MATHEMATICS OF COMPUTATION
Volume 79, Number 269, January 2010, Pages 535–544
S 0025-5718(09)02294-7
Article electronically published on July 22, 2009

SOLVING FERMAT-TYPE EQUATIONS $x^5 + y^5 = dz^p$

NICOLAS BILLEREY AND LUIS V. DIEULEFAIT

Abstract. In this paper, we are interested in solving the Fermat-type equations $x^5 + y^5 = dz^p$, where d is a positive integer and p a prime number ≥ 7. We describe a new method based on modularity theorems which allows us to improve all earlier results for this equation. We finally discuss the present limits of the method by looking at the case $d = 3$.

1. Introduction

Let p be a prime number ≥ 7 and d be a positive integer. We say that a solution (a, b, c) of the equation $x^5 + y^5 = dz^p$ is *primitive* if $(a, b) = 1$ and *non-trivial* if $c \neq 0$ (note that this is not the same definition as in [1]). Let us recall briefly the generalization of the so-called modular method of Frey for solving this equation.

Assume that (a, b, c) is a non-trivial primitive solution of $x^5 + y^5 = dz^p$. Then the equation

$$(\star) \qquad y^2 = x^3 - 5(a^2 + b^2)x^2 + 5\left(\frac{a^5 + b^5}{a + b}\right)x$$

defines an elliptic curve $E(a, b)$ over $\mathbf{Q}$ of conductor N (say) which is semistable at each prime different from 2 and 5. By results of Wiles, Taylor-Wiles, Diamond and Skinner-Wiles, $E(a, b)$ is modular. Furthermore, $E(a, b)$ is a Frey-Hellegouarch curve in the following sense: the Galois representation ρ_p on p-torsion points of $E(a, b)$ is irreducible and unramified outside 2, 5, p and the set of primes dividing d. The conductor $N(\rho_p)$ (prime to p) and the weight k of ρ_p are computed in [1, §3]. Thus, it follows from a theorem of Ribet that there exists a modular form f of weight k, level $N(\rho_p)$ and trivial character such that the associated p-adic representation $\sigma_{f,p}$ satisfies $\sigma_{f,p} \equiv \rho_p \pmod{p}$. More precisely, let us denote by a_q and a'_q the coefficients of the L-functions of E and f, respectively, by K_f the number field generated by all the a'_q's and by $N_{K_f/\mathbf{Q}}$ the corresponding norm map. We then have the following proposition.

Proposition 1.1. *There exists a primitive newform f of weight k and level $N(\rho_p)$ such that, for each prime q, the following conditions hold.*

(1) *If q divides N but q does not divide $pN(\rho_p)$, then*

$$p \text{ divides } N_{K_f/\mathbf{Q}}\left(a'_q \pm (q + 1)\right).$$

(2) *If q does not divide pN, then p divides $N_{K_f/\mathbf{Q}}\left(a'_q - a_q\right)$.*

Received by the editor July 10, 2008 and, in revised form, January 28, 2009.
2000 *Mathematics Subject Classification.* Primary 11F11, 11D41, 14H52; Secondary 11D59.
Key words and phrases. Modular forms, Fermat's equation, elliptic curves, Thue-Mahler equations.

The aim of the modular method is to contradict the existence of such a form f. We describe, in the following section, a method which allows us sometimes to reach this goal.

2. Description of the method

Fix a prime number $p \geq 7$ and a positive integer d. Consider in turn each newform f of weight k and level $N(\rho_p)$. Suppose there exists a prime number q (depending on p, d and f) such that the following conditions hold:

(1) The prime q does not divide $pN(\rho_p)$.
(2) The prime p does not divide $N_{K_f/\mathbf{Q}}\left(a'_q \pm (q+1)\right)$.
(3) Let $(a,b) \in \mathbf{F}_q^2$. Consider the cubic over $\mathbf{F}_q$ given by the equation $(\star)$. If it is non-singular, compute the number of its $\mathbf{F}_q$-points. When (a,b) describes $\mathbf{F}_q \times \mathbf{F}_q$, this gives rise to a finite list of coefficients. The prime p does not divide $N_{K_f/\mathbf{Q}}\left(a'_q - a_q\right)$, for any a_q in this list.

Then the equation $x^5 + y^5 = dz^p$ does not have a non-trivial primitive solution.

3. Applications to the Fermat equation

We apply, in this section, the method described above to some values of d.

3.1. Case where $d = 2^\alpha \cdot 3^\beta \cdot 5^\gamma$.

In this paragraph, we are interested in the case where

$$d = 2^\alpha \cdot 3^\beta \cdot 5^\gamma, \quad \text{with } \alpha \geq 2 \text{ and } \beta, \gamma \text{ arbitrary.}$$

The following theorem generalizes Theorems 1.2 and 1.3 of [1].

Theorem 3.1. *Assume d is as above. Then the equation $x^5 + y^5 = dz^p$ does not have any non-trivial primitive solutions for $p \geq 13$.*

Remark 3.2. Note that although our method fails to solve these Fermat equations for small values of p, it is expected that they do not have a non-trivial solution for any $p \geq 7$.

Proof of Theorem 3.1. Assume that (a,b,c) is a non-trivial primitive solution. It follows from [1, §3] that the representation ρ_p is irreducible of weight $k = 2$.

If $\beta = 0$, then we have $N(\rho_p) = 25$ or 50. Since there is no newform of weight 2 and level 25, we necessarily have $N(\rho_p) = 50$. There are exactly two such forms and both of them have rational coefficients. The curve $E(a,b)$ is semistable at $q = 3$. Assume that $E(a,b)$ has multiplicative reduction at 3. By Prop. 1.1, we have $a'_3 \pm 4 \equiv 0 \pmod{p}$. Besides, by [4], we have $a'_3 = \pm 1$, which is a contradiction, since $p \geq 13$. So, $E(a,b)$ has good reduction at $q = 3$ and by the proposition above, $\pm 1 = a'_3 \equiv a_3 \pmod{p}$. This is also a contradiction because a_3 is even ($E(a,b)$ has a non-trivial 2-torsion subgroup) and $|a_3| \leq 2\sqrt{3}$, i.e. $a_3 = 0$ or ± 2.

If $\beta > 0$, then we have $N(\rho_p) = 75$ or 150. Assume that we have $N(\rho_p) = 75$. By [4], there are exactly 3 primitive newforms of weight 2 and level 75. They all have coefficients in $\mathbf{Q}$ and the form f of Prop. 1.1 is one of them. Moreover, by [4], we have $a'_7 = 0$ or ± 3. Since $p \geq 13$, the first condition of Prop. 1.1 does not hold for $q = 7$ and $E(a,b)$ has good reduction at 7. Following the method described in the previous section, we find that a_7 belongs to the set $\{-4, -2, 2\}$. We then deduce that the second condition of Prop. 1.1 does not hold either. In other words, we have $N(\rho_p) = 150$.

There are exactly 3 primitive newforms of weight 2 and level 150, denoted by 150A1, 150B1 and 150C1 and f is one of them. If $f = 150B1$, then $a'_7 = 4$ and a contradiction follows as above. So, $f = 150A1$ or 150C1 and by [4], we have $a'_{11} = 2$. Since $p \geq 13$, the first condition of Prop. 1.1 does not hold for $q = 11$ and $E(a, b)$ has good reduction at 11. Besides, we have $a_{11} = 0$ or ± 4. So, the second condition of Prop. 1.1 does not hold either and we obtain a contradiction. This ends the proof of the theorem. □

3.2. **Case where $d = 7$.** In this paragraph, we prove the following theorem.

Theorem 3.3. *The equation $x^5 + y^5 = 7z^p$ does not have any non-trivial primitive solutions for $p \geq 13$.*

Proof. Assume that (a, b, c) is a non-trivial primitive solution. It follows from [1, §3], that the representation ρ_p is irreducible, of weight $k = 2$ (since $p \neq 7$) and level $N(\rho_p) = 350$, 1400 or 2800.

Let us first assume that the form f of Prop. 1.1 has eigenvalues which are not rational integers. There are exactly 19 such forms of level 350, 1400 or 2800 and for all of them we have $a'_3 = \alpha$, where α is the generator of the field K_f given in [4]. If $E(a, b)$ has good reduction at $q = 3$, we have $a_3 = \pm 2$. Furthermore, $N_{K_f/\mathbf{Q}}(a'_3 \pm 2)$ belong to the set $\{\pm 2, \pm 4, -6, \pm 10\}$. Since f satisfies the second condition of Prop. 1.1, we deduce that $E(a, b)$ has multiplicative reduction at 3.

If f is not one the forms denoted by 1400S1, 1400T1, 2800QQ1 or 2800RR1 in [4], then $N_{K_f/\mathbf{Q}}(a'_3 \pm 4)$ belong to $\{4, 8, 10, 12, 16, 20\}$ and p divides one of them. This is a contradiction. So, f is necessarily one of the four forms above and we have $N_{K_f/\mathbf{Q}}(a'_3 \pm 4) = \pm 2 \cdot 29$ or $\pm 2 \cdot 11$. It then follows that $p = 29$. Besides, if $E(a, b)$ has good reduction at $q = 17$, then $a_{17} \in \{0, 2, 4, \pm 6, -8\}$, but by [4], 29 does not divide $N_{K_f/\mathbf{Q}}(a'_{17})$, $N_{K_f/\mathbf{Q}}(a'_{17} - 2)$, $N_{K_f/\mathbf{Q}}(a'_{17} - 4)$, $N_{K_f/\mathbf{Q}}(a'_{17} \pm 6)$ and $N_{K_f/\mathbf{Q}}(a'_{17} + 8)$. So, $E(a, b)$ has multiplicative reduction at $q = 17$, and 29 divides $N_{K_f/\mathbf{Q}}(a'_{17} \pm 18) = \pm 2^6 \cdot 79$ or $\pm 2^4 \cdot 359$. This leads us again to a contradiction, and we conclude that the eigenvalues of f are all rational integers.

In other words, f corresponds to an elliptic curve defined over $\mathbf{Q}$. There are exactly 6 isogeny classes of elliptic curves of level 350, 14 of level 1400 and 33 of level 2800. For all of them, we will contradict the conditions of Prop. 1.1 with $q = 3$, 11, 19, 23 or 37. As we have seen in §2, if $E(a, b)$ has good reduction at q, we can list the possible values of a_q. For the above prime numbers q, we find

$$a_3 = \pm 2, \qquad a_{11} \in \{0, \pm 4\}, \qquad a_{19} \in \{0, \pm 4\},$$
$$a_{23} \in \{0, \pm 2, \pm 4, \pm 6, \pm 8\} \quad \text{and} \quad a_{37} \in \{0, -2, \pm 4, -6, \pm 8, \pm 10, 12\}.$$

By the Hasse-Weil bound, $E(a, b)$ has good reduction at $q = 3$. We then deduce that f satisfies $a'_3 = \pm 2$. Among these curves, let us begin to deal with those without 2-torsion rational over $\mathbf{Q}$. If f is one of the curves denoted by 2800W1 and 2800AA1 in [4], we have $a'_{11} = \pm 3$ and this contradicts the congruences of Prop. 1.1 with $q = 11$. If f is one of the curves denoted by 1400D1, 1400K1, 2800D1 and 2800N1, we have $a'_{11} = \pm 1$. We then have a contradiction except maybe for $p = 13$. Besides, for these four curves, we have $a'_{23} = \pm 3$ and the same argument implies another contradiction except for $p = 19$. Bringing these two results together implies that f is not one of these 4 forms. If now f is one of the curves denoted by 1400C1, 1400N1, 2800E1 and 2800M1, we have $a'_{11} = \pm 5$. We then have a contradiction

except maybe for $p = 17$. Besides, for these curves, we have $a'_{19} = \pm 2$. By the same argument as before, a contradiction follows once more.

The two remaining curves of level 350, 1400 or 2800 such that $a'_3 = \pm 2$, denoted by 1400H1 and 2800G1, are the only two curves with non-trivial 2-torsion group. They satisfy $a'_{19} = \pm 2$ and $a'_{37} = 6$. Since these values do not belong to the set of possible values for a_{19} and a_{37} described above, we finally have a contradiction to the existence of a non-trivial primitive solution of $x^5 + y^5 = 7z^p$. □

3.3. **Case where $d = 13$.** In this paragraph, we prove the following theorem.

Theorem 3.4. *The equation $x^5+y^5 = 13z^p$ does not have any non-trivial primitive solutions for $p \geq 19$.*

Proof. Assume that (a, b, c) is a non-trivial primitive solution. It follows from [1, §3], that the representation ρ_p is irreducible, of weight $k = 2$ (since $p \neq 13$) and level $N(\rho_p) = 650$, 2600 or 5200.

Let q be a prime number different from 2, 5, 13 and p. By Prop. 1.1, p divides either $N_{K_f/\mathbf{Q}}\left(a'_q \pm (q+1)\right)$ or $N_{K_f/\mathbf{Q}}\left(a'_q - a_q\right)$. In other words, p is a prime factor of the resultant R_q of the minimal polynomial of a'_q and $P_q(X) = (X^2 - (q+1)^2)\prod(X - a_q)$, where the product runs over all possible values of a_q. For instance, if $q = 3$, then $P_3(X) = (X^2 - 16)(X^2 - 4)$.

Let us first assume that f has rational Fourier coefficients. If $a'_3 \neq \pm 2$, then R_3 has only 2, 3, 5 and 7 as prime factors. So we deduce that $a'_3 = \pm 2$. There are exactly 6 such newforms of level 650, 5 of level 2600 and 37 of level 5200 (for the curves of level 5200, the notation will exceptionally refer to [2]) . For all of them, a'_7 does not belong to the list $\{\pm 2, -4\}$ of possible values for a_7 when $E(a, b)$ has good reduction at 7. The same observation holds for the 13 elliptic curves of level 5200 with $a'_3 = \pm 2$ except for those denoted by 5200S1, 5200BB1, 5200AA1 and 5200Z1 (in [2]). If f is one of the first three of them, then we have $a'_{11} = 6$ or ± 2. Besides, if $E(a, b)$ has good reduction at 11, then a_{11} belongs to $\{0, \pm 4\}$. So, this is a contradiction and $f = 5200$Z1. Nevertheless, in this case, $a'_{17} = -2$ does not belong to the set $\{0, 2, 4, \pm 6, -8\}$ of possible values for a_{17} when $E(a, b)$ has good reduction at 17. We then deduce that the Fourier coefficients of f are not all rational.

Let us now assume that $N(\rho_p) = 650$ or 2800. For each f in these levels, $a'_3 = \alpha$ is a root of the polynomial defining K_f given in [4]. We then verify that R_3 is supported only by 2 and 5 except for the curves denoted 2800QQ1 and 2800RR1. But they both satisfy $a'_7 = \pm 1$, which leads us to a contradiction.

So we necessarily have $N(\rho_p) = 5200$. There are exactly 29 newforms of this level with non-rational eigenvalues numbered from 38 to 66. Four of them (those numbered 39, 42, 46 and 47) satisfy $a'_3 = 0$ or ± 1. So, f is not one of them. If f is curve number 63, then the field of coefficients is generated by a root α of the polynomial $x^4 + 6x^3 - 18x^2 - 30x + 25$ and

$$a'_3 = \frac{1}{10}\left(\alpha^3 + 6\alpha^2 - 13\alpha - 20\right).$$

Its characteristic polynomial is then $x^4+2x^3-7x^2-8x+16$ and we get $R_3 = 2^{18}$ in this case. This is of course a contradiction. The same conclusion will follow if f is curve number 64, since, in this case, the generating polynomial is $x^4+6x^3-87x^2-492x+604$ and the characteristic polynomial of a'_3 is $x^4 - 2x^3 - 7x^2 + 8x + 16$.

For all the other curves, $a'_3 = \alpha$ is a root of the generating polynomial of K_f given in the tables and we have a contradiction in the same way as before, by looking at R_3 except for the following eight pairs (f, p) :

$$(f = 54, p = 43), \quad (f = 55, p = 43), \quad (f = 58, p = 23), \quad (f = 59, p = 67),$$
$$(f = 61, p = 23), \quad (f = 62, p = 67), \quad (f = 65, p = 23), \quad (f = 66, p = 43).$$

For all of these, we have a contradiction as before by looking at the coefficient a'_7, except for the last two curves where we have to consider a'_{19}.

We finally deduce a contradiction to the existence of a non-trivial primitive solution of the equation $x^5 + y^5 = 13z^p$. □

4. The case $d = 3$ and limitations of the method

As is clearly apparent, the method will not work if there exists an elliptic curve over $\mathbf{Q}$ of the form $(\star)$ and level $N(\rho_p)$ (for large p). For convenience, we adopt the following definition, which makes this observation precise (where Supp denotes the support of an integer and v_2 the 2-adic valuation of $\mathbf{Q}$).

Definition 4.1. We say that there is a modular obstruction for the equation $x^5 + y^5 = dz^p$ (or just for d) if there exist two coprime integers (a, b) such that the following two conditions hold.

(1) The integer $m = a^5 + b^5$ is non-zero and we have

$$\mathrm{Supp}(m) \setminus \{2, 5\} = \mathrm{Supp}(d) \setminus \{2, 5\}.$$

(2) We have :
- if $\mathrm{Supp}(d)$ is not included in $\{2, 5\}$, then $ab \neq 0$,
- if $\mathrm{Supp}(d)$ is included in $\{2, 5\}$ and d is even, then $ab \neq 0$,
- if d is odd, then $v_2(m) \neq 2$,
- if $v_2(d) = 1$, then we have either $v_2(m) \geq 3$, or $v_2(m) = 1$, or $\max(v_2(a), v_2(b)) = 1$,
- if $v_2(d) = 2$, then $v_2(m) = 2$,
- if $v_2(d) \geq 3$, then $v_2(m) \geq 3$.

The following lemma gives a sufficient condition to insure that there is no modular obstruction, for several given d.

Lemma 4.2. *Let d be a positive integer such that for any prime ℓ dividing d, we have $\ell \not\equiv 1 \pmod 5$. Then, there is a modular obstruction for d if and only if $d = 5^\gamma$ or $d = 2 \cdot 5^\gamma$ with $\gamma \geq 0$.*

Proof. Assume that there is a modular obstruction for d given by two coprime integers (a, b). Then $m = a^5 + b^5$ is non-zero and $\mathrm{Supp}(m) \setminus \{2, 5\} = \mathrm{Supp}(d) \setminus \{2, 5\}$. Following [1], let us denote by ϕ the irreducible polynomial

$$\phi(x, y) = x^4 - x^3y + x^2y^2 - xy^3 + y^4.$$

By Lemmas 2.5 and 2.6 of [1] and the hypothesis, we have:

(1) either 5 divides m and then $\phi(a, b) = \pm 5$;
(2) or 5 does not divide m and then $\phi(a, b) = \pm 1$.

In other words, (a, b) is a solution of a Thue equation of the form $\phi(x, y) = A$, where $A = \pm 1$ or ± 5 and we can assume that $a \neq 0$ (ϕ is symmetric). Since ϕ is totally complex, this leads to

$$|A| = |a|^4 \prod_{k=1}^{4} |b/a - \alpha_k| \geq |a|^4 \sin^2\left(\frac{2\pi}{5}\right) \cdot \sin^2\left(\frac{4\pi}{5}\right) \geq 0.312 \cdot |a|^4,$$

where $\alpha_k = -\exp(2ik\pi/5)$, $k = 1, \ldots, 4$, are the roots of $\phi(1, x)$. This gives an upper bound for $|a|$.

In the first case, this implies that we have $(a, b) = (1, -1)$ or $(-1, 1)$ and then $m = 0$, which is a contradiction. In the second case, we deduce

$$(a, b) \in \{(1, 1), (-1, -1), (\pm 1, 0), (0, \pm 1)\}.$$

In other words, $m = \pm 1$ or $m = \pm 2$. By the first condition of Def. 4.1, there exist $\alpha, \gamma \geq 0$ such that $d = 2^\alpha \cdot 5^\gamma$. Since $v_2(m) = 0$ or 1, we have, by the second condition, $\alpha = 0$ or 1.

Conversely, if $d = 5^\gamma$ or $d = 2 \cdot 5^\gamma$ with $\gamma \geq 0$, there is a modular obstruction for d given, for example, by $(a, b) = (1, 1)$. □

Remark 4.3. For $d = 11$, there is a modular obstruction given by the elliptic curves $E(2, 3)$ or $E(3, -1)$. Note that, in general, finding a modular obstruction for d involves solving some Thue-Mahler equation. Such an equation can be explicitly solved ([5]), although its solution might turn out to be very complicated.

Let us now look at the case where $d = 3$. By the previous lemma, there is no modular obstruction. Nevertheless, as we will see, we were not able to solve this equation for all p.

Fix for now a prime p and let (a, b, c) be a non-trivial primitive solution of the equation $x^5 + y^5 = 3z^p$. The following lemma makes more precise Lemma 4.3 of [1]. We warn the reader that in this paragraph we are using only Stein's notation [4] for modular forms (including elliptic curves). This is not the case in [1], where the author was referring to Cremona's Tables of elliptic curves [2].

Lemma 4.4. *If $p \geq 17$, then we have*

1. *either 5 divides $a + b$ and $f =$ 1200K1, or*
2. *5 does not divide $a + b$ and $f =$ 1200A1.*

Proof. Assume that 5 divides $a + b$. By Lemma 4.3 of [1], f is one of the following newforms (in Stein's notation) :

$$150B1, 600C1, 600A1, 1200O1, 1200R1, 1200E1, 1200K1.$$

If $f =$ 150B1, 600C1, 1200O1, 1200R1 or 1200E1, we have $a'_7 = 0$ or 4. Besides, if $E(a, b)$ has good reduction at 7, we have $a_7 = \pm 2$ or -4. We then obtain a contradiction by looking at the conditions of Prop. 1.1 for $q = 7$. If $f =$ 600A1, then $a'_{13} = 6$. Besides, if $E(a, b)$ has good reduction at 13, then a_{13} belongs to the set $\{0, \pm 2, \pm 4\}$. So, there is again a contradiction. So, $f =$ 1200K1 in this case.

Assume now that 5 does not divide $a + b$. By Lemma 4.3 of [1], f is one of the following newforms (in Stein's notation) :

$$150A1, 150C1, 600D1, 600G1, 1200H1, 1200L1, 1200G1, 1200A1, 1200M1, 1200S1.$$

For $f =$ 1200S1 we have $a'_7 = 4$ and using this coefficient we derive again a contradiction. For all the other curves except 1200A1, we have $a'_{11} = \pm 2$. Besides, if

$E(a,b)$ has good reduction at 11, we have $a_{11} = 0$ or ± 4. So, f is not one of them and we conclude that $f = 1200\text{A}1$ in this case. □

If $f = 1200\text{K}1$ or $1200\text{A}1$, then for any prime $q > 5$ smaller than 5000, the Fourier coefficient a'_q of f actually lies in the list of possible values for a_q. This is why we have not been able to prove the emptiness of the set of non-trivial primitive solutions for $d = 3$.

Nevertheless, we will give a criterion which is an improvement of the one given in [1] (cf. Th. 4.5). This allows us to conclude the argument for a fixed p; we have verified that it holds for any $17 \leq p \leq 10^7$. Let us consider q a prime number congruent to 1 modulo p, and write $q = np + 1$. The group $\mu_n(\mathbf{F}_q)$ of nth roots of unity in $\mathbf{F}_q$ has order n. We now define four subsets $A^{\pm}(n,q)$ and $B^{\pm}(n,q)$ of $\mu_n(\mathbf{F}_q)$ in the following way.

(1) Let $\widetilde{A}(n,q)$ be the subset of $\mu_n(\mathbf{F}_q)$ consisting of all ζ such that

$$405 + 62500\zeta \text{ is a square in } \mathbf{F}_q.$$

For such a ζ, let us consider the smallest integer $\delta_{1,\zeta} \geq 0$ such that

$$\delta_{1,\zeta}^2 \pmod q = 405 + 62500\zeta.$$

We define $A^+(n,q)$ (resp. $A^-(n,q)$) as the subset of $\widetilde{A}(n,q)$ consisting of ζ such that

$$-225 + 10\delta_{1,\zeta} \quad (\text{resp. } -225 - 10\delta_{1,\zeta})$$

is a square modulo q. For any $\zeta \in A^+(n,q)$, let us consider the cubic curve over $\mathbf{F}_q$ defined by the equation

$$F^+_{1,\zeta} : y^2 = x^3 - \frac{\delta_{1,\zeta}}{25}x^2 + 25\zeta x.$$

Its discriminant $6480\zeta^2 = 2^4 \cdot 3^4 \cdot 5\zeta^2$ is non-zero and $F^+_{1,\zeta}$ is an elliptic curve over $\mathbf{F}_q$. Let us denote by $n^+_{1,q}(\zeta)$ the number of $\mathbf{F}_q$-rational points of $F^+_{1,\zeta}$ and write

$$a^+_q(\zeta) = q + 1 - n^+_{1,q}(\zeta).$$

If $\zeta \in A^-(n,q)$, let us define, in the same way, the cubic curve

$$F^-_{1,\zeta} : y^2 = x^3 + \frac{\delta_{1,\zeta}}{25}x^2 + 25\zeta x.$$

As a twist of $F^+_{1,\zeta}$, it is also an elliptic curve over $\mathbf{F}_q$ and we write

$$a^-_q(\zeta) = q + 1 - n^-_{1,q}(\zeta),$$

where $n^-_{1,q}(\zeta)$ denotes the number of $\mathbf{F}_q$-rational points of $F^-_{1,\zeta}$.

(2) Let $\widetilde{B}(n,q)$ be the subset of $\mu_n(\mathbf{F}_q)$ consisting of all ζ such that

$$405 + 20\zeta \text{ is a square in } \mathbf{F}_q.$$

For such a ζ, let us consider the smallest integer $\delta_{2,\zeta} \geq 0$ such that

$$\delta_{2,\zeta}^2 \pmod q = 405 + 20\zeta.$$

We define $B^+(n,q)$ (resp. $B^-(n,q)$) as the subset of $\widetilde{B}(n,q)$ consisting of ζ such that

$$-225 + 10\delta_{2,\zeta} \quad (\text{resp. } -225 - 10\delta_{2,\zeta})$$

is a square modulo q. For any $\zeta \in B^+(n,q)$, let us consider the cubic curve over $\mathbf{F}_q$ defined by the equation

$$F^+_{2,\zeta} : y^2 = x^3 - \delta_{2,\zeta} x^2 + 5\zeta x.$$

Its discriminant $2^4 \cdot 3^4 \cdot 5^3 \zeta^2$ is non-zero and $F^+_{2,\zeta}$ is an elliptic curve over $\mathbf{F}_q$. Let us denote by $n^+_{2,q}(\zeta)$ the number of $\mathbf{F}_q$-rational points of $F^+_{2,\zeta}$ and write

$$b^+_q(\zeta) = q + 1 - n^+_{2,q}(\zeta).$$

If $\zeta \in B^-(n,q)$, let us define, in the same way, the cubic curve

$$F^-_{2,\zeta} : y^2 = x^3 + \delta_{2,\zeta} x^2 + 5\zeta x.$$

As a twist of $F^+_{2,\zeta}$, it is also an elliptic curve over $\mathbf{F}_q$ and we write

$$b^-_q(\zeta) = q + 1 - n^-_{2,q}(\zeta),$$

where $n^-_{2,q}(\zeta)$ denotes the number of $\mathbf{F}_q$-rational points of $F^-_{2,\zeta}$.

Our criterion is stated in the following theorem. It is a refinement of [1, Th. 1.4], since only two curves have to be removed, instead of seven in loc. cit.

Theorem 4.5. *Let p be a prime number ≥ 17. Assume that the following two conditions hold.*

(1) *For the curve $f = 1200\mathrm{K}1$, there exists an integer $n \geq 2$ such that*
   (a) *the integer $q = np + 1$ is a prime number;*
   (b) *we have $a'^2_q \not\equiv 4 \pmod{p}$;*
   (c) *for all ζ in $A^+(n,q)$, we have $a'_q \not\equiv a^+_q(\zeta) \pmod{p}$;*
   (d) *for all ζ in $A^-(n,q)$, we have $a'_q \not\equiv a^-_q(\zeta) \pmod{p}$.*

(2) *For the curve $f = 1200\mathrm{A}1$, there exists an integer $n \geq 2$ such that*
   (a) *the integer $q = np + 1$ is a prime number;*
   (b) *we have $a'^2_q \not\equiv 4 \pmod{p}$;*
   (c) *for all ζ in $B^+(n,q)$, we have $a'_q \not\equiv b^+_q(\zeta) \pmod{p}$;*
   (d) *for all ζ in $B^-(n,q)$, we have $a'_q \not\equiv b^-_q(\zeta) \pmod{p}$.*

Then, there is no non-trivial primitive solution of $x^5 + y^5 = 3z^p$.

Proof. Let n be as in the theorem. By Lemma 4.4, ρ_p is isomorphic to the mod p representation $\overline{\sigma_{f,p}}$ of $f = 1200\mathrm{A}1$ or $1200\mathrm{K}1$. If $E(a,b)$ does not have good reduction at q, then $E(a,b)$ has multiplicative reduction ([1, Lem. 2.7]) and by [3, Prop. 3(*iii*)], we have

$$a'_q \equiv \pm(q+1) \equiv \pm 2 \pmod{p}.$$

This contradicts the conditions (4.5) and (4.5) of the theorem. So, we deduce that $E(a,b)$ has good reduction at q; in other words, q does not divide c.

We now follow step by step the discussion of [1, §4.4], without giving all the details. Let us denote by ϕ the polynomial $\phi(x,y) = x^4 - x^3y + x^2y^2 - xy^3 + y^4$ and by $\overline{a}$ (resp. $\overline{b}$) the reduction of a (resp. b) modulo q.

(1) Assume that 5 divides $a + b$. Then, there exist two integers c_1 and c_2 such that

$$5(a+b) = 3c_1^p, \quad \phi(a,b) = 5c_2^p \quad \text{and} \quad c = c_1 c_2.$$

Furthermore, if $u = c_1^p \pmod{q}$ and $v = c_2^p \pmod{q}$, then

$$\overline{a}' = \frac{\overline{a}}{u}, \quad \overline{b}' = \frac{\overline{b}}{u} \quad \text{and} \quad \zeta = \frac{v}{u^4}$$

satisfy

$$5(\overline{a}' + \overline{b}') = 3 \quad \text{and} \quad \phi(\overline{a}', \overline{b}') = 5\zeta.$$

We then deduce that $\overline{b}'$ is a root of the polynomial

$$P_{1,\zeta}(X) = X^4 - \frac{6}{5}X^3 + \frac{18}{25}X^2 - \frac{27}{125}X + \frac{81}{3125} - \zeta \in \mathbf{F}_q[X].$$

So, $\overline{b}'$ is one of the following elements:

$$\frac{3}{10} + \frac{\alpha_{1,\zeta}}{50}, \quad \frac{3}{10} - \frac{\alpha_{1,\zeta}}{50}, \quad \frac{3}{10} + \frac{\beta_{1,\zeta}}{50}, \quad \frac{3}{10} - \frac{\beta_{1,\zeta}}{50},$$

where $\alpha_{1,\zeta}$ (resp. $\beta_{1,\zeta}$) is a square root of $-225 + 10\delta_{1,\zeta}$ (resp. $-225 - 10\delta_{1,\zeta}$) modulo q.

(a) Assume that we have

$$\left\{\overline{a}', \overline{b}'\right\} = \left\{\frac{3}{10} + \frac{\alpha_{1,\zeta}}{50}, \frac{3}{10} - \frac{\alpha_{1,\zeta}}{50}\right\}.$$

Then ζ belongs to the set $A^+(n,q)$ and the reduction modulo q of the curve $E(a,b)$ is isomorphic to $F^+_{1,\zeta}$. So we deduce that

$$a_q \equiv a_q^+(\zeta) \pmod{p}.$$

But, by Lemma 4.4, we have $a_q \equiv a'_q \pmod{p}$, where a'_q is the qth Fourier coefficient of 1200K1. This contradicts our hypothesis (4.5).

(b) Assume that we have

$$\left\{\overline{a}', \overline{b}'\right\} = \left\{\frac{3}{10} + \frac{\beta_{1,\zeta}}{50}, \frac{3}{10} - \frac{\beta_{1,\zeta}}{50}\right\}.$$

Then ζ belongs to the set $A^-(n,q)$ and the reduction modulo q of the curve $E(a,b)$ is isomorphic to $F^-_{1,\zeta}$. So we deduce that

$$a_q \equiv a_q^-(\zeta) \pmod{p}.$$

But, by Lemma 4.4, we have $a_q \equiv a'_q \pmod{p}$, where a'_q is the qth Fourier coefficient of 1200K1. This contradicts our hypothesis (4.5).

We finally deduce that 5 does not divide $a + b$.

(2) If 5 does not divide $a + b$, then there exist two integers c_1 and c_2 such that

$$a + b = 3c_1^p, \quad \phi(a,b) = c_2^p \quad \text{and} \quad c = c_1c_2.$$

Furthermore, if $u = c_1^p \pmod{q}$ and $v = c_2^p \pmod{q}$, then

$$\overline{a}' = \frac{\overline{a}}{u}, \quad \overline{b}' = \frac{\overline{b}}{u} \quad \text{and} \quad \zeta = \frac{v}{u^4}$$

satisfy

$$\overline{a}' + \overline{b}' = 3 \quad \text{and} \quad \phi(\overline{a}', \overline{b}') = \zeta.$$

We then deduce that $\overline{b}'$ is a root of the polynomial

$$P_{2,\zeta}(X) = X^4 - 6X^3 + 18X^2 - 27X + \frac{81 - \zeta}{5} \in \mathbf{F}_q[X].$$

So, $\overline{b}'$ is one of the elements

$$\frac{3}{2} + \frac{\alpha_{2,\zeta}}{10}, \quad \frac{3}{2} - \frac{\alpha_{2,\zeta}}{10}, \quad \frac{3}{2} + \frac{\beta_{2,\zeta}}{10}, \quad \frac{3}{2} - \frac{\beta_{2,\zeta}}{10},$$

where $\alpha_{2,\zeta}$ (resp. $\beta_{2,\zeta}$) is a square root of $-225+10\delta_{2,\zeta}$ (resp. $-225-10\delta_{2,\zeta}$) modulo q.

(a) Assume that we have

$$\left\{\overline{a}', \overline{b}'\right\} = \left\{\frac{3}{2}+\frac{\alpha_{2,\zeta}}{10}, \frac{3}{2}-\frac{\alpha_{2,\zeta}}{10}\right\}.$$

Then ζ belongs to the set $B^+(n,q)$ and the reduction modulo q of the curve $E(a,b)$ is isomorphic to $F^+_{2,\zeta}$. So we deduce that

$$a_q \equiv b_q^+(\zeta) \pmod{p}.$$

But, by Lemma 4.4, we have $a_q \equiv a'_q \pmod{p}$, where a'_q is the qth Fourier coefficient of 1200A1. This contradicts our hypothesis (4.5).

(b) Assume that we have

$$\left\{\overline{a}', \overline{b}'\right\} = \left\{\frac{3}{2}+\frac{\beta_{2,\zeta}}{10}, \frac{3}{2}-\frac{\beta_{2,\zeta}}{10}\right\}.$$

Then ζ belongs to the set $B^-(n,q)$ and the reduction modulo q of the curve $E(a,b)$ is isomorphic to $F^-_{2,\zeta}$. So we deduce that

$$a_q \equiv b_q^-(\zeta) \pmod{p}.$$

But, by Lemma 4.4, we have $a_q \equiv a'_q \pmod{p}$, where a'_q is the qth Fourier coefficient of 1200A1. This contradicts our hypothesis (4.5).

We finally deduce that there is no non-trivial primitive solution of the equation $x^5+y^5=3z^p$. □

Remark 4.6. For a given p, a `pari/gp` program giving an integer n as in the theorem is available at: `http://www.institut.math.jussieu.fr/billerey/Fermatnew`. Using this and [1, Prop. 1.1], we were able to prove that the equation $x^5+y^5=3z^p$ does not have a non-trivial primitive solution for $5 \leq p \leq 10^7$.

References

1. Nicolas Billerey. Équations de Fermat de type $(5,5,p)$. *Bull. Austral. Math. Soc.*, 76(2):161–194, 2007. MR2353205 (2008i:11049)
2. J. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997. MR1628193 (99e:11068)
3. A. Kraus and J. Oesterlé. Sur une question de B. Mazur. *Math. Ann.*, 293:259–275, 1992. MR1166121 (93e:11074)
4. W. Stein. The Modular Forms Database. `http://modular.fas.harvard.edu/Tables`, 2004.
5. N. Tzanakis and B. M. M. de Weger. How to explicitly solve a Thue-Mahler equation. *Compositio Math.*, 84(3):223–288, 1992. MR1189890 (93k:11025)

Université Pierre et Marie Curie – Paris 6, UMR 7586, Case 247, 4, place Jussieu, Institut de Mathématiques, 75252 Paris, France
E-mail address: `billerey@math.jussieu.fr`

Departament d'Algebra i Geometria, Universitat de Barcelona, Gran Via de les Corts Catalanes 585, (08007) Barcelona, Spain
E-mail address: `ldieulefait@ub.edu`