Panoramas & Synthèses
36, 2012, p. 119–149

THE GENERALIZED FERMAT EQUATION

by

Frits Beukers

***Abstract.* —** This article will be devoted to generalisations of Fermat's equation $x^n + y^n = z^n$. Very soon after the Wiles and Taylor proof of Fermat's Last Theorem, it was wondered what would happen if the exponents in the three term equation would be chosen differently. Or if coefficients other than 1 would be chosen. We discuss the reduction of the resolution of such equations to the determination of rational points on finite sets of algebraic curves (over $\mathbb{Q}$ if possible) and explain the full resolution of the particular equation with exponents $2, 3, 5$.

***Résumé* (L'équation de Fermat généralisée). —** Cet article étudie les généralisations de l'équation de Fermat $x^n + y^n = z^n$. Dès la démonstration du « grand théorème de Fermat » par Wiles et Taylor, on s'est démandé ce qu'il adviendrait si les exposants dans l'équation à trois termes étaient choisis différemment. Ou si l'on plaçait d'autres coefficients que 1 devant les monômes. Nous discutons la réduction de la résolution de telles équations à la détermination des points rationnels d'un ensemble fini de courbes algébriques (définies sur $\mathbb{Q}$ si possible), puis résolvons complètement l'équation d'exposants $2, 3, 5$.

1. Introduction

Let $A, B, C \in \mathbb{Z}$ be non-zero and $p, q, r \in \mathbb{Z}_{\geq 2}$. Consider the diophantine equation

$$Ax^p + By^q = Cz^r, \qquad \gcd(x, y, z) = 1$$

in the unknown integers x, y, z. The gcd-condition is really there to avoid trivialities. For example, from $a + b = c$ it would follow, after multiplication by $a^{21}b^{14}c^6$, that

$$(a^{11}b^7c^3)^2 + (a^7b^5c^2)^3 = (a^3b^2c)^7$$

thus providing us with infinitely many trivial solutions of $x^2 + y^3 = z^7$. There are three cases to be distinguished.

2000 *Mathematics Subject Classification.* — Primary 11D41; Secondary 11G30.
***Key words and phrases.* —** Fermat's last theorem, generalized Fermat equation, Galois cover, invariant theory.

© Panoramas et Synthèses 36, SMF 2012

1. The hyperbolic case
$$\frac{1}{p}+\frac{1}{q}+\frac{1}{r}<1.$$
In this case the number of solutions is at most finite, as shown in [**DG**, Theorem 2].
2. The euclidean case
$$\frac{1}{p}+\frac{1}{q}+\frac{1}{r}=1.$$
A simple calculation shows that the set $\{p,q,r\}$ equals one of $\{3,3,3\}$, $\{2,4,4\}$, $\{2,3,6\}$. In this case the solution of the equation comes down to the determination of rational points on twists of genus 1 curves over $\mathbb{Q}$ with $j=0,1728$.
3. The spherical case
$$\frac{1}{p}+\frac{1}{q}+\frac{1}{r}>1.$$
A simple calculation shows that the set $\{p,q,r\}$ equals one of the following: $\{2,2,k\}$ with $k\geq 2$ or $\{2,3,m\}$ with $m=3,4,5$. In this case there are either no solution or infinitely many. In the latter case the solutions are given by a finite set of polynomial parametrisations of the equation, see [**Beu**].

A special case of interest is when $A=B=C=1$. In many such cases the solution set has been found. Below we list the exponent triples (p,q,r) of solved equations together with the non-trivial solutions ($xyz\neq 0$). We exclude the generic solution $1^k+2^3=3^2$ from our listing. If no solution are mentioned it is proven that no other solutions exist. The notation $\{p,q,r\}$ implies that all permutations of the ordered triple (p,q,r) are taken into account. This is important in the case of two even exponents.

We start with the *hyperbolic cases*. The first case $\{n,n,n\}$ is of course Wiles's proof of Fermat's Last Theorem. As is well-known this proof is based on the proof of the Shimura-Taniyama-Weil conjecture for stable elliptic curves. Later Breuil, Conrad, Diamond and Taylor proved the full conjecture for any elliptic curve in [**BCDT**]. In the following list the cases with variable n are all solved using Wiles's modular form approach, with possibly a few exceptions which are resolved using Chabauty's method. The isolated cases in this table are all solved using a Chabauty approach.

- $\{n,n,n\}$ and $n\geq 4$. Wiles and Taylor [**W, TW**] (formerly Fermat's Last Theorem).
- $\{n,n,2\}$ Darmon and Merel [**DM**] (for n prime ≥ 7), and Poonen for $n=5,6,9$.
- $\{n,n,3\}$ Darmon and Merel [**DM**] (for n prime ≥ 7), Lucas (19th century) for $n=4$ and Poonen for $n=5$.
- $\{3,3,n\}$ Kraus [**Kr1**] (for $17\leq n\leq 10000$) and Bruin [**Br2, Br3**] for $n=4,5$. Later, $17\leq n\leq 10^9$ in Chen, Siksek [**ChS**] and $n=7,11,13$ by Dahmen [**Da1**].
- $(2,n,4)$ Application of [**BS**], includes $(4,n,4)$ by Darmon [**D**].
- $(2,4,n)$ Ellenberg [**El**] (for prime $n\geq 211$) and Ghioca for $n=7$ (email, see [**PSS**]).
- $(2n,2n,5)$ Bennett [**Ben**] (for $n\geq 7$ and $n=2$) Bruin [**Br3**] for $n=3$ and $n=5$ follows from Fermat's last theorem.

- $(2, 2n, 3)$ Chen [**Ch1**] (for n prime and $7 < n < 1000$ and $n \neq 31$) The case $n = 31$ and $n \equiv -1 (\mathrm{mod}\ 6)$ is dealt with in Dahmen, see [**Da2**].
- $(2, 2n, 5)$ Chen [**Ch2**] (for $n > 17$ prime and $n \equiv 1 (\mathrm{mod}\ 4)$)
- $\{2, 4, 6\}$ Bruin [**Br1**].
- $\{2, 4, 5\}$ $2^5 + 7^2 = 3^4$, $3^5 + 11^4 = 122^2$, Bruin [**Br2**].
- $\{2, 3, 9\}$ $13^2 + 7^3 = 2^9$, Bruin [**Br4**]
- $\{2, 3, 8\}$ $1^8 + 2^3 = 3^2$, $43^8 + 96222^3 = 30042907^2$, $33^8 + 1549034^2 = 15613^3$, Bruin [**Br1, Br2**].
- $\{2, 3, 7\}$ $1^7 + 2^3 = 3^2$, $2^7 + 17^3 = 71^2$, $17^7 + 76271^3 = 21063928^2$, $9262^3 + 15312283^2 = 113^7$, Poonen, Schaefer, Stoll [**PSS**].

Presumably the solutions listed above are the only solutions in the hyperbolic case. Note that in all cases one of the exponents equals 2. This led Tijdeman and Zagier (in 1994) to the following conjecture.

Conjecture 1.1. — *The diophantine equation*

$$x^p + y^q = z^r$$

in $x, y, z \in \mathbb{Z}$ *with* $\gcd(x, y, z) = 1$, $xyz \neq 0$ *and* $p, q, r \in \mathbb{Z}_{\geq 3}$ *has no solution.*

Nowadays this conjecture is also known as Beal's conjecture or the Fermat-Catalan conjecture.

In the *euclidean case* it is well-known that the only non-trivial solutions arise from the equality $1^6 + 2^3 = 2^2$, as the elliptic curves $x^3 + y^3 = 1, y^2 = x^4 + 1, y^2 = x^3 \pm 1$ contain only finitely many obvious rational points.

In the *spherical cases* the solution set is infinite. In the case $\{2, 2, k\}$ this is an exercise in number theory. The case $\{2, 3, 3\}$ was solved by Mordell, $\{2, 3, 4\}$ by Zagier and $\{2, 3, 5\}$ by J. Edwards [**Ed**] in 2004. The families of solutions are listed in Appendix A (please read the explanation in the beginning of Appendix A). In [**Co**, Chapter 14] we find a very extensive treatment of spherical and euclidean cases. The explanation of the solution of the case $\{2, 3, 5\}$ is the topic of the present notes starting from Section 7.

2. A sample solution

To illustrate the phenomena we encounter when solving the generalized Fermat equation, we give a partial solution of $x^2 + y^8 = z^3$. This equation lends itself very well to a stepwise descent method.

First we solve $x^2 + u^2 = z^3$. By factorisation on both sides over $\mathbb{Z}[i]$ we quickly see that $x + iu$ should be the cube of a gaussian integer, $(a + bi)^3$. By comparison of real and imaginary parts we get $x = a^3 - 3ab^2,\ u = b(3a^2 - b^2)$. Note that a, b should be relatively prime in order to ensure $\gcd(x, u, z) = 1$.

Next we partly solve $x^2 + v^4 = z^3$. This can be done by requiring that u, as found in the previous equation should be a square, *e.g.*, $v^2 = b(3a^2 - b^2)$. The two factors on the right should be squares up to some factors $\pm 1, \pm 3$, since their product is a square and a, b are relatively prime. We should explore all possibilities, but in this partial solution we only continue with the possibility $b = -v_1^2,\ 3a^2 - b^2 = -v_2^2$. The latter equation

can be rewritten as $3a^2 = b^2 - v_2^2$. The right hand side factors as $(b - v_2)(b + v_2)$ and hence each factor is a square up to a finite number of factors. Here several possibilities present themselves again and we choose one, namely $b - v_2 = -6a_1^2,\ b + v_2 = -2a_2^2$ (and of course $a = 2a_1a_2$). Summation of the two equalities and use of $b = -v_1^2$ gives us $v_1^2 - a_2^2 = 3a_1^2$. Now the left hand side factors and we choose the possibility $v_1 - a_2 = 6t^2,\ v_1 + a_2 = 2s^2$ (and of course $a_1 = 2st$). Solving for v_1 and a_2 gives $v_1 = s^2 + 3t^2$ and $a_2 = s^2 - 3t^2$. Hence $a = 4st(s^2 - 3t^2)$ and $b = -(s^2 + 3t^2)^2$. Further straightforward computation gives us

$$\begin{aligned} v &= (s^2 + 3t^2)(s^4 - 18s^2t^2 + 9t^4) \\ x &= 4st(s^2 - 3t^2)(3s^4 + 2s^2t^2 + 3t^4)(s^4 + 6s^2t^2 + 81t^4) \\ z &= (s^4 - 2s^2t^2 + 9t^4)(s^4 + 30s^2t^2 + 9t^4) \end{aligned}$$

As might be clear now, this gives us an infinite set of integer solutions to the equation $x^2 + v^4 = z^3$. Had we followed all possibilities we would have found more parametrised solutions to recover the full solution set in integers. For a full list see Appendix A, or Henri Cohen's recent book [**Co**, Chapter 14.4], where one finds a complete derivation of the above type.

Finally we consider $x^2 + y^8 = z^3$. Continuing with our choices we must solve

$$y^2 = (s^2 + 3t^2)(s^4 - 18s^2t^2 + 9t^4).$$

After division by t^6 and putting $\xi = s/t,\ \eta = y/t^3$ we get

$$\eta^2 = (\xi^2 + 3)(\xi^4 - 18\xi^2 + 9),$$

i.e., we must determine the rational points on a genus two curve. To solve the equation completely we must determine the rational points on several genus two curves, namely those arising from the different parametrising solutions above. To cut things short now, we can easily calculate that

$$\frac{z^3}{y^8} = \frac{(\xi^4 - 2\xi^2 + 9)^3(\xi^4 + 30\xi^2 + 9)^3}{\eta^8}.$$

Thus, any point z^3/y^8 coming from a solution of $x^2 + y^8 = z^3$ is the image of a rational point (ξ, η) on our genus two curve under the map just given. This map is an example of a Galois cover map.

Had we followed all possibilities of the above argument, we would have obtained a number of covering maps from a genus 2 curve to $\mathbb{P}^1$ which would have covered the full set of values z^3/y^8 corresponding to all solutions of $x^2 + y^8 = z^3$ in co-prime integers x, y, z.

In this example the curves arose naturally as a result of a descent procedure. In many cases, like $x^3 + y^5 = z^7$, this descent is not so obvious any more and we have to start by constructing covers of $\mathbb{P}^1$ by curves which have a suitable ramification behaviour.

3. Galois covers of $\mathbb{P}^1$

In all approaches to the solution of the (generalised) Fermat equations one uses Galois covers in one form or another.

First we recall a few facts from the theory of algebraic curves and their function fields. For a more complete introduction we recommend Chapter II of Silverman's book [**Si**]. Let K be a field of characteristic zero and X a complete, smooth and geometrically irreducible curve X defined over K. In the function field $K(X)$ we consider a non-constant element which we denote by ϕ. Note that $K(X)$ is now a finite extension of the field $K(\phi)$. The degree of this extension is also called the degree of the map ϕ. Let $P \in X(\overline{K})$ (by $X(L)$ we denote the L-rational points of X, where L is a field extension of K). Assuming for the moment $\phi(P) \neq \infty$ we call the vanishing order of $\phi - \phi(P)$ at P the *ramification index* of ϕ at P. Notation: e_P. In case $\phi(P) = \infty$ we take for e_P the vanishing order of $1/\phi$ at P. If $e_P > 1$ we call P a *ramification point* of ϕ. The image $\phi(P)$ under ϕ of a ramification point P is called *branch point*. The set of branch points is called the *branch set* or *branch locus*. We now recall the Riemann-Hurwitz formula

Theorem 3.1. — *With the notation above let N be the degree of the map ϕ and $g(X)$ the geometric genus of X. Then,*

$$2g(X) - 2 = -2N + \sum_{P \in X(\overline{K})} (e_P - 1).$$

As we have $e_P = 1$ for all points of X except finitely many, the sum on the right is in fact a finite sum.

We call the map given by ϕ a *geometric Galois cover* if the extension $\overline{K}(X)/\overline{K}(\phi)$ is a Galois extension of fields. The Galois group G is a subgroup of the automorphism group (over $\overline{K}$) of X and is called the *covering group*. Note that the extension $K(X)/K(\phi)$ need not be Galois. If it is we call the cover simply a *Galois cover*. For a geometric Galois cover the ramification indices of all points above a given branch point are the same. In particular we shall be interested in geometric Galois covers whose branch locus is $0, 1, \infty$. These are examples of so-called Belyi maps. An immediate consequence of the Riemann-Hurwitz theorem is the following.

Corollary 3.2. — . *Let $X \to \mathbb{P}^1$ be a geometric Galois cover whose branch locus is contained in the set $\{0, 1, \infty\}$. Suppose that above these points the ramification indices are p, q, r. Suppose the degree of the cover is N. Then*

$$2g(X) - 2 = N\Big(1 - \frac{1}{p} - \frac{1}{q} - \frac{1}{r}\Big).$$

In particular we see that if $1/p + 1/q + 1/r > 1$, then $g(X) = 0$ and when $1/p + 1/q + 1/r < 1$ we have $g(X) \geq 2$.

Here we list a series of geometric Galois covers that will occur in the sequel. We start with $X = \mathbb{P}^1$. The finite subgroups of $\mathrm{Aut}_{\overline{\mathbb{Q}}}(\mathbb{P}^1)$ have been classified by Felix Klein. Up to conjugation they are given by

1. The cyclic group of order N