A SUPERELLIPTIC EQUATION INVOLVING ALTERNATING SUMS OF POWERS

MICHAEL A. BENNETT

Dedicated to Kalman Győry on the occasion of his 70th birthday

Abstract. In this short note, we solve completely the Diophantine equation

$$1^k - 3^k + 5^k - \cdots + (4x-3)^k - (4x-1)^k = -y^n,$$

for $3 \leq k \leq 6$. This may be viewed as a "character-twisted" analogue of a classic equation of Schaffer (in which context, it was previously considered by Dilcher). In our proof, we appeal primarily to techniques based upon the modularity of Galois representations and, in particular, to a combination of these ideas with suitable local information.

1. Introduction

In the study of Diophantine equations, there exists an interesting, and sometimes subtle, distinction between the effective and the explicit. As a case in point, given a polynomial $f(x) \in \mathbb{Z}[x]$, with, say, three distinct simple complex roots, the *superelliptic* equation

$$f(x) = y^n$$

has, effectively, at most finitely many solutions in integers x, y and *variable* $n \geq 2$, via work of Schinzel and Tijdeman [8] using lower bounds for linear forms in logarithms. Here, we count the solutions with $y^n = 0$ or ± 1 only once. On the other hand, there are really very few situations where such equations can be completely solved, essentially all corresponding to polynomials $f(x)$ with factors over $\mathbb{Z}[x]$ of very small degree (typically, at most three). As a case study, consider the equation

$$1^k + 2^k + \cdots + x^k = y^n. \tag{1.1}$$

Here, the left-hand-side can be expressed as a polynomial $f_k(x)$ of degree $k+1$ in $\mathbb{Q}[x]$, where the denominators of the corresponding coefficients are well behaved. The presence of linear factors $x(x+1)$ in $f_k(x)$ makes it possible (see [2]) to solve equation (1.1) completely when, say, $k \leq 11$. The techniques of [2], while not strictly speaking "algorithmic", do provide a method for explicitly solving (1.1) for any k of moderate size.

We have, in general, no analogous approach for the apparently similar equation

$$1^k - 3^k + 5^k - \cdots + (4x-3)^k - (4x-1)^k = -y^n, \tag{1.2}$$

effectively solved by Dilcher [5]. If we set

$$g_k(x) = 1^k - 3^k + 5^k - \cdots + (4x-3)^k - (4x-1)^k,$$

Date: May 8, 2011.

The author was supported in part by a grant from NSERC.

then $g_k(x)$ is related (see [5]) to the classical Euler polynomials via the identity

$$g_k(x) = -2^{k-1}E_k(2x + 1/2).$$

Work of Brillhart [4] therefore classifies the rational and repeated roots of the polynomials $g_k(x)$; in the following table, we list the first few values of $g_k(x)$:

k	$g_k(x)$	k	$g_k(x)$
1	$-2x$	4	$-16x^2(8x^2 - 3)$
2	$-8x^2$	5	$-2x(16x^2 - 5)^2$
3	$-2x(16x^2 - 3)$	6	$-8x^2(256x^4 - 240x^2 + 75)$

It is worth noting that, at least for $k \geq 6$, there are no $g_k(x)$ known to possess an irreducible quadratic factor.

In this paper, we will show that it is still possible to solve equation (1.2), at least for small values of k; we prove the following

Theorem 1.1. *Let $k \in \{3, 4, 5, 6\}$. If there exist positive integers x, y and $n \geq 2$ satisfying (1.2), then*

$$(k, x, y, n) = (5, 2\,t^2, 2\,t\,(64t^4 - 5), 2),$$

for t a positive integer.

We would like to emphasize that, in contrast to the work of Győry, Pintér and the author [2] on equation (1.1), we are genuinely unable to treat values of $k \geq 7$. For the cases $k \in \{3, 4, 5\}$, our approach is a simple appeal to known results on ternary Diophantine equations, together with some machinery for solving cubic Thue inequalities. The novelty of our approach, we must confess, is limited to the case $k = 6$. Here, we apply local information at the primes 2 and 7, together with techniques based upon associating Frey-Hellegouarch curves to modular forms, to conclude that (1.2) has no solutions in nonzero integers. These ideas have applications to more general superelliptic equations, but we will not explore them here.

2. Proof of Theorem 1.1 : the cases $k = 3, 4$ and 5

We begin with the straightforward cases, treating each value of $k \in \{3, 4, 5\}$ in turn.

2.1. **$k = 3$.** Let us suppose first that $k = 3$ and write $d = \gcd(x, 16x^2 - 3)$, so that $d \in \{1, 3\}$. We thus have

$$x = 2^{n-1}\,d^{n-1}\,a^n \quad \text{and} \quad 16x^2 - 3 = d\,b^n,$$

for positive integers a and b (whereby, from considering the latter equation modulo 8, we may suppose that n is an odd prime). If $d = 3$, writing $c = 2^{n+1}3^{n-2}a^n$, we have $b^n + 1 = 3c^2$. This immediately contradicts Theorem 1.1 of [3], provided $n \geq 4$. If $n = 3$, we have

$$4(12a^2)^3 - b^3 = 1,$$

whereby the inequality

$$\left|x^3 - 2y^3\right| \geq \sqrt{|x|}, \tag{2.1}$$

valid for all integers x and y (see Theorem 6.1 of [1]), implies $24a^2 \leq 4$, and so $a = 0$.

If, on the other hand, we have $d = 1$, then

$$b^n - 2^{2n+2}a^{2n} = -3.$$

For $n \geq 5$ prime, this contradicts work of Kraus [6], since it implies the existence of a weight 2 cuspidal newform of level 6. If $n = 3$, we may again appeal to inequality (2.1) to conclude as desired.

2.2. $k = 4$**.** Next, we turn our attention to the case $k = 4$, setting

$$d = \gcd(16x^2, 8x^2 - 3) \in \{1, 3\},$$

so that

$$16x^2 = 2^{2n}d^{n-1}a^n \text{ and } 8x^2 - 3 = d\,b^n,$$

for positive integers a and b. The latter equation is insoluble modulo 8 if $n = 2$; we thus suppose that n is an odd prime (so that $a = a_1^2$ is a perfect square). If $d = 3$, then for $c = 2^{n-1}3^{(n-3)/2}a_1^n$ we have $b^n + 1 = 6c^2$. Again, Theorem 1.1 of [3] implies that $n = 3$. We thus have $12\,(2a)^3 - b^3 = 1$ and hence

$$\left| \sqrt[3]{12} - \frac{b}{2a} \right| < \frac{1}{3 \cdot 12^{2/3}\,(2a)^3}.$$

Combining this with the inequality

$$\left| \sqrt[3]{12} - \frac{b}{2a} \right| > 0.28\,(2a)^{-2.95},$$

valid for all positive integers a and b (see Corollary 1.2 of [1]) implies that $a = 0$, a contradiction.

If $k = 4$ and $d = 1$, then

$$b^n - 2^{n-1}a^n = -3.$$

As previously, we appeal to [6] for $n \geq 5$ prime (where the implied newforms are now at levels 3 or 6), or to inequality (2.1), if $n = 3$.

2.3. $k = 5$**.** To begin, let us observe that if $n = 2$, we have that necessarily $2x$ is a square, say $x = 2t^2$ for t a positive integer. We thus obtain the infinite family of solutions referenced in Theorem 1.1. For the remainder of this subsection, let us suppose that n is either an odd prime, or that $n = 4$. Writing

$$d = \gcd(x, 16x^2 - 5) \in \{1, 5\},$$

there exist positive integers a and b for which

$$2x = d^{n-2}2^n a^n \text{ and } (16x^2 - 5)^2 = d^2 b^n,$$

whence either $n = 4$ or we can find b_1 such that $b = b_1^2$. In the first case, we have $16x^2 - 5 = db^2$, a contradiction modulo 4. In the second, if $d = 5$, we have $b_1^n + 1 = 5c^2$, for $c = 2^{n+1}5^{n-3}a^n$ and so Theorem 1.1 of [3] again suffices to treat $n \geq 5$. If $n = 3$, then $1280\,a^6 - 1 = b_1^3$, whereby

$$\left| \sqrt[3]{20} - \frac{b_1}{4a^2} \right| < \frac{1}{3 \cdot 20^{2/3}\,64\,a^6}.$$

In conjunction with the inequality

$$\left| \sqrt[3]{20} - \frac{p}{q} \right| > 0.01\,q^{-2.23},$$

valid for all positive integers p and q (again see Corollary 1.2 of [1]), we obtain that $a = 1$, a contradiction. If, however, $d = 1$, then

$$b_1^n - 2^{2n+2}a^{2n} = -5.$$

The techniques of [6] allow us to conclude as desired for $n \geq 5$ prime (since there do not exist cuspidal newforms of weight 2 and level 10), while inequality (2.1) does likewise, in case $n = 3$

3. Proof of Theorem 1.1 : the case $k = 6$

We now complete the proof of Theorem 1.1 by treating the case $k = 6$. Notice that $g_6(x)$ is always divisible by 2 to an odd exponent, whereby we may assume, without loss of generality, that n is an odd prime. Set

$$d = \gcd(8x^2, 256x^4 - 240x^2 + 75) \in \{1, 3, 25, 75\}.$$

There thus exist positive integers a and b for which

$$8x^2 = 2^n \, 3^{\nu_3(d)(n-1)} \, 5^{\nu_5(d)(n-2)/2} \, a^n \quad \text{and} \quad 256x^4 - 240x^2 + 75 = d \, b^n,$$

where $\nu_p(d)$ denotes the largest power of p dividing d. Writing $d \, d_1 = 75$, the second equation becomes

$$3^{\nu_3(d)}c^2 + d_1 = 4b^n, \tag{3.1}$$

where

$$c = 2^{n+2} \cdot 3^{\nu_3(d)(n-2)} \cdot 5^{\nu_5(d)(n-3)/2} \cdot a^n - 15 \cdot 3^{-\nu_3(d)} \cdot 5^{-\nu_5(d)/2}.$$

Suppose first that $n \geq 7$ is prime. Following [3], we define a Frey-Hellegouarch curve

$$E \ : \ Y^2 = X^3 + 3^{\nu_3(d)} \, cX^2 + 3^{\nu_3(d)} \, b^n X.$$

Notice that, for each choice of d, we have

$$b \equiv -c \equiv -3^{\nu_3(d)} \pmod 4.$$

Combining Lemmata 2.1 and 3.3 of [3] thus implies that the canonical representation ρ_n^E of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the n-torsion points of E arises from a weight 2, cuspidal newform f of trivial Nebentypus character and level

$$N = 2^2 \cdot 3^{1+\nu_3(d)} \cdot 5^{1-\nu_5(d)/2}.$$

For $d = 1$ or $d = 25$, the absence of nonzero cuspforms at levels 60 and 12, respectively, therefore completes the proof of Theorem 1.1, in case $n \geq 7$ is prime. If $d = 75$, equation (3.1) has, via Theorem 1.2 of [3], no solutions in integers $c > 1$.

The primary novelty in this paper lies in our treatment of the remaining case, when $d = 3$. Here, equation (3.1) becomes

$$3c^2 + 25 = 4b^n \tag{3.2}$$

and ρ_n^E arises from a weight 2, cuspidal newform f of level 180. Since this space is one-dimensional, corresponding to an elliptic curve $E_1/\mathbb{Q}$ of conductor 180, it follows that, for each prime p coprime to $30\,n$, we have

$$a_p(E) \equiv a_p(E_1) \pmod n, \tag{3.3}$$

if p fails to divide b, while

$$a_p(E_1) \equiv \pm(p+1) \pmod n, \tag{3.4}$$

if $p \mid b$.

We will apply these congruences with $p = 7$ – the choice of prime here is, as we shall see, far from arbitrary. For our purposes, it is crucial that $a_7(E_1) = 2$. Note that from (3.2), the value of $a_7(E)$ is completely determined by the residue class of c modulo 7. If $c \equiv \pm 1 \pmod 7$, then $7 \mid b$ and so (3.4) implies that $n \leq 5$. Otherwise, we have $a_7(E) = 0$ (if $c \equiv 0, \pm 3 \pmod 7$) or $a_7(E) = \pm 4$ (if $c \equiv \pm 2 \pmod 7$). In each case, $a_7(E) \neq a_7(E_1)$ and appealing to (3.3) leads to the conclusion that $n \leq 5$.

It remains, then, to treat the exponents $n = 3$ and 5. In the first case, solutions to (3.1) correspond to integral points on elliptic curves of the shape

$$E \ : \ Y^2 = X^3 - 2^4 \cdot 3^{1+2\nu_3(d)} \cdot 5^{2-\nu_5(d)}.$$

Standard computational packages (e.g. Magma) for finding such points on fixed models of elliptic curves may thus be applied to show that there are no integer points on E, if $d = 1$ or 3, and, if $d = 25$, only the points $(X, Y) = (4, \pm 4)$ and $(28, \pm 148)$, corresponding to $(b, c) = (1, \pm 1)$ and $(7, \pm 37)$ in equation (3.1). None of these have, as required in this case, $c \equiv -3 \pmod{32}$. If $d = 75$, we find the points $(X, Y) = (12, \pm 36)$, corresponding to $c = \pm 1$, again a contradiction.

Finally, let us suppose that $n = 5$. In case $d = 1$, the fact that $x^2 = 4a^5$ implies that $a = a_1^2$ for some integer a_1, and so $x^2 \equiv \pm 4 \pmod{25}$, whereby

$$b^5 \equiv -4 \pm 10 \pmod{25},$$

a contradiction. For $d \in \{3, 25, 75\}$, we note that solutions to (3.1) imply the existence of integral points on hyperelliptic curves of the shape

$$C \ : \ Y^2 = X^5 - 2^8 \cdot 3^{1+4\nu_3(d)} \cdot 5^{2-\nu_5(d)}.$$

In case $d = 3$, since the Jacobian $\mathrm{Jac}(C)$ is readily shown to have rank 0 over $\mathbb{Q}$, a relatively easy application of Chabauty techniques implies that no such points exist. If $d = 25$ or 75, we can argue similarly, or note that, since the curves C have defining equations of the shape $Y^2 = X^5 - 2^\alpha 3^\beta$ and Theorem 5.1 of Mulholland [7] provides all solutions to equations of these types, we may conclude that $(X, Y) = (4, \pm 16)$, if $d = 25$, and that $(X, Y) = (12, \pm 432)$, if $d = 75$. In each case, these correspond to $c = \pm 1$. This contradiction finishes the proof of Theorem 1.1.

4. Concluding remarks

What we have really proved in our treatment of equation (3.2) is the following :

Theorem 4.1. *The Diophantine equation*

$$3c^2 + 25 = 4b^n$$

has no solutions in coprime integers b and c with $c \equiv \pm 3 \pmod 8$, and integer $n \geq 2$.

One can probably solve this equation completely, without restriction upon c, though not through a simple application of techniques based solely upon the modularity of Galois representations. Indeed, for $c \equiv \pm 1 \pmod 8$, after suitable level lowering, one is led to consider modular forms of level 360 rather than 180. At the former level, there are five forms, each one-dimensional, three of which resist easy elimination. Our argument based upon analysis of Fourier coefficients at $p = 7$ fails in such a case, since one of these forms corresponds to an elliptic curve $E_1/\mathbb{Q}$ with $a_7(E_1) = -4$.

References

[1] M.A. Bennett, Effective measures of irrationality for certain algebraic numbers, *J. Austral. Math. Soc.* 62 (1997), 329–344.
[2] M.A. Bennett, K. Győry and Á. Pintér, On the Diophantine equation $1^k+2^k+\cdots+x^k = y^n$, *Compositio Math.* 140 (2004), 1417–1431.
[3] M.A. Bennett and C. Skinner, Ternary Diophantine equations via Galois representations and modular forms, *Canad. J. Math.* 56 (2004), 23–54.
[4] J. Brillhart, On the Euler and Bernoulli polynomials, *J. Reine Angew. Math.* 234 (1969), 45–64.
[5] K. Dilcher, On a diophantine equation involving quadratic characters, *Compositio Math.* 57 (1986), 383–403.
[6] A. Kraus, Majorations effectives pour l'équation de Fermat généralisée, *Canad. J. Math.* 49 (1997), 1139–1161.
[7] J. Mulholland, Elliptic Curves with Rational 2-torsion and Related Ternary Diophantine Equations, Ph.D. Thesis, University of British Columbia, 2006.
[8] A. Schinzel and R. Tijdeman, On the equation $y^m = P(x)$, *Acta Arith.* 31 (1976), 199–204.

Department of Mathematics, University of British Columbia, Vancouver BC
E-mail address: bennett@math.ubc.ca