Differences between perfect powers : the Lebesgue-Nagell equation

Michael Bennett (joint with Philippe Michaud-Jacobs and Samir Siksek)

University of British Columbia (and Warwick)

April 2022

Differences between perfect powers : Catalan's Conjecture

Theorem ($Mihăilescu$, 2004)

If x, y, n and m are positive integers with $n, m \geq 2$, then the equation

$$x^m - y^n = 1$$

has only the solution $(x, y, m, n) = (3, 2, 2, 3)$.

Differences between perfect powers : Catalan's Conjecture

Theorem ($Mih\check{a}ilescu$, 2004)

If x, y, n and m are positive integers with $n, m \geq 2$, then the equation

$$x^m - y^n = 1$$

has only the solution $(x, y, m, n) = (3, 2, 2, 3)$.

Question Is there another gap of length 2 other than that following 25? i.e. What about the equation

$$x^m - y^n = 2?$$

Pillai's Conjecture

Conjecture If c is a positive integer, then there are at most finitely many positive integers x, y, m and n with $m, n \geq 2$ such that

$$x^m - y^n = c.$$

Pillai's Conjecture

Conjecture If c is a positive integer, then there are at most finitely many positive integers x, y, m and n with $m, n \geq 2$ such that

$$x^m - y^n = c.$$

i.e. the length of the gaps in the sequence of perfect powers goes to ∞.

Pillai's Conjecture

Conjecture If c is a positive integer, then there are at most finitely many positive integers x, y, m and n with $m, n \geq 2$ such that

$$x^m - y^n = c.$$

i.e. the length of the gaps in the sequence of perfect powers goes to ∞.

This conjecture is open for every $c > 1$.

Gaps between squares and other powers

If we denote by $P(m)$ the greatest prime divisor of a nonzero integer m, we may prove that there exists an absolute positive constant c such that

$$P(x^2 - y^n) \geq c \log n$$

and, for suitably large x,

$$P(x^2 - y^n) \geq \frac{\log \log y}{30n}.$$

What we'll focus on

We will consider the equation

$$x^2 + D = y^n,$$

in situations where either

1. D is a fixed integer, or
2. the prime divisors of D belong to a fixed, finite set of primes S.

What we'll focus on

We will consider the equation

$$x^2 + D = y^n,$$

in situations where either

1. D is a fixed integer, or
2. the prime divisors of D belong to a fixed, finite set of primes S.

These problems are generally known as *Lebesgue-Nagell* equations.

What we'll focus on

We will consider the equation

$$x^2 + D = y^n,$$

in situations where either

1. D is a fixed integer, or
2. the prime divisors of D belong to a fixed, finite set of primes S.

These problems are generally known as *Lebesgue-Nagell* equations.

The aforementioned results from linear forms in logarithms imply the existence of an algorithm to solve such equations.

A sketch of how such results are proved

Consider the equation

$$x^2 + D = y^n.$$

Then if we have

$$\pm x + \sqrt{-D} = (a + b\sqrt{-D})^n,$$

for integers a and b, it follows that we have a solution to our equation with $y = a^2 + Db^2$.

A sketch of how such results are proved: continued

Now the existence of integers a and b for which

$$\pm x + \sqrt{-D} = (a + b\sqrt{-D})^n$$

is *necessary* in order to have a solution to $x^2 + D = y^n$ if

A sketch of how such results are proved: continued

Now the existence of integers a and b for which

$$\pm x + \sqrt{-D} = (a + b\sqrt{-D})^n$$

is *necessary* in order to have a solution to $x^2 + D = y^n$ if

- $D \not\equiv 3 \mod 4$,

A sketch of how such results are proved: continued

Now the existence of integers a and b for which

$$\pm x + \sqrt{-D} = (a + b\sqrt{-D})^n$$

is *necessary* in order to have a solution to $x^2 + D = y^n$ if

- $D \not\equiv 3 \mod 4$,
- the question of units did not arise,

A sketch of how such results are proved: continued

Now the existence of integers a and b for which

$$\pm x + \sqrt{-D} = (a + b\sqrt{-D})^n$$

is *necessary* in order to have a solution to $x^2 + D = y^n$ if

- $D \not\equiv 3 \mod 4$,
- the question of units did not arise,
- $\mathbb{Q}(\sqrt{-D})$ has class number one,

A sketch of how such results are proved: continued

Now the existence of integers a and b for which

$$\pm x + \sqrt{-D} = (a + b\sqrt{-D})^n$$

is *necessary* in order to have a solution to $x^2 + D = y^n$ if

- $D \not\equiv 3 \mod 4$,
- the question of units did not arise,
- $\mathbb{Q}(\sqrt{-D})$ has class number one,
- D is squarefree, and

A sketch of how such results are proved: continued

Now the existence of integers a and b for which

$$\pm x + \sqrt{-D} = (a + b\sqrt{-D})^n$$

is *necessary* in order to have a solution to $x^2 + D = y^n$ if

- $D \not\equiv 3 \mod 4$,
- the question of units did not arise,
- $\mathbb{Q}(\sqrt{-D})$ has class number one,
- D is squarefree, and
- the factors $\pm x + \sqrt{-D}$ are coprime.

A sketch of how such results are proved: continued

If we have

$$\pm x + \sqrt{-D} = (a + b\sqrt{-D})^n$$

then, writing $\alpha = a + b\sqrt{-D}$,

$$\alpha^n - \overline{\alpha}^n = 2\sqrt{-D}$$

and so

$$\left| n \log \left(\frac{\alpha}{\overline{\alpha}} \right) - k\pi i \right| = \left| n \log \left(\frac{\alpha}{\overline{\alpha}} \right) - k \log(-1) \right|$$

is really small, for a suitable choice of k.

A sketch of how such results are proved: continued

If we have

$$\pm x + \sqrt{-D} = (a + b\sqrt{-D})^n$$

then, writing $\alpha = a + b\sqrt{-D}$,

$$\alpha^n - \overline{\alpha}^n = 2\sqrt{-D}$$

and so

$$\left| n \log \left(\frac{\alpha}{\overline{\alpha}} \right) - k\pi i \right| = \left| n \log \left(\frac{\alpha}{\overline{\alpha}} \right) - k \log(-1) \right|$$

is really small, for a suitable choice of k. Lower bounds for linear forms in two complex logarithms then gives an upper bound upon n.

Moreover

For each *fixed* $n \geq 3$, the equation

$$\pm x + \sqrt{-D} = (a + b\sqrt{-D})^n$$

leads to a degree n *Thue* equation.

Moreover

For each *fixed* $n \geq 3$, the equation

$$\pm x + \sqrt{-D} = (a + b\sqrt{-D})^n$$

leads to a degree n *Thue* equation.

Also, writing

$$L_n = \frac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}},$$

we may show that L_n is a *Lucas sequence*, and that $L_n = \pm 1$.

Moreover

For each *fixed* $n \geq 3$, the equation

$$\pm x + \sqrt{-D} = (a + b\sqrt{-D})^n$$

leads to a degree n *Thue* equation.

Also, writing

$$L_n = \frac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}},$$

we may show that L_n is a *Lucas sequence*, and that $L_n = \pm 1$.

The Primitive Divisor Theorem of Bilu, Hanrot and Voutier then provides a very sharp bound upon n.

More generally : the easy cases

Similar arguments work for the equation

$$x^2 + D = y^n,$$

where we assume

- $D > 0$,
- $\gcd(x, D) = 1$,
- y is odd, and
- $\gcd(n, h(\mathbb{Q}(\sqrt{-D})) = 1$.

More generally : the easy cases

This enable one to easily solve, by way of example, the equation

$$x^2 + D = y^n,$$

if

- e.g. $D = 5$, or
- e.g. $D = 2^a 3^b 11^c$, etc

More generally : the easy cases

This enable one to easily solve, by way of example, the equation

$$x^2 + D = y^n,$$

if

- e.g. $D = 5$, or
- e.g. $D = 2^a 3^b 11^c$, etc

There is a very extensive literature on equations solved via appeal to the Primitive Divisor Theorem.

A hard case : $D = -2$

Consider the equation

$$x^2 - 2 = y^n.$$

A hard case : $D = -2$

Consider the equation

$$x^2 - 2 = y^n.$$

Linear forms in logs enable us to explicitly bound x, y and n. In fact, we have (assuming that n is prime), $n \leq 4111$.

A hard case : $D = -2$

Consider the equation

$$x^2 - 2 = y^n.$$

Linear forms in logs enable us to explicitly bound x, y and n. In fact, we have (assuming that n is prime), $n \leq 4111$.

For each fixed smaller $n \geq 3$, solutions to our equations correspond to solutions to a given *Thue equation* of the shape $F(a, b) = \pm 1$. Here, $F(a, b)$ is a binary form over $\mathbb{Z}[a, b]$ of degree n.

A hard case : $D = -2$

Consider the equation

$$x^2 - 2 = y^n.$$

Linear forms in logs enable us to explicitly bound x, y and n. In fact, we have (assuming that n is prime), $n \leq 4111$.

For each fixed smaller $n \geq 3$, solutions to our equations correspond to solutions to a given *Thue equation* of the shape $F(a, b) = \pm 1$. Here, $F(a, b)$ is a binary form over $\mathbb{Z}[a, b]$ of degree n.

We're left with prime n, $41 \leq n \leq 4111$, $n \equiv 13, 17, 19, 23 \mod 24$.

Our focus

We consider the equations

$$x^2 + 2^\alpha 3^\beta 5^\gamma 7^\delta 11^\tau = y^n$$

and

$$x^2 \pm q^a = y^n,$$

where q is prime and primitive divisor arguments fail.

Our focus : continued

i.e., we will consider equations of the shape

$$x^2 + 2^\alpha 3^\beta 5^\gamma 7^\delta 11^\tau = y^n,$$

$$x^2 - q^a = y^n$$

and

$$x^2 + q^a = y^n,$$

where q is prime and, in the last case, $q \equiv 7 \mod 8$.

The equation $x^2 + 2^\alpha 3^\beta 5^\gamma 7^\delta 11^\tau = y^n$

Theorem (B., Siksek, 2022)

There are precisely 1240 *solutions to the equation*

$$x^2 + 2^\alpha 3^\beta 5^\gamma 7^\delta 11^\tau = y^n,$$

in integers, with x, y *positive,* $\gcd(x, y) = 1$ *and* $n \geq 3$. *They are distributed as follows.*

n	$\#(x,y)$	n	$\#(x,y)$	n	$\#(x,y)$	n	$\#(x,y)$
3	755	7	5	12	4	26	1
4	385	8	17	13	1		
5	11	9	1	14	4		
6	51	10	4	15	1		

Ingredients in the proof

$$x^2 + 2^\alpha 3^\beta 5^\gamma 7^\delta 11^\tau = y^n$$

1. appeal to bounds for linear forms in two p-adic logarithms
2. refined use of lower bounds for linear forms in two and three complex logarithms
3. efficient sieving with Frey-Hellegouarch curves
4. a computationally efficient approach to treat the genus one curves encountered when solving the equation for $n \in \{3, 4\}$
5. new practical techniques for solving Thue-Mahler equations of moderate ($n \leq 13$) degree.

Linear forms in p-adic logarithms

$$x^2 + 2^\alpha 3^\beta 5^\gamma 7^\delta 11^\tau = y^n$$

With $\alpha = 0$, $3^\beta 5^\gamma 7^\delta 11^\tau = c^2 d$, $d \in \{7, 15, 55, 231\}$ and y even, we apply bounds for p-adic logarithms with $p \in \{3, 5, 7, 11\}$ and, when all is said and done, obtain from our lower bounds for linear forms in three complex logarithms, essentially the same upper bound upon n as one does for the equation

$$x^2 + d = y^n.$$

Upper bounds on n and elliptic curve obstructions

d	$N(d)$	Primes $13 \leq n < N(d)$	Pairs (E, d)
7	6×10^8	31324698	39
15	4×10^8	21336321	28
55	5×10^8	26355862	27
231	1.2×10^9	60454700	20

Table: The table records the number of primes in the interval $13 \leq n < N(d)$ and the number of pairs (E, d).

Efficient sieving with Frey-Hellegouarch curves I

We applied an argument originally due to Kraus to the remaining $\approx 3.7 \times 10^9$ triples (E, d, n). For each such triple, we searched for a prime $q = kn + 1$ with $k < 10^3$ such that a particular technical hypothesis was satisfied. This computation took around 29000 hours, but was in fact distributed over 64 processors, and finished in around 20 days. For all but 1230 of the 3739782484 triples (E, d, n) the script found some q which enabled us to eliminate the triple. We are therefore reduced to considering the remaining 1230 triples (E, d, n); we note that the largest value of n appearing in any of these triples is $n = 1861$ and this corresponds to E being the elliptic curve with Cremona label `210A1` and $d = 15$.

Efficient sieving with Frey-Hellegouarch curves II

For the remaining triples, we applied a more refined sieve, using several auxiliary primes simultaneously and applying additional symplectic criteria. We reached an empty intersection in 1224 cases. The remaining 6 cases are as follows :

Elliptic Curve	d	n
462b1	231	13
462f1	231	13
2310j1	231	13
2310l1	231	13
2310m1	231	13
2310o1	15	13

Efficient sieving with Frey-Hellegouarch curves III

To eliminate the first 5 of these cases, we make use of the following result of Halberstadt and Kraus :

Theorem (Halberstadt and Kraus)

Let E_1 and E_2 be elliptic curves over $\mathbb{Q}$ and write Δ_j for the minimal discriminant of E_j. Let $n \geq 5$ be a prime such that $\overline{\rho}_{E_1,n} \sim \overline{\rho}_{E_2,n}$. Let q_1, $q_2 \neq n$ be distinct primes of multiplicative reduction for both elliptic curves such that $ord_{q_i}(\Delta_j) \not\equiv 0 \pmod{n}$ for $i, j \in \{1, 2\}$. Then

$$\frac{ord_{q_1}(\Delta_1) \cdot ord_{q_2}(\Delta_1)}{ord_{q_1}(\Delta_2) \cdot ord_{q_2}(\Delta_2)}$$

is congruent to a square modulo n.

The remaining obstruction

We are left with the last triple, which we are unable to eliminate by any of our sieving.

The remaining obstruction

We are left with the last triple, which we are unable to eliminate by any of our sieving.

This is because it arises from a solution to our equation, namely

$$8143^2 + 3^3 \cdot 5 \cdot 7^2 \cdot 11^2 = 4^{13}.$$

We are thus forced to solve the equation

$$x^2 + 3^\beta 5^\gamma 7^\delta 11^\tau = y^{13},$$

with y even, $\beta\gamma \equiv 1 \mod 2$ and $\delta \equiv \tau \equiv 0 \mod 2$.

A Thue-Mahler equation

Standard arguments reduce this problem to that of solving the Thue-Mahler equation

$$F_{13}(r,s) = \sum_{i=0}^{13} a_i r^{13-i} s^i = \pm 4 \cdot 3^{\beta_3} \cdot 5^{\beta_5} \cdot 7^{\beta_7} \cdot 11^{\beta_{11}},$$

where

i	a_i	i	a_i	i	a_i
0	1	5	36036	10	195624
1	0	6	−34320	11	−95160
2	−312	7	−226512	12	−51428
3	−1144	8	−66924	13	924.
4	8580	9	340340		

A Thue-Mahler equation

The only solution is with

$$r = 0,\ s = \pm 1,\ \beta_3 = 1,\ \beta_5 = 0,\ \beta_7 = 1 \ \text{ and } \ \beta_{11} = 1.$$

This corresponds to the identity

$$8143^2 + 3^3 \cdot 5 \cdot 7^2 \cdot 11^2 = 4^{13}.$$

Finishing touches : small values of n

1. $n = 3$ – solutions correspond to elliptic curves over $\mathbb{Q}$ with good reduction outside $\{2, 3, 5, 7, 11\}$.
2. $n = 4$ – solutions correspond to solutions to equations of the shape $u + v = z^2$, where u and v are S-units for $S = \{2, 3, 5, 7, 11\}$.
3. $n = 5$ – Thue-Mahler equations.

$x^2 - q^a = y^n$: earlier work . . . linear forms in logarithms

Theorem (Bugeaud, 1997)

If x, y, n and a are positive integers with y odd, and q is an odd prime with $\gcd(x, q) = 1$ and

$$x^2 - q^a = y^n,$$

then

$$n < 4.5 \times 10^6 q^2 \log^2 q.$$

The bounds on n in case y is even, or for the equation $x^2 + q^a = y^n$ are quite a bit worse.

$x^2 - q^a = y^n$: earlier work . . . Frey curves

Theorem (Ivorra and Kraus, 2004)

"Solves" the more general equation

$$x^n + q^a y^n = z^2,$$

unless q *can be written in the form*

$$q = |t^2 \pm 2^k|,$$

where t *and* k *are integers, with* $k = 0$, $k = 3$ *or* $k \geq 7$.

Frey curves, continued

The primes q with $q < 100$ that are not of the form $|t^2 \pm 2^k|$, for t and k integers, with $k = 0$, $k = 3$ or $k \geq 7$, are

$$q \in \{11, 13, 19, 29, 43, 53, 59, 61, 67, 83\}.$$

A conclusion : the good news

The *modular method* (based on the modularity of Galois representations attached to Frey curves) enable one to solve equations like

$$x^2 - q^a = y^n$$

and

$$x^2 + q^a = y^n,$$

"completely", without recourse to linear forms in logarithms, for *most* primes q.

A conclusion : the bad news

The *modular method*, at least with current technology, does not appear to be able to fully solve equations like

$$x^2 - q^a = y^n,$$

when, say, $q = 3$ or $q = t^2 + 1$, for t an integer, even with all the help linear forms in logarithms can provide.

What about the ugly?

What if $q = |t^2 \pm 8|$ or $q = |t^2 \pm 2^k|$, with $k \geq 7$, but $q \neq u^2 \pm 1$, for every $u \in \mathbb{Z}$?

Theorem (B., Siksek, 2022)

If $q \in \{7, 11, 13, 19, 23, 29, 31, 43, 47, 53, 59, 61, 67, 71, 79, 83\}$, *then there are no solutions to the equation*

$$x^2 - q^a = y^n,$$

in integers x, y *and* a *with* $q \nmid x$ *and prime* $n \geq 7$.

Theorem (B., Siksek, 2022)

If x, y, q, a *and* n *are positive integers with* q *prime,* $2 \leq q < 100$, $q \nmid x$, $n \geq 3$ *and*

$$x^2 + q^a = y^n,$$

then $n = 3$ *or* (q, a, y, n) *is one of*

$$(2,5,3,4), (7,1,2,4), (7,2,5,4), (7,1,2,5),$$
$$(7,1,8,5), (7,1,2,7), (7,3,2,9), (7,1,2,15),$$
$$(17,1,3,4), (19,1,55,5), (23,3,78,4), (23,1,2,5),$$
$$(23,1,2,11), (29,2,5,7), (31,1,4,4), (31,1,2,5),$$
$$(31,1,2,8), (41,2,29,4), (41,2,5,5), (47,1,3,5),$$
$$(47,1,2,7), (53,1,3,6), (71,1,6,4), (71,1,3,7),$$
$$(71,1,2,9), (79,1,2,7), (83,1,3,9) \text{ or } (97,1,7,4).$$

Ingredients in the proofs

$$x^2 \pm q^a = y^n$$

1. Refinements in the modular method, using auxiliary primes,
2. Minor sharpenings of complex linear form bounds,
3. Careful use of bounds for q-adic logarithms, and
4. Sieving using Frey curves, symplectic criteria and primes $\equiv 1 \mod n$.

Remaining unsolved cases for $x^2 - q^a = y^n,\ q < 100$

$$x^2 - 2 = y^n, \tag{1}$$

$$x^2 - q^{2k+1} = y^n, \quad 2 \nmid y, \tag{2}$$

for $q \in \{3, 5, 17, 37, 41, 73, 89\}$, and

$$x^2 - q^{2k+1} = y^n, \quad 2 \mid y, \tag{3}$$

for $q \in \{17, 41, 89, 97\}$.

Remaining unsolved cases for $x^2 - q^a = y^n,\ q < 100$

The fundamental obstructions to resolving equation (3) correspond to the identities

$$23^2 - 17 = 2^9,\ 13^2 - 41 = 2^7,\ 91^2 - 89 = 2^{13}$$

and $15^2 - 97 = 2^7$.

Remaining unsolved cases for $x^2 - q^a = y^n,\ q < 100$

Theorem (B., Michaud-Jacobs, Siksek, 2022)

Let $q \in \{41, 97\}$. Then the solutions to the equation

$$x^2 - q^{2k+1} = y^n, \quad 2 \mid y,$$

in integers x, y, k, n, with $x, k \geq 0$, $n \geq 3$ and $\gcd(x, y) = 1$ are as follows:

$$(q, x, y, k, n) = (41, 3, -2, 0, 5), (41, 7, 2, 0, 3), (41, 13, 2, 0, 7),$$
$$(41, 411, 10, 1, 5), (97, 15, 2, 0, 7) \text{ and } (97, 77, 18, 0, 3).$$

Remaining unsolved cases for $x^2 - q^a = y^n,\ q < 100$

We overcome our obstructions through the use of $\mathbb{Q}$-curves and multi-Frey techniques.

The identities $13^2 - 41 = 2^7$ and $15^2 - 97 = 2^7$ have corresponding Frey $\mathbb{Q}$-curves without multiplicative reduction at primes above 2.

Regrettably, this fails to be the case for the identities $23^2 - 17 = 2^9$ and $91^2 - 89 = 2^{13}$.