Sums of Consecutive Perfect Powers is Seldom a Perfect Power

Vandita Patel
University of Warwick

Journées Algophantiennes Bordelaises 2017,
Université de Bordeaux

June 7, 2017
A Diophantine Equation

\[ x^k + (x + 1)^k + \cdots + (x + d - 1)^k = y^n. \]

**Question**

*Fix \( k \geq 2 \) and \( d \geq 2 \). Determine all of the integer solutions \((x, y, n)\), \( n \geq 2 \).*
A Brief History

Theorem (Zhang and Bai, 2013)

Let $q$ be a prime such that $q \equiv 5, 7 \pmod{12}$. Suppose $q \parallel d$. Then the equation $x^2 + (x+1)^2 + \ldots + (x+d-1)^2 = y^n$ has no integer solutions.

Corollary (Use Dirichlet’s Theorem)

Let $A_2$ be the set of integers $d \geq 2$ such that the equation

$$x^2 + (x+1)^2 + \ldots + (x+d-1)^2 = y^n$$

has a solution $(x,y,n)$. Then $A_2$ has natural density zero.
**A Brief History**

---

**Theorem (Zhang and Bai, 2013)**

Let \( q \) be a prime such that \( q \equiv 5, 7 \pmod{12} \). Suppose \( q \parallel d \). Then the equation \( x^2 + (x + 1)^2 + \cdots + (x + d - 1)^2 = y^n \) has no integer solutions.

---

**Corollary (Use Dirichlet’s Theorem)**

Let \( A_2 \) be the set of integers \( d \geq 2 \) such that the equation

\[
x^2 + (x + 1)^2 + \cdots + (x + d - 1)^2 = y^n
\]

has a solution \((x, y, n)\). Then \( A_2 \) has natural density zero.

---

Vandita Patel

University of Warwick

Sums of Consecutive Perfect Powers is Seldom a Perfect Power
The Result

**Theorem (V. Patel, S. Siksek)**

Let \( k \geq 2 \) be an even integer. Let \( A_k \) be the set of integers \( d \geq 2 \) such that the equation

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

has a solution \((x, y, n)\). Then \( A_k \) has natural density zero. In other words we have

\[
\lim_{X \to \infty} \frac{\#\{d \in A_k : d \leq X\}}{X} = 0.
\]
The Result

Theorem (V. Patel, S. Siksek)

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

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

has a solution $(x, y, n)$. Then $A_{k,r}$ has natural density zero. In other words we have

$$\lim_{X \to \infty} \frac{\#\{d \in A_{k,r} : d \leq X\}}{X} = 0.$$
BERNOULLI POLYNOMIALS AND RELATION TO SUMS OF CONSECUTIVE POWERS

**Definition (Bernoulli Numbers, \( b_k \))**

\[
\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} b_k \frac{x^k}{k!}.
\]

\( b_0 = 1, b_1 = -1/2, b_2 = 1/6, b_3 = 0, b_4 = -1/30, b_5 = 0, b_6 = 1/42. \)

**Lemma**

\( b_{2k+1} = 0 \) for \( k \geq 1. \)
Bernoulli polynomials and relation to sums of consecutive powers

Definition (Bernoulli Polynomial, $B_k$)

$$B_k(x) := \sum_{m=0}^{k} \binom{k}{m} b_m x^{k-m}.$$  

Lemma

$$x^k + (x+1)^k + \cdots + (x+d-1)^k = \frac{1}{k+1} (B_{k+1}(x+d) - B_k(x)).$$
**Bernoulli polynomials and relation to sums of consecutive powers**

**Definition (Bernoulli Polynomial, $B_k$)**

$$B_k(x) := \sum_{m=0}^{k} \binom{k}{m} b_m x^{k-m}.$$  

**Lemma**

$$x^k + (x+1)^k + \cdots + (x+d-1)^k = \frac{1}{k+1} \left( B_{k+1}(x + d) - B_k(x) \right).$$
BERNOULLI POLYNOMIALS AND RELATION TO SUMS OF CONSEQUENTIAL POWERS

**Lemma**

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

Apply Taylor’s Theorem and use \( B'_{k+1}(x) = (k + 1) \cdot B_k(x) \).

**Lemma**

Let \( q \geq k + 3 \) be a prime. Let \( d \geq 2 \). Suppose that \( q \mid d \). Then

\[ x^k + (x + 1)^k + \cdots + (x + d - 1)^k \equiv d \cdot B_k(x) \pmod{q^2}. \]
Bernoulli polynomials and relation to sums of consecutive powers

**Lemma**

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

Apply Taylor’s Theorem and use \( B'_{k+1}(x) = (k + 1) \cdot B_k(x) \).

**Lemma**

Let \( q \geq k + 3 \) be a prime. Let \( d \geq 2 \). Suppose that \( q \mid d \). Then

\[
x^k + (x + 1)^k + \cdots + (x + d - 1)^k \equiv d \cdot B_k(x) \pmod{q^2}.
\]
BERNOULLI POLYNOMIALS AND RELATION TO SUMS OF CONSECUTIVE POWERS

\[ x^k + (x + 1)^k + \cdots + (x + d - 1)^k = y^n. \]

**Proposition (Criterion)**

Let \( k \geq 2 \). Let \( q \geq k + 3 \) be a prime such that the congruence \( B_k(x) \equiv 0 \pmod{q} \) has no solutions. Let \( d \) be a positive integer such that \( \text{ord}_q(d) = 1 \). Then the equation has no solutions. (i.e. \( d \notin A_k \)).

**Remark:** Computationally we checked \( k \leq 75,000 \) and we could always find such a \( q \).
Bernoulli polynomials and relation to sums of consecutive powers

\[ x^k + (x + 1)^k + \cdots + (x + d - 1)^k = y^n. \]

**Proposition (Criterion)**

Let \( k \geq 2 \). Let \( q \geq k + 3 \) be a prime such that the congruence \( B_k(x) \equiv 0 \pmod{q} \) has no solutions. Let \( d \) be a positive integer such that \( \text{ord}_q(d) = 1 \). Then the equation has no solutions. (i.e. \( d \notin A_k \)).

**Remark:** Computationally we checked \( k \leq 75,000 \) and we could always find such a \( q \).
We need to use Chebotarev’s density theorem, which can be seen as “a generalisation of Dirichlet’s theorem” on primes in arithmetic progression.

**Proposition**

Let \( k \geq 2 \) be even and let \( G \) be the Galois group of \( B_k(x) \). Then there is an element \( \mu \in G \) that acts freely on the roots of \( B_k(x) \).

Assuming the proposition, we may then use Chebotarev’s density theorem to find a set of primes \( q_i \) with positive Dirichlet density such that \( \text{Frob}_{q_i} \in G \) is conjugate to \( \mu \). Then we can apply Niven’s results to deduce our Theorem.
Relation to Densities?

We need to use Chebotarev’s density theorem, which can be seen as “a generalisation of Dirichlet’s theorem” on primes in arithmetic progression.

**Proposition**

Let \( k \geq 2 \) be even and let \( G \) be the Galois group of \( B_k(x) \). Then there is an element \( \mu \in G \) that acts freely on the roots of \( B_k(x) \).

Assuming the proposition, we may then use Chebotarev’s density theorem to find a set of primes \( q_i \) with positive Dirichlet density such that \( \text{Frob}_{q_i} \in G \) is conjugate to \( \mu \). Then we can apply Niven’s results to deduce our Theorem.
Niven’s Results (Flash!)

The setup:

1. Let \( A \) be a set of positive integers.
2. Define: \( A(X) = \#\{d \in A : d \leq X\} \) for positive \( X \).
3. Natural Density: \( \delta(A) = \lim_{X \to \infty} \frac{A(X)}{X} \).
4. Given a prime \( q \), define: \( A^{(q)} = \{d \in A : \operatorname{ord}_q(d) = 1\} \).

Theorem (Niven)

Let \( \{q_i\} \) be a set of primes such that \( \delta(A^{(q_i)}) = 0 \) and \( \sum q_i^{-1} = \infty \). Then \( \delta(A) = 0 \).
A Legendre Symbol analogue

**Proposition**

Let $k \geq 2$ be even and let $G$ be the Galois group $B_k(x)$. Then there is an element $\mu \in G$ that acts freely on the roots of $B_k(x)$.

**Conjecture**

For any even integer $k$, $B_k(x)$ is irreducible over $\mathbb{Q}$.

**Remark:** The conjecture implies the Proposition. This then proves our Theorem.
A Legendre Symbol analogue

**Proposition**

Let $k \geq 2$ be even and let $G$ be the Galois group $B_k(x)$. Then there is an element $\mu \in G$ that acts freely on the roots of $B_k(x)$.

**Conjecture**

For any even integer $k$, $B_k(x)$ is irreducible over $\mathbb{Q}$.

**Remark:** The conjecture implies the Proposition. This then proves our Theorem.
Tough Stuff

A sketch of an unconditional proof!

**Proposition**

Let $k \geq 2$ be even and let $G$ be the Galois group $B_k(x)$. Then there is an element $\mu \in G$ that acts freely on the roots of $B_k(x)$.

**Theorem (von Staudt-Clausen)**

Let $n \geq 2$ be even. Then

$$b_n + \sum_{(p-1)|n} \frac{1}{p} \in \mathbb{Z}.$$
2 is the Oddest Prime

The Newton Polygon of $B_k(x)$ for $k = 2^s \cdot t$, $s \geq 1$.

$$B_k(x) = \sum_{i=0}^{k} \binom{k}{k-i} b_{k-i} x^i = \sum_{i=0}^{k} a_i x^i$$
Another nice result

1. Sloping part corresponds to irreducible factor over $\mathbb{Q}_2$.
2. Root in $\mathbb{Q}_2$ must have valuation zero.
3. Root belongs to $\mathbb{Z}_2$ and is odd.
4. Symmetry $(-1)^k B_k(x) = B_k(1-x)$ gives a contradiction.

Theorem (V. Patel, S. Siksek)

Let $k \geq 2$ be an even integer. Then $B_k(x)$ has no roots in $\mathbb{Q}_2$.

Theorem (K. Inkeri, 1959)

Let $k \geq 2$ be an even integer. Then $B_k(x)$ has no roots in $\mathbb{Q}$.
Another nice result

1. Sloping part corresponds to irreducible factor over $\mathbb{Q}_2$.
2. Root in $\mathbb{Q}_2$ must have valuation zero.
3. Root belongs to $\mathbb{Z}_2$ and is odd.
4. Symmetry $(-1)^kB_k(x) = B_k(1 - x)$ gives a contradiction.

Theorem (V. Patel, S. Siksek)

Let $k \geq 2$ be an even integer. Then $B_k(x)$ has no roots in $\mathbb{Q}_2$.

Theorem (K. Inkeri, 1959)

Let $k \geq 2$ be an even integer. Then $B_k(x)$ has no roots in $\mathbb{Q}$.
Another nice result

1. Sloping part corresponds to irreducible factor over $\mathbb{Q}_2$.
2. Root in $\mathbb{Q}_2$ must have valuation zero.
3. Root belongs to $\mathbb{Z}_2$ and is odd.
4. Symmetry $(-1)^k B_k(x) = B_k(1-x)$ gives a contradiction.

**Theorem (V. Patel, S. Siksek)**

Let $k \geq 2$ be an even integer. Then $B_k(x)$ has no roots in $\mathbb{Q}_2$.

**Theorem (K. Inkeri, 1959)**

Let $k \geq 2$ be an even integer. Then $B_k(x)$ has no roots in $\mathbb{Q}$.
**WHAT IS GOING ON?**

\[ L = \text{Splitting Field of } B_k(x) \quad L_{\mathbb{F}_p} \quad \mathbb{F}_2 \]

\[ G = \text{Galois Group} \quad H \subset G \quad C = \text{Cyclic} \]

\[ \mathbb{Q} \quad \mathbb{Q}_2 \quad \mathbb{F}_2 = \text{Residue Field} \]
What is Going On?

\[ L = \text{Splitting Field of } B_k(x) \]
\[ L_{\wp} \]
\[ \mathbb{F}_{\wp} \]

\[ G = \text{Galois Group} \]
\[ H \subset G \]
\[ C = \text{Cyclic} \]

\[ \mathbb{Q} \]
\[ \mathbb{Q}_2 \]
\[ \mathbb{F}_2 = \text{Residue Field} \]

\[ \mu \text{ lives here!} \]
A sketch proof of the Proposition

The Setup:

- $k \geq 2$ is even.
- $L$ is the splitting field of $B_k(x)$.
- $G$ is the Galois group of $B_k(x)$.
- $\mathfrak{P}$ be a prime above 2.
- $\nu_2$ on $\mathbb{Q}_2$ which we extend uniquely to $L_{\mathfrak{P}}$ (also call it $\nu_2$).
- $H = \text{Gal}(L_{\mathfrak{P}}/\mathbb{Q}_2) \subset G$ be the decomposition subgroup corresponding to $\mathfrak{P}$. 
A sketch proof of the Proposition

\[ B_k(x) = g(x)h(x) \]

where \( g(x) \) has degree \( k - 2^s \). Label the roots \( \{ \alpha_1, \ldots, \alpha_{k-2^s} \} \), and \( h(x) \) has degree \( 2^s \). Label the roots \( \{ \beta_1, \ldots, \beta_{2^s} \} \).

- All roots \( \subset L_\beta \).
- \( h(x) \) is irreducible.
- Therefore \( H \) acts transitively on \( \beta_j \).
- Pick \( \mu \in H \) such that \( \mu \) acts freely on the roots of \( h(x) \).
- Check it doesn’t end up fixing a root of \( g(x) \).
“Bad Prime = Extremely Useful Prime!”

The Newton Polygon of $B_k(x)$ for $k = 2^s \cdot t$, $s \geq 1$.

The Newton Polygon of $B_k(x)$ for $k = 2^s \cdot t$, $s \geq 1$. 

\[ \nu_2(a_i) \]

$(0, 0)$  $(k - 2^s, 0)$  $(k, 0)$

$(0, -1)$  $(k - 2^s, -1)$

\[ \text{slope} = \frac{1}{2^s} \]
Finding $\mu$

**Lemma**

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

1. Let $F_\mathfrak{P}$ be the residue field of $\mathfrak{P}$.
2. Let $C = \text{Gal}(F_\mathfrak{P}/F_2)$.
3. $C$ is cyclic generated by the Frobenius map: $\bar{\gamma} \to \bar{\gamma}^2$.
4. Let $\pi : H \to C$ be the induced surjection.
5. Finally use the Lemma.
**Finding \( \mu \)**

**Lemma**

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

1. Let \( \mathbb{F}_p \) be the residue field of \( \mathfrak{P} \).
2. Let \( C = \text{Gal}(\mathbb{F}_p/\mathbb{F}_2) \).
3. \( C \) is cyclic generated by the Frobenius map: \( \bar{\gamma} \to \bar{\gamma}^2 \).
4. Let \( \pi : H \to C \) be the induced surjection.
5. Finally use the Lemma.
**Check** $g(x)$

\[ B_k(x) = g(x)h(x) \]

where $g(x)$ has degree $k - 2^s$. Label the roots \( \{\alpha_1, \ldots, \alpha_{k-2^s}\} \), and $h(x)$ has degree $2^s$. Label the roots \( \{\beta_1, \ldots, \beta_{2^s}\} \).

**Lemma**

\( \mu \) acts freely on the \( \alpha_i \).

1. Suppose not. Let \( \alpha \) be a root that is fixed by \( \mu \).
2. \( \nu_2(\alpha) = 0 \) so let \( \bar{\alpha} = \alpha \pmod{\mathfrak{P}} \), \( \bar{\alpha} \in \mathbb{F}_\mathfrak{P} \).
3. \( \alpha \) fixed by \( \mu \) hence \( \bar{\alpha} \) fixed by \( \langle \pi(\mu) \rangle = C \).
4. Hence \( \bar{\alpha} \in \mathbb{F}_2 \). \( f(x) = 2B_k(x) \in \mathbb{Z}_2[x] \).
5. \( f(\bar{1}) = f(\bar{0}) = \bar{1} \). A contradiction!
Thank you for Listening!
Solving the equations for $k = 2$

$$d \left( \left( x + \frac{d + 1}{2} \right)^2 + \frac{(d - 1)(d + 1)}{12} \right) = y^p.$$ 

$$X^2 + C \cdot 1^p = \left(\frac{1}{d}\right)y^p$$
# Solving the Equations for $k = 2$

<table>
<thead>
<tr>
<th>$d$</th>
<th>Equation</th>
<th>Level</th>
<th>Dimension</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>$2y^p - 5 \times 7 = 3(x+7)^2$</td>
<td>$2^7 \times 3^2 \times 5 \times 7$</td>
<td>480</td>
</tr>
<tr>
<td>11</td>
<td>$11^{p-1}y^p - 2 \times 5 = (x+6)^2$</td>
<td>$2^7 \times 5 \times 11$</td>
<td>160</td>
</tr>
<tr>
<td>13</td>
<td>$13^{p-1}y^p - 2 \times 7 = (x+7)^2$</td>
<td>$2^7 \times 7 \times 13$</td>
<td>288</td>
</tr>
<tr>
<td>22</td>
<td>$2 \times 11^{p-1}y^p - 7 \times 23 = (2x+23)^2$</td>
<td>$2^7 \times 7 \times 11 \times 23$</td>
<td>5,280</td>
</tr>
<tr>
<td>23</td>
<td>$23^{p-1}y^p - 2^2 \times 11 = (x+12)^2$</td>
<td>$2^3 \times 11 \times 23$</td>
<td>54</td>
</tr>
<tr>
<td>26</td>
<td>$2 \times 13^{p-1}y^p - 3^2 \times 5^2 = (2x+27)^2$</td>
<td>$2^7 \times 3 \times 5 \times 13$</td>
<td>384</td>
</tr>
<tr>
<td>33</td>
<td>$11^{p-1}y^p - 2^4 \times 17 = 3(x+17)^2$</td>
<td>$2^3 \times 3^2 \times 11 \times 17$</td>
<td>200</td>
</tr>
<tr>
<td>37</td>
<td>$37^{p-1}y^p - 2 \times 3 \times 19 = (x+19)^2$</td>
<td>$2^7 \times 3 \times 19 \times 37$</td>
<td>5,184</td>
</tr>
<tr>
<td>39</td>
<td>$13^{p-1}y^p - 2^2 \times 5 \times 19 = 3(x+20)^2$</td>
<td>$2^3 \times 3^2 \times 5 \times 13 \times 19$</td>
<td>1,080</td>
</tr>
<tr>
<td>46</td>
<td>$2 \times 23^{p-1}y^p - 3^2 \times 5 \times 47 = (2x+47)^2$</td>
<td>$2^7 \times 3 \times 5 \times 23 \times 47$</td>
<td>32,384</td>
</tr>
<tr>
<td>47</td>
<td>$47^{p-1}y^p - 2^3 \times 23 = (x+24)^2$</td>
<td>$2^5 \times 23 \times 47$</td>
<td>1,012</td>
</tr>
<tr>
<td>59</td>
<td>$59^{p-1}y^p - 2 \times 5 \times 29 = (x+30)^2$</td>
<td>$2^7 \times 5 \times 29 \times 59$</td>
<td>25,984</td>
</tr>
</tbody>
</table>
## Solving the Equations for $k = 4$

<table>
<thead>
<tr>
<th>$d$</th>
<th>Equation</th>
<th>Level</th>
<th>Dimension</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>$y^p + 2 \times 73 = 5(X)^2$</td>
<td>$2^7 \times 5^2 \times 73$</td>
<td>5,472</td>
</tr>
<tr>
<td>6</td>
<td>$y^p + 7 \times 53 = 6(X)^2$</td>
<td>$2^8 \times 3^2 \times 7 \times 53$</td>
<td>12,480</td>
</tr>
<tr>
<td>7</td>
<td>$7^{p-1}y^p + 2^2 \times 29 = (X)^2$</td>
<td>$2^3 \times 7 \times 29$</td>
<td>42</td>
</tr>
<tr>
<td>10</td>
<td>$y^p + 3 \times 11 \times 149 = 10(X)^2$</td>
<td>$2^8 \times 5^2 \times 3 \times 11 \times 149$</td>
<td>449,920</td>
</tr>
<tr>
<td>13</td>
<td>$13^{p-1}y^p + 2 \times 7 \times 101 = (X)^2$</td>
<td>$2^7 \times 7 \times 13 \times 101$</td>
<td>28,800</td>
</tr>
<tr>
<td>14</td>
<td>$7^{p-1}y^p + 13 \times 293 = 2(X)^2$</td>
<td>$2^8 \times 7 \times 13 \times 293$</td>
<td>168,192</td>
</tr>
<tr>
<td>15</td>
<td>$y^p + 2^3 \times 7 \times 673 = 15(X)^2$</td>
<td>$2^5 \times 3^2 \times 5^2 \times 7 \times 673$</td>
<td>383,040</td>
</tr>
<tr>
<td>17</td>
<td>$17^{p-1}y^p + 2^3 \times 3 \times 173 = (X)^2$</td>
<td>$2^5 \times 3 \times 17 \times 173$</td>
<td>5,504</td>
</tr>
<tr>
<td>19</td>
<td>$19^{p-1}y^p + 2 \times 3 \times 23 \times 47 = (X)^2$</td>
<td>$2^7 \times 3 \times 19 \times 23 \times 47$</td>
<td>145,728</td>
</tr>
<tr>
<td>21</td>
<td>$7^{p-1}y^p + 2 \times 11 \times 1321 = 3(X)^2$</td>
<td>$2^7 \times 3^2 \times 7 \times 11 \times 1321$</td>
<td>1,584,000</td>
</tr>
<tr>
<td>26</td>
<td>$13^{p-1}y^p + 3^2 \times 5 \times 1013 = 2(X)^2$</td>
<td>$2^8 \times 3 \times 5 \times 13 \times 1013$</td>
<td>777,216</td>
</tr>
<tr>
<td>29</td>
<td>$29^{p-1}y^p + 2 \times 7 \times 2521 = (X)^2$</td>
<td>$2^7 \times 7 \times 29 \times 2521$</td>
<td>1,693,440</td>
</tr>
<tr>
<td>30</td>
<td>$y^p + 19 \times 29 \times 31 \times 71 = 30(X)^2$</td>
<td>$2^8 \times 3^2 \times 5^2 \times 19 \times 29 \times 31 \times 71$</td>
<td>804,384,000</td>
</tr>
</tbody>
</table>

Where $X$ is a quadratic in the original variable $x$. 

### References

Vandita Patel
University of Warwick

Sums of Consecutive Perfect Powers is Seldom a Perfect Power