16(abc)^2(xy z)^{2p} = 16(ABC)^2.$$

If $\ell \neq 2$ is a prime dividing $\tilde{\Delta}$, it cannot divide \tilde{c}_4 . Hence E_0 is semi-stable outside 2.

To study the reduction of E_0 at $\ell = 2$, let us change the variables to $X' = 4X$ and $Y' = 8Y + 4X$. Assuming that 16 divides B (since we will assume that $p \geq 5$, even 32 divides B), one obtains a global minimal Weierstrass equation for E_0 over \mathbb{Q} . At this point the minimal discriminant turns out to be

$$(2) \quad \Delta(E_0) = 2^{-8}(ABC)^2,$$

and $c_4(E_0)$ is odd. Finally, E_0 is also semi-stable at $\ell = 2$, and thus is semi-stable. Its conductor is the radical of the discriminant, that is (because 32 divides B)

$$N_{E_0} = \prod_{\ell \text{ prime}, \ell \nmid ABC} \ell.$$

Key observation: Notice the factor 2^{-8} involved in formula (2) for the minimal discriminant. The “minus sign” of the exponent turns out to be crucial in the proof of Theorem 1.1.

The set of p -torsion points $E_0[p]$ of $E_0(\bar{\mathbb{Q}})$ forms a \mathbb{F}_p -vector space of dimension 2. The absolute Galois group $G_{\mathbb{Q}} = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts naturally on $E_0[p]$. Thus we obtain a representation

$$\rho : G_{\mathbb{Q}} \rightarrow \text{Aut}(E_0[p]) \simeq GL_2(\mathbb{F}_p).$$

If ρ is reducible, then E_0 contains a rational subgroup of order p . This cannot be the case if $p \geq 17$ because of the boundedness result of Mazur [Maz77, Th. 8] for the torsion of elliptic curves over \mathbb{Q} . Hence ρ is irreducible if p is large enough. Notice how our original Diophantine question has been transferred to this new Diophantine problem solved by Mazur. For more on this result, see [Reb] in this volume. This bound $p \geq 17$ is sufficient for us to prove Theorem 1.1. Nevertheless, a more precise result is given in [Kra97, Lemma 4] showing that ρ is irreducible as soon as $p \geq 5$.

Serre [Ser87] associates to such a representation a conductor $N|N_{E_0}$. In our context we have

$$N = 2 \text{rad}(abc) := 2 \prod_{\ell \text{ prime}, \ell \mid abc} \ell.$$

By the result of Wiles [Wil95], the semi-stable elliptic curve E_0 is modular: the function on the upper half-plane $\tau \mapsto \sum_{n \geq 1} a_n(E_0)q^n$ belongs to the space $S_2(\Gamma_0(N_{E_0}))$ of cuspidal modular forms of weight 2 on $\Gamma_0(N_{E_0})$.

The “lowering the level” Theorem of Ribet [Rib90] ensures that the representation ρ is then modular: there exists a newform $f = q + \sum_{n \geq 2} a_n q^n$ of weight 2 on $\Gamma_0(N)$ (where N now depends only on abc and not on (x, y, z) or p) and a place \mathfrak{p} of $K_f = \mathbb{Q}(a_2, \dots, a_n, \dots)$ above p such that

$$(3) \quad \begin{array}{ll} i) & a_\ell \equiv a_\ell(E_0) \pmod{\mathfrak{p}} \text{ if } \ell \nmid N_{E_0} p \\ ii) & a_\ell \equiv \pm(\ell + 1) \pmod{\mathfrak{p}} \text{ if } \ell \mid N_{E_0} \text{ and } \ell \nmid pN. \end{array}$$

In the case of Fermat’s last Theorem, one could show that $N = 2$ and the previous results were enough (!) to derive a contradiction since there is no cusp form of weight 2 and this level. In proving Theorem 1.1 and 1.2, Halberstadt and Kraus needed to refute the existence of such a form using an additional argument.

3. Proof of Theorems 1.1 and 1.2.

Let f be the modular form of level N given by the previous construction. Both f and N do not depend on the solution (x, y, z) nor on p . We first reduce to the case where the modular form f has coefficients in \mathbb{Z} . Otherwise, the finite extension $K = K_f$ of \mathbb{Q} has degree bounded by $g = \dim_{\mathbb{Q}}(S_2^{\text{new}}(\Gamma_0(N)))$. Let $a_\ell \notin \mathbb{Z}$ for the smallest possible prime ℓ . Both g and ℓ do not depend on p . We can assume that ℓ does not divide pN because a_ℓ would be 0, ± 1 . Thus in the previous case $i)$ p divides $N_{K/\mathbb{Q}}(a_\ell - a_\ell(E_0))$, while in case $ii)$ p divides $N_{K/\mathbb{Q}}(a_\ell \pm (\ell + 1))$. The Hasse bound gives $|a_\ell(E_0)| \leq 2\sqrt{\ell}$, while Weil-Deligne’s bound shows that $|\sigma(a_\ell)| \leq 2\sqrt{\ell}$ for each real embedding σ of K .