On powers that are sums of consecutive like powers

Vandita Patel and Samir Siksek

Abstract

Let \( k \geq 2 \) be even, and let \( r \) be a non-zero integer. We show that for almost all \( d \geq 2 \) (in the sense of natural density), the equation

\[
x^k + (x + r)^k + \cdots + (x + (d - 1)r)^k = y^n, \quad x, y, n \in \mathbb{Z}, \quad n \geq 2,
\]

has no solutions.

Keywords: Exponential equation, Bernoulli polynomial, Newton polygon

Mathematics Subject Classification: Primary 11D61, Secondary 11B68

1 Background

The problem of cubes that are sums of consecutive cubes goes back to Euler ([10] art. 249) who noted the remarkable relation \( 3^3 + 4^3 + 5^3 = 6^3 \). Similar problems were considered by several mathematicians during the nineteenth and early twentieth century as surveyed in Dickson’s History of the Theory of Numbers ([7] p. 582–588). These questions are still of interest today. For example, both Cassels [5] and Uchiyama [17] determined the squares that can be written as sums of three consecutive cubes. Stroeker [16] determined all squares that are expressible as the sum of \( 2 \leq d \leq 50 \) consecutive cubes, using a method based on linear forms in elliptic logarithms. More recently, Bennett, Patel and Siksek [2] determined all perfect powers that are expressible as sums of \( 2 \leq d \leq 50 \) consecutive cubes, using linear forms in logarithms, sieving and Frey curves. There has been some interest in powers that are sums of \( k \)-th powers for other exponents \( k \). For example, the solutions to the equation

\[
x^k + (x + 1)^k + (x + 2)^k = y^n, \quad x, y, n \in \mathbb{Z}, \quad n \geq 2,
\]

have been determined by Zhongfeng Zhang [18] for \( k = 2, 3, 4 \) and by Bennett, Patel and Siksek [1] for \( k = 5, 6 \), and similar problems are considered by Soydan [15].

In view of the above, it is natural to consider the equation

\[
x^k + (x + 1)^k + \cdots + (x + d - 1)^k = y^n, \quad x, y, n \in \mathbb{Z}, \quad n \geq 2
\]

(1)

with \( k, d \geq 2 \). This was studied by Zhang and Bai [19] for \( k = 2 \). They show that if \( q \) is a prime \( \equiv \pm 5 \pmod{12} \) and \( \nu_q(d) = 1 \) then Eq. (1) has no solutions for \( k = 2 \); here \( \nu_q(d) \) denotes the \( q \)-adic valuation of \( d \). It follows from a standard result in analytic number
theory (as we shall see later) that the set of $d$ for which there is a solution with $k = 2$ has natural density 0. We prove the following generalization to all even exponents $k$.

**Theorem 1** Let $k \geq 2$ be even and let $r$ be a non-zero integer. Write $A_{k,r}$ for the set of integers $d \geq 2$ such that the equation

$$x^k + (x + r)^k + \cdots + (x + (d - 1)r)^k = y^n, \quad x, y, n \in \mathbb{Z}, \quad n \geq 2,$$

has a solution $(x, y, n)$. Then $A_{k,r}$ has natural density 0; by this we mean

$$\lim_{X \to \infty} \frac{\# \{d \in A_{k,r} : d \leq X\}}{X} = 0.$$

If $k$ is odd, then $A_{k,r}$ contains all of the odd $d$; we can take $(x, y, n) = (r(1 - d)/2, 0, n)$. Thus the conclusion of the theorem does not hold for odd $k$.

**2 Some properties of Bernoulli numbers and polynomials**

In this section we summarise some classical properties of Bernoulli numbers and polynomials. These are found in many references, including [8]. The Bernoulli numbers $B_k$ are defined via the expansion

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}.$$

The first few Bernoulli numbers are

$$B_0 = 1, \quad B_1 = -1/2, \quad B_2 = 1/6, \quad B_3 = 0, \quad B_4 = -1/30, \quad B_5 = 0, \quad B_6 = 1/42.$$

It is easy to show that $B_{2k+1} = 0$ for all $k \geq 1$. The $B_k$ are rational numbers, and the von Staudt–Clausen theorem asserts that for $k \geq 2$ even

$$B_k + \sum_{(p-1) | k} \frac{1}{p} \in \mathbb{Z},$$

where the sum ranges over primes $p$ such that $(p - 1) \mid k$.

The $k$-th Bernoulli polynomial can be defined by

$$B_k(x) = \sum_{m=0}^{k} \binom{k}{m} B_m x^{k-m}.$$  \hfill (3)

Thus it is a monic polynomial with rational coefficients, and all primes appearing in the denominators are bounded by $k + 1$. It satisfies the symmetry

$$B_k(1 - x) = (-1)^k B_k(x),$$  \hfill (4)

the identity

$$B_k(x + 1) - B_k(x) = kx^{k-1},$$  \hfill (5)

and the recurrence

$$B'_k(x) = kB_{k-1}(x).$$  \hfill (6)

Whilst all the above results have been known since at least the nineteenth century, we also make use of the following far more recent and difficult theorem due to Brillhart [3] and Dilcher [9].
**Theorem 2** (Brillhart and Dilcher) The Bernoulli polynomials are squarefree.

**Relation to sums of consecutive like powers**

**Lemma 2.1** Let \( r \) be a non-zero integer and \( k, d \geq 1 \). Then

\[
x^k + (x + r)^k + \cdots + (x + r(d - 1))^k = \frac{r^k}{k+1} \left( B_{k+1} \left( \frac{x}{r} + d \right) - B_{k+1} \left( \frac{x}{r} \right) \right).
\]

This formula can be found in ([8] Section 24.4), but is easily deduced from the identity (5).

**Lemma 2.2** Let \( q \geq k + 3 \) be a prime. Let \( a, r, d \) be integers with \( d \geq 2 \), and \( r \neq 0 \). Suppose \( q \mid d \) and \( q \nmid r \). Then

\[
a^k + (a + r)^k + \cdots + (a + r(d - 1))^k \equiv r^k \cdot d \cdot B_k(a/r) \pmod{q^2}.
\]

**Proof** By Taylor’s Theorem

\[
B_{k+1}(x + d) = B_{k+1}(x) + d \cdot B'_{k+1}(x) + \frac{d^2}{2} B''_{k+1}(x) + \cdots + \frac{d^{k+2}}{(k+2)!} B^{(k+2)}_{k+1}(x).
\]

It follows from the assumption \( q \geq k + 3 \) that the coefficients of \( B_{k+1}(x) \) are \( q \)-adic integers. Thus the coefficients of the polynomials \( B^{(i)}_{k+1}(x)/i! \) are also \( q \)-adic integers. As \( q \mid d \) and \( q \nmid r \) we have

\[
B_{k+1} \left( \frac{d}{r} + d \right) - B_{k+1} \left( \frac{d}{r} \right) \equiv d \cdot B'_{k+1}(a/r) \pmod{q^2}.
\]

The lemma follows from (6) and Lemma 2.1. \( \square \)

**Lemma 2.3** Let \( k, r \) be integers with \( k \geq 2 \) and \( r \neq 0 \). Let \( q \geq k + 3 \) be a prime not dividing \( r \) such that the congruence \( B_k(x) \equiv 0 \pmod{q} \) has no solutions. Let \( d \) be a positive integer such that \( \nu_q(d) = 1 \). Then Eq. (2) has no solutions (i.e. \( d \not\in A_{k,r} \)).

**Proof** Suppose \( (x, y, n) = (a, b, n) \) is a solution to (2). By Lemma 2.2,

\[
r^k \cdot d \cdot B_k(a/r) \equiv b^n \pmod{q^2}.
\]

However, the hypotheses of the lemma ensure that the left-hand side has \( q \)-adic valuation 1. Thus \( \nu_q(b^n) = 1 \) giving a contradiction. \( \square \)

**Remarks**

- For \( k \geq 3 \) odd, the \( k \)-th Bernoulli polynomial has known rational roots 0, 1/2, 1. Thus the criterion in the lemma fails to hold for all primes \( q \). For even \( k \geq 2 \) we shall show that there is a positive density of primes \( q \) such that \( B_k(x) \) has no roots modulo \( q \).

- The second Bernoulli polynomial is \( B_2(x) = x^2 - x + 1/6 \). By quadratic reciprocity, this has a root modulo \( q \mid 6 \) if and only if \( q \equiv \pm1 \pmod{12} \). We thus recover the result of Bai and Zhang mentioned in the introduction: if \( q \equiv \pm5 \pmod{12} \) and \( \nu_q(d) = 1 \) then (1) has no solutions with \( k = 2 \).

### 3 A Galois property of even Bernoulli polynomials

**Proposition 3.1** Let \( k \geq 2 \) be even, and let \( G_k \) be the Galois group of the Bernoulli polynomial \( B_k(x) \). Then there is an element \( \mu \in G_k \) that acts freely on the roots of \( B_k(x) \).

There is a long-standing conjecture that the even Bernoulli polynomials are irreducible; see for example [3, 4, 14]. One can easily deduce Proposition 3.1 from this conjecture. We
give an unconditional proof of Proposition 3.1 in Sect. 5. As noted previously, if \( k \) is odd, then \( B_k(x) \) has rational roots 0, 1/2, 1, so the conclusion of the proposition certainly fails for odd \( k \).

**A density result**

Let \( A \) be a set of positive integers. For \( X \) positive, define

\[
A(X) = \#\{ d \in A : d \leq X \}.
\]

The *natural density* of \( A \) is defined as the limit (if it exists)

\[
\delta(A) = \lim_{X \to \infty} \frac{A(X)}{X}.
\]

For a given prime \( q \), define

\[
A^{(q)} = \{ d \in A : \nu_q(d) = 1 \}.
\]

We shall need the following result of Niven ([13] Corollary 1).

**Theorem 3** (Niven) Let \( \{ q_i \} \) be a set of primes such that \( \delta(A^{(q_i)}) = 0 \) and \( \sum q_i^{-1} = \infty \). Then \( \delta(A) = 0 \).

**Proposition 3.1 implies Theorem 1**

We now suppose Proposition 3.1 and use it to deduce Theorem 1. Let \( k \geq 2 \) be an even integer. Write \( G_k \) for the Galois group of the Bernoulli polynomial \( B_k(x) \). Let \( \mu \in G_k \) be the element acting freely on the roots of \( B_k(x) \) whose existence is asserted by Proposition 3.1.

By the Chebotarev density theorem ([6] Chapter VIII) there is a set of primes \( \{ q_i \}_{i=1}^{\infty} \) having positive Dirichlet density such that for each \( q = q_i \), the Frobenius element \( \text{Frob}_q \in G_k \) is conjugate to \( \mu \). We omit from \( \{ q_i \} \) (without affecting the density) the following:

- primes \( q \leq k + 2 \); 
- primes \( q \) dividing \( r \); 
- primes \( q \) dividing the numerator of the discriminant of \( B_k(x) \) (which is non-zero by Theorem 2).

As \( \mu \) acts freely on the roots of \( B_k(x) \), it follows that the polynomial \( B_k(x) \) has no roots modulo any of the \( q_i \). Now let \( A = A_{k,r} \) be as in the statement of Theorem 1. By Lemma 2.3, if \( \nu_{q_i}(d) = 1 \) then \( d \not\in A \). It follows that \( A^{(q_i)} = \emptyset \). By Theorem 3, we have \( \delta(A) = 0 \) as required.

**4 The 2-adic Newton polygons of even Bernoulli polynomials**

**Lemma 4.1** Let \( k \geq 2 \) be even and write \( k = 2^t \) where \( t \) is odd and \( s \geq 1 \). The 2-adic Newton polygon of \( B_k(x) \) consists two segments:

- (i) a horizontal segment joining the points \( (0, -1) \) and \( (k - 2^s, -1) \); 
- (ii) a segment joining the points \( (k - 2^s, -1) \) and \( (k, 0) \) of slope \( 1/2^s \).

**Proof** Consider the definition of \( B_k(x) \) in (3). We know that \( B_0 = 1, B_1 = -1/2 \) and \( B_m = 0 \) for all odd \( m \geq 3 \). From the von Staudt–Clausen theorem, we know that \( \nu_2(B_m) = -1 \) for even \( m \geq 2 \). It follows that the Newton polygon is bounded below by the Horizontal line \( y = -1 \).
We shall need to make use of the following result of Kummer (see [11]): if \( p \) is a prime, and \( u, v \) are positive integers then
\[
\binom{u}{v} \equiv \binom{u_0}{v_0} \binom{u_1}{v_1} \pmod{p},
\]
where \( u_0, u_1 \) are respectively the remainder and quotient on dividing \( u \) by \( p \), and likewise \( v_0, v_1 \) are respectively the remainder and quotient on dividing \( v \) by \( p \). Here we adopt the convention \( \binom{r}{s} = 0 \) if \( r < s \). Applying this with \( p = 2 \) we see that
\[
\binom{k}{2^s} \equiv \binom{2^{2t}}{2^t} \equiv \binom{t}{1} \equiv t \equiv 1 \pmod{2}.
\]
Thus the coefficient of \( x^{k-2^s} \) in \( B_k(x) \) has 2-adic valuation \(-1\). Since the constant coefficient of \( B_k(x) \) also has valuation \(-1\), we obtain the segment (i) as part of the Newton polygon.

We also see that for \( 0 < v < 2^s \),
\[
\binom{k}{v} \equiv 0 \pmod{2},
\]
and so the valuation of the coefficient of \( x^{k-v} \) is \( \geq 0 \). Finally the coefficient of \( x^k \) is \( B_0 = 1 \) and so has valuation 0. This gives segment (ii) and completes the proof.

**Remarks** Inkeri [12] showed that \( B_k(x) \) has no rational roots for \( k \) even. His proof required very precise (and difficult) estimates for the real roots of \( B_k(x) \). Lemma 4.1 allows us to give a much simpler proof of the following stronger result.

**Theorem 4** Let \( k \) be even. Then \( B_k(x) \) has no roots in \( \mathbb{Q}_2 \).

**Proof** Indeed, suppose \( \alpha \in \mathbb{Q}_2 \) is a root of \( B_k(x) \). From the slopes of the Newton polygon segments we see that \( \nu_2(\alpha) = 0 \) or \(-1/2^s\). As \( \nu_2 \) takes only integer values on \( \mathbb{Q}_2 \), we see that \( \nu_2(\alpha) = 0 \) and so \( \alpha \in \mathbb{Z}_2 \). Let \( f(x) = 2B_k(x) \in \mathbb{Z}_2[x] \). Thus \( f(\alpha) = 0 \) and so \( f(\overline{\alpha}) = \overline{0} \in \mathbb{F}_2 \). However, \( \overline{\alpha} \in \mathbb{F}_2 = \{\overline{0}, \overline{1}\} \). Now \( f(\overline{0}) = (2B_k) = \overline{1} \), and from (4) we know that \( f(\overline{1}) = f(\overline{0}) = \overline{1} \). This gives a contradiction.

Although Theorem 4 is not needed by us, its proof helps motivate part of the proof of Proposition 3.1.

## 5 Completing the proof of Theorem 1

### A little group theory

**Lemma 5.1** Let \( H \) be a finite group acting transitively on a finite set \( \{\beta_1, \ldots, \beta_n\} \). Let \( H_i \subseteq H \) be the stabilizer of \( \beta_i \), and suppose \( H_1 = H_2 \). Let \( \pi : H \rightarrow C \) be a surjective homomorphism from \( H \) onto a cyclic group \( C \). Then there is some \( \mu \in H \) acting freely on \( \{\beta_1, \ldots, \beta_n\} \) such that \( \pi(\mu) \) is a generator of \( C \).

**Proof** Let \( m = \#C \) and write \( C = \langle \sigma \rangle \). Consider the subset
\[
C' = \{\sigma^r \mid \gcd(r, m) = 1\};
\]
this is the set of elements that are cyclic generators of \( C \), and has cardinality \( \varphi(m) \), where \( \varphi \) is the Euler totient function. As \( \pi \) is surjective we see that
\[
\#\pi^{-1}(C') = \frac{\varphi(m)}{m} \cdot \#H.
\]
As $H$ acts transitively on the $\beta_i$, the stabilizers $H_i$ are conjugate and so have the same image $\pi(H_i)$ in $C$. If this image is a proper subgroup of $C$, then take $\mu$ to be any preimage of $\sigma$. Thus $\pi(\mu) = \sigma$ is a generator of $C$, and moreover, $\mu$ does not belong to any of the stabilizers $H_i$ and so acts freely on $\{\beta_1, \ldots, \beta_n\}$, completing the proof in this case. Thus we suppose that $\pi(H_i) = C$ for all $i$. It follows that

$$\#\pi^{-1}(C') \cap H_i = \frac{\phi(m)}{m} \cdot \#H_i = \frac{\phi(m)}{m} \cdot \#H,$$

where the second equality follows from the Orbit-Stabilizer Theorem. The lemma states that there is some element $\mu$ belonging to $\pi^{-1}(C')$ but not to $\cup H_i$. Suppose otherwise. Then

$$\pi^{-1}(C') \subseteq \bigcup_{i=1}^n H_i,$$

and therefore

$$\pi^{-1}(C') = \bigcup_{i=1}^n \pi^{-1}(C') \cap H_i. \quad (9)$$

Now (7), (8) and (9) together imply that the $\pi^{-1}(C') \cap H_i$ are pairwise disjoint. This contradicts the hypothesis that $H_1 = H_2$ completing the proof.

Proof of Proposition 3.1 We now complete the proof of Theorem 1 by proving Proposition 3.1. Fix an even $k \geq 2$, and let $L$ be the splitting field of $B_k(x)$. Let $G_k = \text{Gal}(L/\mathbb{Q}) = \text{Gal}(B_k(x))$ be the Galois group of $B_k(x)$. Let $\wp$ be a prime of $L$ above $2$. The $2$-adic valuation $v_2$ on $\mathbb{Q}_2$ has a unique extension to $L_\wp$ which we continue to denote by $v_2$. We let $H = \text{Gal}(L_\wp/\mathbb{Q}_2) \subseteq G_k$ be the decomposition subgroup corresponding to $\wp$.

From Lemma 4.1 we see that $B_k(x)$ factors as $B_k(x) = g(x)h(x)$ over $\mathbb{Q}_2$ where the factors $g, h$ correspond respectively to the segments (i), (ii) in the lemma. Thus $g, h$ have degree $k - 2^r$ and $2^r$ respectively. We denote the roots of $g$ by $\{\alpha_1, \ldots, \alpha_{k-2^r}\} \subset L_\wp$ and the roots of $h$ by $\{\beta_1, \ldots, \beta_{2^r}\} \subset L_\wp$. From the slopes of the segments we see that $v_2(\alpha_i) = 0$ and $v_2(\beta_j) = -1/2^r$. It clearly follows that $h$ is irreducible and therefore that $H$ acts transitively on the $\beta_j$. Moreover, from the symmetry (4) we see that $1 - \beta_1$ is a root of $B_k(x)$, and by appropriate relabelling we can suppose that $\beta_2 = 1 - \beta_1$. In the notation of Lemma 5.1, we have $H_1 = H_2$. Now let $C = \text{Gal}(\mathbb{F}_\wp/\mathbb{F}_2)$, where $\mathbb{F}_\wp$ is the residue field of $\wp$. This group is cyclic generated by the Frobenius map: $\wp \mapsto \wp^{2^n}$. We let $\pi : H \to C$ be the induced surjection. By Lemma 5.1 there is some $\mu \in H$ that acts freely on the $\beta_i$ and such that $\pi(\mu)$ generates $C$. To complete the proof of Proposition 3.1 it is enough to show that $\mu$ also acts freely on the $\alpha_i$. Suppose otherwise, and let $\alpha$ be one of the $\alpha_i$ that is fixed by $\mu$. As $v_2(\alpha) = 0$, we can write $\overline{\alpha} \in \mathbb{F}_\wp$ for the reduction of $\alpha$ modulo $\wp$. Now $\alpha$ is fixed by $\mu$, and so $\overline{\alpha} \in \mathbb{F}_\wp$ is fixed by $\langle \pi(\mu) \rangle = C$. Thus $\overline{\alpha} \in \mathbb{F}_2$ and so $\overline{\alpha} = \overline{0}$ or $\overline{1}$. Now let $f(x) = 2B_k(x) \in \mathbb{Z}_2[x]$. Thus $f(\overline{\alpha}) = \overline{0}$. But $f(\overline{0}) = (2B_k)(\overline{0}) = \overline{1}$, and from (4) we know that $f(\overline{1}) = f(\overline{0}) = \overline{1}$. This contradiction completes the proof.
Acknowledgements
The first-named author is supported by an EPSRC studentship. The second-named author is supported by the EPSRC LMF: L-Functions and Modular Forms Programme Grant EP/K034383/1.

Received: 29 July 2016  Accepted: 25 November 2016
Published online: 14 February 2017

References
1. Bennett, M.A., Patel, V., Siksek, S.: Perfect powers that are sums of consecutive cubes. Mathematika 63, 230–249 (2016)
2. Bennett, M.A., Patel, V., Siksek, S.: Superelliptic equations arising from sums of consecutive powers, Acta Arithmetica, to appear
3. Brillhart, J.: On the Euler and Bernoulli polynomials. J. Reine Angew. Math. 234, 45–64 (1969)
4. Carlitz, L.: Note on irreducibility of the Bernoulli and Euler polynomial. Duke Math. J. 19, 475–481 (1952)
5. Cassels, J.W.S.: A Diophantine equation. Glasgow Math. J. 27, 11–88 (1985)
6. Cassels, J.W.S., Frölich, A. (eds.): Algebraic Number Theory. Academic Press, New York (1967)
7. Dickson, L.E.: History of the theory of numbers, vol. II. Chelsea, New York (1971)
8. Dilcher, K.: Chapter 24: Bernoulli and Euler polynomials, in digital library of mathematical functions: http://dlmf.nist.gov/24
9. Dilcher, K.: On multiple zeros of Bernoulli polynomials. Acta Arithmetica 134(2), 149–155 (2008)
10. Euler L.: Vollständige Anleitung zur Algebra, vol. 2, St. Petersburg (1770)
11. Granville, A.: Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers. CMS Conf. Proc. Amer. Math. Soc. 20, 253–276 (1997)
12. Inkeri, K.: The real roots of Bernoulli polynomials. Ann. Univ. Turku. Ser. A I (37), 1–20 (1959)
13. Niven, I.: The asymptotic density of sequences. Bull. Amer. Math. Soc. 57, 420–434 (1951)
14. Kimura, N.: On the degree of an irreducible factor of the Bernoulli polynomials. Acta Arith. 50, 243–249 (1988)
15. Soydan G., On the Diophantine equation \((x + 1)^k + (x + 2)^k + \cdots + (x + d)^k = y^n\), preprint (2016)
16. Stroeker, R.J.: On the sum of consecutive cubes being a square. Compositio Mathematica 97, 295–307 (1995)
17. Uchiyama, S.: On a Diophantine equation. Proc. Japan Acad. Ser. A Math. Sci. 55(9), 367–369 (1979)
18. Zhang, Z.: On the Diophantine equation \((x − 1)^k + x^k + (x + 1)^k = y^n\). Publ. Math. Debrecen 85, 93–100 (2014)
19. Zhang, Z., Bai, M.: On the Diophantine equation \((x + 1)^k + (x + 2)^k + \cdots + (x + d)^k = y^n\). Funct. Approx. Comment. Math. 49, 73–77 (2013)