

Non-abelian descent and the generalized Fermat equation

Hugo Chapdelaine

ABSTRACT. We prove a finiteness result about the set of primitive solutions of the generalized Fermat equation $x^p + y^q = z^r$ when $1/p + 1/q + 1/r < 1$.

CONTENTS

| | |
|--|----|
| 1. The main result | 55 |
| 2. Construction of the branched covering | 58 |
| 3. A Chevalley-Weil theorem for branched coverings | 65 |
| References | 68 |

1. The main result

This Chapter gives some finiteness results for the set of primitive solutions of the generalized Fermat equation

$$(1) \quad x^p + y^q = z^r$$

where the exponents p, q, r satisfy the inequality $1/p + 1/q + 1/r < 1$. The very special ‘shape’ of the surface defined by (1) allows us to use some geometry to reduce its study to the study of non-abelian unramified covers of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ of *signature* (p, q, r) in the sense of Definition 1.1. Therefore the study of the arithmetic of equation (1) can be transferred to the setting of algebraic curves. The main ingredients in the proof are a variant of the Chevalley-Weil theorem, and the finiteness theorems of Hermite-Minkowski and Faltings. This finiteness result for (1) which was proved in [DG95] can be viewed as an illustrative special case of the Campana program which was presented in Dan Abramovich’s lecture series at this summer school.

The author would like to thank Henri Darmon for a careful proofreading of this article which led to many improvements.

A solution $(a, b, c) \in \mathbb{Z}^3$ of (1) is called *nontrivial* if $abc \neq 0$ and *primitive* if $\gcd(a, b, c) = 1$. When the exponents p, q and r are pairwise coprime, the following

2000 *Mathematics Subject Classification*. Primary 11D41, Secondary 11G30, 14H30.

exercise shows that (1) has infinitely many nontrivial but not necessarily primitive solutions.

Exercise 1 Let p, q and r be pairwise coprime. Show that the affine surface defined by $x^p + y^q = z^r$ in $\mathbb{A}_{\mathbb{Q}}^3$ is rational, i.e., the quotient field of $\mathbb{Q}[x, y, z]/(x^p + y^q - z^r)$ is purely transcendental of degree 2 over \mathbb{Q} .

From now on we are only interested in studying the set of nontrivial primitive solutions of (1). The study of (1) can be split into three cases:

- (1) The *spherical case*: $1/p + 1/q + 1/r > 1$. The possibilities are $\{p, q, r\} = \{2, 2, k\}$ with $k \geq 2$, $\{2, 3, 3\}$, $\{2, 3, 4\}$ and $\{2, 3, 5\}$.
- (2) The *Euclidean case*: $1/p + 1/q + 1/r = 1$. The possibilities are $\{p, q, r\} = \{3, 3, 3\}$, $\{2, 4, 4\}$ and $\{2, 3, 6\}$.
- (3) The *hyperbolic case*: $1/p + 1/q + 1/r < 1$.

This division is reminiscent of the classification of algebraic curves which also falls into 3 cases depending on the genus or the sign of the Euler characteristic. Here is the main theorem that we wish to prove.

THEOREM 1.1. (*Darmon, Granville*) *If $1/p + 1/q + 1/r < 1$ then (1) has only finitely many nontrivial primitive solutions.*

Note that the statement of this theorem concerns the existence of integral points on a surface. We would like to reduce the study of integral solutions of (1) to the study of K -rational points on an auxiliary projective curve X/K where K is a suitable number field. We consider the map

$$\begin{aligned} \{\text{Set of nontrivial primitive solutions of equation (1)}\} &\rightarrow \mathbb{P}^1(\mathbb{Q}) \subseteq \mathbb{P}^1(\mathbb{C}) \\ (a, b, c) &\mapsto \frac{a^p}{c^r}, \end{aligned}$$

which allows us to reduce the study of (1) to the study of certain branched coverings of $\mathbb{P}^1(\mathbb{C})$. We define the set

$$\Sigma_{p,q,r} := \left\{ \frac{a^p}{c^r} \in \mathbb{Q} : a^p + b^q = c^r, abc \neq 0, \gcd(a, b, c) = 1 \right\} \subseteq \mathbb{P}^1(\mathbb{Q}).$$

Exercise 2 Show that $\#\Sigma_{p,q,r} < \infty$ if and only if (1) has finitely many primitive solutions.

Now let us explain the main ideas of Theorem 1.1.

Proof of Theorem 1.1 We want to show that the set of nontrivial primitive solutions of (1) is finite. By Exercise 2, it is enough to show that $\Sigma_{p,q,r}$ is finite when $1/p + 1/q + 1/r < 1$. The proof can be broken into four steps.

First step: The existence of a Galois branched covering.

DEFINITION 1.1. A Galois covering $\pi : X \rightarrow \mathbb{P}^1$ is said to be of *signature* (p, q, r) if its ramification indices above $0, 1$ and ∞ are equal to p, q and r respectively, and if π is unramified everywhere else.

The first stage of the proof consists in constructing a Galois covering of \mathbb{P}^1 of signature (p, q, r) defined over a suitable number field K and Galois over that field (The construction of such a cover will be done in detail in Section 2). The Riemann-Hurwitz formula then determines the genus $g(X)$ of X in terms of the

degree d of π :

$$\begin{aligned} 2g(X) - 2 &= d(2g(\mathbb{P}^1(\mathbb{C})) - 2) + \frac{d}{p}(p-1) + \frac{d}{q}(q-1) + \frac{d}{r}(r-1) \\ &= d(1 - 1/p - 1/q - 1/r). \end{aligned}$$

Since $1 - 1/p - 1/q - 1/r > 0$ we conclude that $g(X) > 1$.

Second step: A Chevalley-Weil theorem for branched coverings.

Given $t \in \mathbb{P}^1(K)$, let L_t be the smallest field of definition of the closed points in $\pi^{-1}(t)$. As is explained in Section 3, the field L_t is a Galois extension of K with Galois group isomorphic (non-canonically) to a subgroup of $\text{Gal}(X/\mathbb{P}^1)$. The Chevalley-Weil theorem for branched coverings (see Theorem 3.2) shows that the ramification of L_t , for $t \in \Sigma_{p,q,r}$, is bounded *independently* of t , in light of the following elementary property of $\Sigma_{p,q,r}$:

LEMMA 1.1. Let $t = \frac{a^p}{c^r} \in \Sigma_{p,q,r}$; then for all prime numbers ℓ we have

- (1) $v_\ell(\text{Numerator}(t)) \equiv 0 \pmod{p}$,
- (2) $v_\ell(\text{Numerator}(t-1)) \equiv 0 \pmod{q}$,
- (3) $v_\ell(\text{Numerator}(\frac{1}{t})) \equiv 0 \pmod{r}$,

where for $x \in \mathbb{Q}$, $v_\ell(x)$ stands for the valuation of x at the prime ℓ .

Note that the proof of Lemma 1.1 uses in a crucial way the primitivity of the solution (a, b, c) corresponding to $t = \frac{a^p}{c^r}$ and the fact that $t-1 = -\frac{b^q}{c^r}$.

Third step: Hermite-Minkowski.

By the Hermite-Minkowski theorem (cf. Theorem 1.1 in Section 1.1 of [Dar]) the compositum L of all the number fields L_t , for $t \in \Sigma_{p,q,r}$, is a finite extension of K .

Fourth step: Faltings' Theorem.

By definition of L we have $\pi^{-1}(\Sigma_{p,q,r}) \subseteq X(L)$. Since $g(X) > 1$, we deduce by Faltings' theorem that $X(L)$ is a finite set and therefore $\pi^{-1}(\Sigma_{p,q,r})$ and $\Sigma_{p,q,r}$ are also finite sets. This concludes the sketch of the proof of Theorem 1.1. \square

REMARK 1.1. The conclusion of Theorem 1.1 remains the same if we replace the equation $x^p + y^q = z^r$ by the more general equation $Ax^p + By^q = Cz^r$ for nonzero fixed integers A, B and C . For a further discussion of the equation $Ax^p + By^q = Cz^r$, see [DG95].

REMARK 1.2. In some special cases, for example when $(p, q, r) = (n, n, n)$ with $n \geq 3$ we know by the work of Wiles and Taylor (see [Wil95] and [TW95]) that (1) has no nontrivial solutions. Using similar techniques, Darmon and Merel (see [Dar00] and [DM97]) could also treat the case (p, p, r) where $r = 2$ or 3 and p is a prime number larger than or equal to $6 - r$ to conclude that (1) has no nontrivial primitive solutions.

For the rest of the paper, we would like first to explain in detail the construction of the auxiliary branched covering $(X_K, \pi, \mathbb{P}_K^1)$ of signature (p, q, r) above $\{0, 1, \infty\}$ which was needed in the first step of the proof of Theorem 1.1. Secondly, we would like to give a more detailed discussion about the variant of the Chevalley-Weil theorem that we have used to control the ramification of the number field L_t over K for the special elements $t \in \Sigma_{p,q,r}$. We won't say anything about Steps 3 and 4, which are discussed in [Dar]. Sections 2 and 3 are devoted to a discussion of Steps 1 and 2 respectively.