Perfect Powers that are Sums of Consecutive k-th Powers

Vandita Patel

University of Warwick

October 26, 2016

A Diophantine Equation

$$(x+1)^k + (x+2)^k + \cdots + (x+d)^k = y^n.$$

Question

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

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).

Remark: We can let $n = p$ be a prime.

A Brief History

Euler:

$$6^3 = 3^3 + 4^3 + 5^3.$$

Dickson's *"History of the Theory of Numbers"*:

Catalan, Cunningham, Lucas and Gennochi.

Later contributions from:

1. Pagliani (1829): parametric solutions.
2. Cassels (1985): $y^2 = x^3 + (x+1)^3 + (x+2)^3$.
3. Uchiyama (1979): independently to Cassels.
4. Zhongfeng Zhang (2014): $y^p = x^3 + (x+1)^3 + (x+2)^3$.

A Brief History

Euler:

$$6^3 = 3^3 + 4^3 + 5^3.$$

Dickson's *"History of the Theory of Numbers"*:

Catalan, Cunningham, Lucas and Gennochi.

Later contributions from:

1. Pagliani (1829): parametric solutions.
2. Cassels (1985): $y^2 = x^3 + (x+1)^3 + (x+2)^3$.
3. Uchiyama (1979): independently to Cassels.
4. Zhongfeng Zhang (2014): $y^p = x^3 + (x+1)^3 + (x+2)^3$.

A Brief History

Euler:

$$6^3 = 3^3 + 4^3 + 5^3.$$

Dickson's *"History of the Theory of Numbers"*:

Catalan, Cunningham, Lucas and Gennochi.

Later contributions from:

1. Pagliani (1829): parametric solutions.
2. Cassels (1985): $y^2 = x^3 + (x+1)^3 + (x+2)^3$.
3. Uchiyama (1979): independently to Cassels.
4. Zhongfeng Zhang (2014): $y^p = x^3 + (x+1)^3 + (x+2)^3$.

A Brief History

Euler:

$$6^3 = 3^3 + 4^3 + 5^3.$$

Dickson's *"History of the Theory of Numbers"*:

Catalan, Cunningham, Lucas and Gennochi.

Later contributions from:

1. Pagliani (1829): parametric solutions.
2. Cassels (1985): $y^2 = x^3 + (x+1)^3 + (x+2)^3$.
3. Uchiyama (1979): independently to Cassels.
4. Zhongfeng Zhang (2014): $y^p = x^3 + (x+1)^3 + (x+2)^3$.

A Brief History

Euler:

$$6^3 = 3^3 + 4^3 + 5^3.$$

Dickson's *"History of the Theory of Numbers"*:

Catalan, Cunningham, Lucas and Gennochi.

Later contributions from:

1. Pagliani (1829): parametric solutions.
2. Cassels (1985): $y^2 = x^3 + (x+1)^3 + (x+2)^3$.
3. Uchiyama (1979): independently to Cassels.
4. Zhongfeng Zhang (2014): $y^p = x^3 + (x+1)^3 + (x+2)^3$.

A Brief History

Well–Known:

$$\sum_{i=0}^{d} i^3 = \sum_{i=1}^{d} i^3 = \left(\frac{d(d+1)}{2}\right)^2 .$$

Pagliani:

$$\sum_{i=1}^{v^3} \left(\frac{v^4 - 3v^3 - 2v^2 - 2}{6} + i\right)^3 = \left(\frac{v^5 + v^3 - 2v}{6}\right)^3 .$$

where $v \equiv 2, 4 \pmod 6$.

A Brief History

Well–Known:

$$\sum_{i=0}^{d} i^3 = \sum_{i=1}^{d} i^3 = \left(\frac{d(d+1)}{2}\right)^2.$$

Pagliani:

$$\sum_{i=1}^{v^3} \left(\frac{v^4 - 3v^3 - 2v^2 - 2}{6} + i\right)^3 = \left(\frac{v^5 + v^3 - 2v}{6}\right)^3.$$

where $v \equiv 2, 4 \pmod 6$.

Recent work

$$(x+1)^k + (x+2)^k + \cdots + (x+d)^k = y^n.$$

Theorem (M. A. Bennett, V. Patel, S. Siksek)

Let $k = 3$ and $2 \le d \le 50$. Then, any integer solution (x, y, n) must have $n = 2$ or $n = 3$.

$$291^3 + 292^3 + \cdots + 338^3 + 339^3 = 1155^3.$$

Recent work

$$(x+1)^k + (x+2)^k + \cdots + (x+d)^k = y^n.$$

Theorem (M. A. Bennett, V. Patel, S. Siksek)

Let $k = 3$ and $2 \leq d \leq 50$. Then, any integer solution (x, y, n) must have $n = 2$ or $n = 3$.

$$291^3 + 292^3 + \cdots + 338^3 + 339^3 = 1155^3.$$

The Result

Theorem (V. Patel, S. Siksek)

Let $k \geq 2$ be an even integer. Let $\mathcal{A}_k$ 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 $\mathcal{A}_k$ has natural density zero. In other words we have

$$\lim_{X \to \infty} \frac{\#\{d \in \mathcal{A}_k : d \leq X\}}{X} = 0.$$

The Case $k = 2$

$$(x+1)^2 + (x+2)^2 + \cdots + (x+d)^2 = y^n.$$

$$dx^2 + d(d+1)x + \frac{d(d+1)(2d+1)}{6} = y^n.$$

$$d\left(x^2 + (d+1)x + \frac{(d+1)(2d+1)}{6}\right) = y^n.$$

Idea

Let q be a prime (not 2 or 3) such that $\operatorname{ord}_q(d) = 1$. Suppose that $q \nmid x^2 + (d+1)x + (d+1)(2d+1)/6$. Then we must have $n = 1$.

The Case $k = 2$

$$(x+1)^2 + (x+2)^2 + \cdots + (x+d)^2 = y^n.$$

$$dx^2 + d(d+1)x + \frac{d(d+1)(2d+1)}{6} = y^n.$$

$$d\left(x^2 + (d+1)x + \frac{(d+1)(2d+1)}{6}\right) = y^n.$$

Idea

Let q be a prime (not 2 or 3) such that $\mathrm{ord}_q(d) = 1$. Suppose that $q \nmid x^2 + (d+1)x + (d+1)(2d+1)/6$. Then we must have $n = 1$.

The Case $k = 2$

$$(x+1)^2 + (x+2)^2 + \cdots + (x+d)^2 = y^n.$$

$$dx^2 + d(d+1)x + \frac{d(d+1)(2d+1)}{6} = y^n.$$

$$d\left(x^2 + (d+1)x + \frac{(d+1)(2d+1)}{6}\right) = y^n.$$

Idea

Let q be a prime (not 2 or 3) such that $\mathrm{ord}_q(d) = 1$. Suppose that $q \nmid x^2 + (d+1)x + (d+1)(2d+1)/6$. Then we must have $n = 1$.

The Case $k = 2$

$$(x+1)^2 + (x+2)^2 + \cdots + (x+d)^2 = y^n.$$

$$dx^2 + d(d+1)x + \frac{d(d+1)(2d+1)}{6} = y^n.$$

$$d\left(x^2 + (d+1)x + \frac{(d+1)(2d+1)}{6}\right) = y^n.$$

Idea

Let q be a prime (not 2 or 3) such that $\mathrm{ord}_q(d) = 1$. Suppose that $q \nmid x^2 + (d+1)x + (d+1)(2d+1)/6$. Then we must have $n = 1$.

The Bernoulli Polynomial!!!

Idea

Let q be a prime (not 2 or 3) such that $\mathrm{ord}_q(d) = 1$. Suppose that $q \nmid x^2 + (d+1)x + (d+1)(2d+1)/6$. Then we must have $n = 1$.

A reduction modulo q:

$$x^2 + x + 1/6 \not\equiv 0 \pmod{q}.$$

We complete the square and make a sensible change of variables.

$$Y^2 \not\equiv 12 \pmod{q}.$$

Legendre Symbols and a Density!

We want 12 to **NOT** be a square modulo q.

$$Y^2 \not\equiv 12 \pmod{q}.$$

$$\left(\frac{12}{q}\right) = \left(\frac{3}{q}\right) = -1$$

Precisely when $q \equiv 5, 7 \pmod{12}$.

Lemma

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

Legendre Symbols and a Density!

We want 12 to **NOT** be a square modulo q.

$$Y^2 \not\equiv 12 \pmod{q}.$$

$$\left(\frac{12}{q}\right) = \left(\frac{3}{q}\right) = -1$$

Precisely when $q \equiv 5, 7 \pmod{12}$.

Lemma

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

Legendre Symbols and a Density!

Lemma

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

Theorem (Dirichlet)

Let a and n be coprime integers. Then there exists infinitely many primes, $\{p_i\}$ such that $p_i \equiv a \pmod{n}$. Moreover,

$$\sum p_i^{-1} = \infty.$$

Legendre Symbols and a Density!

The setup:

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

Theorem (Niven)

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

Recall: If q is a prime such that $q \equiv 5, 7 \pmod{12}$, then we have no solutions.

Legendre Symbols and a Density!

The setup:

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

Theorem (Niven)

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

Recall: If q is a prime such that $q \equiv 5, 7 \pmod{12}$, then we have no solutions.

Legendre Symbols and a Density!

The setup:

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

Theorem (Niven)

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

Recall: If q is a prime such that $q \equiv 5, 7 \pmod{12}$, then we have no solutions.

Legendre Symbols and a Density!

The setup:

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

Theorem (Niven)

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

Recall: If q is a prime such that $q \equiv 5, 7 \pmod{12}$, then we have no solutions.

Legendre Symbols and a Density!

The setup:

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

Theorem (Niven)

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

Recall: If q is a prime such that $q \equiv 5, 7 \pmod{12}$, then we have no solutions.

Result for $k = 2$

Proposition

Let $\mathcal{A}_2$ be the set of integers $d \geq 2$ such that the equation

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

has a solution (x, y, n). Then $\mathcal{A}_2$ has natural density zero.

Can we extend this result to any exponent k?

Answer: No.

Result for $k = 2$

Proposition

Let $\mathcal{A}_2$ be the set of integers $d \geq 2$ such that the equation

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

has a solution (x, y, n). Then $\mathcal{A}_2$ has natural density zero.

Can we extend this result to any exponent k?
Answer: No.

The Result

Theorem (V. Patel, S.Siksek)

Let $k \geq 2$ be an even integer. Let $\mathcal{A}_k$ 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 $\mathcal{A}_k$ has natural density zero. In other words we have

$$\lim_{X \to \infty} \frac{\#\{d \in \mathcal{A}_k : d \leq X\}}{X} = 0.$$

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

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

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 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

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 $\mathrm{ord}_q(d) = 1$. Then the equation has no solutions. (i.e. $d \notin \mathcal{A}_k$).

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 $\operatorname{ord}_q(d) = 1$. Then the equation has no solutions. (i.e. $d \notin \mathcal{A}_k$).

Remark: Computationally we checked $k \leq 75{,}000$ and we could always find such a q.

Recall: Result for $k = 2$

Proposition

Let $\mathcal{A}_2$ be the set of integers $d \geq 2$ such that the equation

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

has a solution (x, y, n). Then $\mathcal{A}_2$ has natural density zero.

Can we extend this result to any exponent k?
Answer: No.

Odd k: A Complete Disaster

This is one of the few slides where we consider k to be odd!

$$x^k + (x+1)^k + \cdots + (x+(d-1))^k \equiv d \cdot B_k(x) \pmod{q^2}.$$

We want to find a prime q such that $B_k(x) \equiv 0 \pmod{q}$ has no solutions.
However, it is well–known that the odd degree Bernoulli polynomials have linear factors!

$$B_k(x) = x(x-1)(x-1/2)h(x) \equiv 0 \pmod{q}.$$

Hence our criterion fails for every single prime q.

Odd k: A Complete Disaster

This is one of the few slides where we consider k to be odd!

$$x^k + (x+1)^k + \cdots + (x+(d-1))^k \equiv d \cdot B_k(x) \pmod{q^2}.$$

We want to find a prime q such that $B_k(x) \equiv 0 \pmod{q}$ has no solutions.

However, it is well–known that the odd degree Bernoulli polynomials have linear factors!

$$B_k(x) = x(x-1)(x-1/2)h(x) \equiv 0 \pmod{q}.$$

Hence our criterion fails for every single prime q.

Odd k: A Complete Disaster

This is one of the few slides where we consider k to be odd!

$$x^k + (x+1)^k + \cdots + (x+(d-1))^k \equiv d \cdot B_k(x) \pmod{q^2}.$$

We want to find a prime q such that $B_k(x) \equiv 0 \pmod{q}$ has no solutions.
However, it is well–known that the odd degree Bernoulli polynomials have linear factors!

$$B_k(x) = x(x-1)(x-1/2)h(x) \equiv 0 \pmod{q}.$$

Hence our criterion fails for every single prime q.

Odd k: A Complete Disaster

This is one of the few slides where we consider k to be odd!

$$x^k + (x+1)^k + \cdots + (x+(d-1))^k \equiv d \cdot B_k(x) \pmod{q^2}.$$

We want to find a prime q such that $B_k(x) \equiv 0 \pmod{q}$ has no solutions.
However, it is well–known that the odd degree Bernoulli polynomials have linear factors!

$$B_k(x) = x(x-1)(x-1/2)h(x) \equiv 0 \pmod{q}.$$

Hence our criterion fails for every single prime q.

Odd k: A Complete Disaster

This is one of the few slides where we consider k to be odd!

$$x^k + (x+1)^k + \cdots + (x+(d-1))^k \equiv d \cdot B_k(x) \pmod{q^2}.$$

We want to find a prime q such that $B_k(x) \equiv 0 \pmod{q}$ has no solutions.
However, it is well–known that the odd degree Bernoulli polynomials have linear factors!

$$B_k(x) = x(x-1)(x-1/2)h(x) \equiv 0 \pmod{q}.$$

Hence our criterion fails for every single prime q.

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 $\mathrm{Frob}_{q_i} \in G$ is conjugate to μ. 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 $\mathrm{Frob}_{q_i} \in G$ is conjugate to μ. Then we can apply Niven's results to deduce 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.

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)

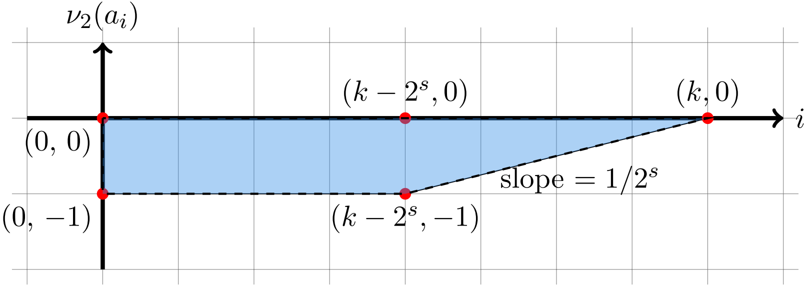
Let $n \geq 2$ be even. Then

$$b_n + \sum_{(p-1)|n} \frac{1}{p} \in \mathbb{Z}.$$

"Bad Prime 2"

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 $(-1)^k B_k(x) = B_k(1-x)$ 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 $(-1)^k B_k(x) = B_k(1-x)$ 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 $\mathbb{Q}$.

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.
- ν_2 on $\mathbb{Q}_2$ which we extend uniquely to $L_{\mathfrak{P}}$ (also call it ν_2).
- $H = \mathrm{Gal}(L_{\mathfrak{P}}/\mathbb{Q}_2) \subset G$ be the decomposition subgroup corresponding to $\mathfrak{P}$.

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.
- ν_2 on $\mathbb{Q}_2$ which we extend uniquely to $L_{\mathfrak{P}}$ (also call it ν_2).
- $H = \mathrm{Gal}(L_{\mathfrak{P}}/\mathbb{Q}_2) \subset G$ be the decomposition subgroup corresponding to $\mathfrak{P}$.

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.
- ν_2 on $\mathbb{Q}_2$ which we extend uniquely to $L_{\mathfrak{P}}$ (also call it ν_2).
- $H = \mathrm{Gal}(L_{\mathfrak{P}}/\mathbb{Q}_2) \subset G$ be the decomposition subgroup corresponding to $\mathfrak{P}$.

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.
- ν_2 on $\mathbb{Q}_2$ which we extend uniquely to $L_{\mathfrak{P}}$ (also call it ν_2).
- $H = \mathrm{Gal}(L_{\mathfrak{P}}/\mathbb{Q}_2) \subset G$ be the decomposition subgroup corresponding to $\mathfrak{P}$.

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.
- ν_2 on $\mathbb{Q}_2$ which we extend uniquely to $L_{\mathfrak{P}}$ (also call it ν_2).
- $H = \mathrm{Gal}(L_{\mathfrak{P}}/\mathbb{Q}_2) \subset G$ be the decomposition subgroup corresponding to $\mathfrak{P}$.

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.
- ν_2 on $\mathbb{Q}_2$ which we extend uniquely to $L_{\mathfrak{P}}$ (also call it ν_2).
- $H = \mathrm{Gal}(L_{\mathfrak{P}}/\mathbb{Q}_2) \subset G$ be the decomposition subgroup corresponding to $\mathfrak{P}$.

A sketch proof of the Proposition

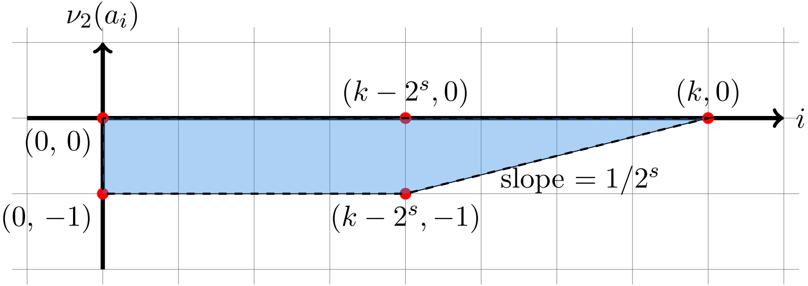
$$B_k(x) = g(x)h(x)$$

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 β_j.
- Pick $\mu \in H$ such that μ 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 $k = 2^s \cdot t$, $s \geq 1$.



Finding μ

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 β_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 $\mathbb{F}_{\mathfrak{P}}$ be the residue field of $\mathfrak{P}$.
2. Let $C = \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_2)$.
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.

Finding μ

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 β_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 $\mathbb{F}_{\mathfrak{P}}$ be the residue field of $\mathfrak{P}$.
2. Let $C = \mathrm{Gal}\left(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_2\right)$.
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 μ

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 β_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 $\mathbb{F}_{\mathfrak{P}}$ be the residue field of $\mathfrak{P}$.
2. Let $C = \mathrm{Gal}\left(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_2\right)$.
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 μ

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 β_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 $\mathbb{F}_{\mathfrak{P}}$ be the residue field of $\mathfrak{P}$.
2. Let $C = \mathrm{Gal}\left(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_2\right)$.
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 μ

Lemma

Let H be a finite group acting transitively on a finite set $\{\beta_1, \dots, \beta_n\}$. Let $H_i \subset H$ be the stabiliser of β_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 $\{\beta_1, \dots, \beta_n\}$ such that $\pi(\mu)$ is a generator of C.

1. Let $\mathbb{F}_{\mathfrak{P}}$ be the residue field of $\mathfrak{P}$.
2. Let $C = \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_2)$.
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.

Finding μ

Lemma

Let H be a finite group acting transitively on a finite set $\{\beta_1, \dots, \beta_n\}$. Let $H_i \subset H$ be the stabiliser of β_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 $\{\beta_1, \dots, \beta_n\}$ such that $\pi(\mu)$ is a generator of C.

1. Let $\mathbb{F}_{\mathfrak{P}}$ be the residue field of $\mathfrak{P}$.
2. Let $C = \mathrm{Gal}\left(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_2\right)$.
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.

Recap: 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 β_j.
- Pick $\mu \in H$ such that μ acts freely on the roots of $h(x)$.
- Check it doesn't end up fixing a root of $g(x)$.

Check $g(x)$

$$B_k(x) = g(x)h(x)$$

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

Lemma

μ acts freely on the α_i.

1. Suppose not. Let α be a root that is fixed by μ.
2. $\nu_2(\alpha) = 0$ so let $\bar{\alpha} = \alpha \pmod{\mathfrak{P}}$, $\bar{\alpha} \in \mathbb{F}_{\mathfrak{P}}$.
3. α fixed by μ 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!

Check $g(x)$

$$B_k(x) = g(x)h(x)$$

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

Lemma

μ acts freely on the α_i.

1. Suppose not. Let α be a root that is fixed by μ.
2. $\nu_2(\alpha) = 0$ so let $\bar{\alpha} = \alpha \pmod{\mathfrak{P}}$, $\bar{\alpha} \in \mathbb{F}_{\mathfrak{P}}$.
3. α fixed by μ 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!

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

μ acts freely on the α_i.

1. Suppose not. Let α be a root that is fixed by μ.
2. $\nu_2(\alpha) = 0$ so let $\bar{\alpha} = \alpha \pmod{\mathfrak{P}}$, $\bar{\alpha} \in \mathbb{F}_{\mathfrak{P}}$.
3. α fixed by μ 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!

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

μ acts freely on the α_i.

1. Suppose not. Let α be a root that is fixed by μ.
2. $\nu_2(\alpha) = 0$ so let $\bar{\alpha} = \alpha \pmod{\mathfrak{P}}$, $\bar{\alpha} \in \mathbb{F}_{\mathfrak{P}}$.
3. α fixed by μ 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!

Check $g(x)$

$$B_k(x) = g(x)h(x)$$

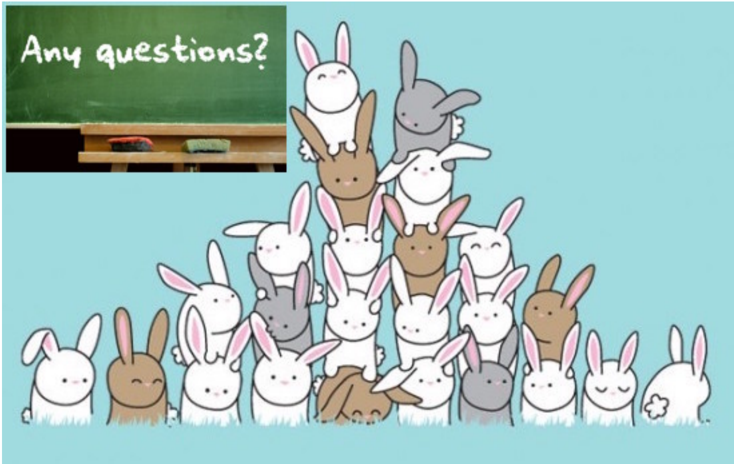
where $g(x)$ has degree $k - 2^s$. Label the roots $\{\alpha_1, \dots, \alpha_{k-2^s}\}$, and $h(x)$ has degree 2^s. Label the roots $\{\beta_1, \dots, \beta_{2^s}\}$.

Lemma

μ acts freely on the α_i.

1. Suppose not. Let α be a root that is fixed by μ.
2. $\nu_2(\alpha) = 0$ so let $\bar{\alpha} = \alpha \pmod{\mathfrak{P}}$, $\bar{\alpha} \in \mathbb{F}_{\mathfrak{P}}$.
3. α fixed by μ 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 $k = 2$

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

$$X^2 + C \cdot 1^p = (1/d)y^p$$

Solving the equations for $k = 2$

d	Equation	Level	Dimension
6	$2y^p - 5 \times 7 = 3(2x+7)^2$	$2^7 \times 3^2 \times 5 \times 7$	480
11	$11^{p-1}y^p - 2 \times 5 = (x+6)^2$	$2^7 \times 5 \times 11$	160
13	$13^{p-1}y^p - 2 \times 7 = (x+7)^2$	$2^7 \times 7 \times 13$	288
22	$2 \times 11^{p-1}y^p - 7 \times 23 = (2x+23)^2$	$2^7 \times 7 \times 11 \times 23$	5,280
23	$23^{p-1}y^p - 2^2 \times 11 = (x+12)^2$	$2^3 \times 11 \times 23$	54
26	$2 \times 13^{p-1}y^p - 3^2 \times 5^2 = (2x+27)^2$	$2^7 \times 3 \times 5 \times 13$	384
33	$11^{p-1}y^p - 2^4 \times 17 = 3(x+17)^2$	$2^3 \times 3^2 \times 11 \times 17$	200
37	$37^{p-1}y^p - 2 \times 3 \times 19 = (x+19)^2$	$2^7 \times 3 \times 19 \times 37$	5,184
39	$13^{p-1}y^p - 2^2 \times 5 \times 19 = 3(x+20)^2$	$2^3 \times 3^2 \times 5 \times 13 \times 19$	1,080
46	$2 \times 23^{p-1}y^p - 3^2 \times 5 \times 47 = (2x+47)^2$	$2^7 \times 3 \times 5 \times 23 \times 47$	32,384
47	$47^{p-1}y^p - 2^3 \times 23 = (x+24)^2$	$2^5 \times 23 \times 47$	1,012
59	$59^{p-1}y^p - 2 \times 5 \times 29 = (x+30)^2$	$2^7 \times 5 \times 29 \times 59$	25,984

SOLVING THE EQUATIONS FOR $k = 4$

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

Where X is a quadratic in the original variable x.