Perfect powers in products with terms from arithmetic progression - A survey

Kálmán Győry

University of Debrecen
Hungary

Erdős 100 Conference
Diophantine Number Theory
Budapest

5th July, 2013

Let $k \geq 3$, $n \geq 2$, m, $d \geq 1$ be integers with $\gcd(m, d) = 1$. Can

$$m(m+d)\dots(m+(k-1)d)$$

be an n-th power?

$\mathbf{n = 2}$

$\mathbf{k = 3}$, $m = x^2$, $m + d = z^2$, $m + 2d = y^2 \iff x^2 + y^2 = 2z^2$, $\gcd(x, y) = 1$, infinitely many solutions

$\mathbf{k = 4}$, **Fermat**: each of m, $m + d$, $m + 2d$, $m + 3d$ cannot be square;
Euler: $m(m+d)(m+2d)(m+3d) \neq \square$

$\mathbf{n} > \mathbf{2}$, very rich literature

$\mathbf{k} = \mathbf{3}$, $m = x^n$, $m + d = z^n$, $m + 2d = y^n \iff$ $x^n + y^n = 2z^n$, $\gcd(x, y) = 1$, $y, z > 1$ **Darmon and Merel (1997)**: *There is no solution*

For **products**, a great number of partial results, but the **general problem** is still **open**.

After a lot of *special results* (**Euler**, **Erdős**, **Rigge**, **Siegel** and others), the **problem** has been **solved** for $\mathbf{d = 1}$.

Theorem A (Erdős and Selfridge, 1975)

The equation

$$m(m+1)\dots(m+k-1) = y^n \qquad (1)$$

has no solutions in positive integers m, k, y, n *with* $k \geq 2$, $n \geq 2$.

Proof: elementary but complicated and ingenious

A **related equation** is

$$\binom{m+k-1}{k} = y^n, \qquad (2)$$

m, k, y, n integers with $k, y, n \geq 2$ and $m \geq k+1$

- $\mathbf{k = n = 2}$: Pell equation, infinitely many solutions
- $(\mathbf{k}, \mathbf{n}) = (\mathbf{3}, \mathbf{2})$, **Meyl (1878)**, **Watson(1919)**: The only solution is $\binom{50}{3} = 140^2$

Erdős (1951): *for* $k \geq 4$, *there is no solution*
elementary method, does not work for $k < 4$.

Gy (1997): *for* $k = 2, 3$, $n > 2$, *there is no solution.*
Baker's method and deep results on generalized Fermat's equations.

Theorem B (**Erdős** $k \geq 4$, **Győry**, $k = 2, 3$)

Apart from the case $k = n = 2$,
$(m, k, y, n) = (48, 3, 140, 2)$ *is the only solution of* (2).

Common generalization of equations (1) and (2)

$$m(m+1)\dots(m+k-1) = by^n, \qquad (3)$$

m, k, b, y, n positive integers with $k \geq 2$, $n \geq 2$, $P(b) \leq k$; $P(b)$ the *greatest prime factor* of b.

- $\mathbf{k = b = n = 2}$: infinitely many solutions
- **given k**: (m, y) yields a solution with $P(y) \leq k \iff m \in \{1, 2, \dots, p^{(k)} - k\}$, where $p^{(k)}$ is the *least prime* with $p^{(k)} > k$; such solutions are called **trivial**, they can be easily found.
  non-trivial solutions: $P(y) > k$.

Theorem C (Erdős and Selfridge, 1975, $P(b) < k$; Saradha, 1997, $k \geq 4$; Gy, 1998, $k = 2, 3$)

Apart from the case $(k, b, n) = (2, 2, 2)$, the only non-trivial solution of equation (3) is $(m, k, b, y, n) = (48, 3, 6, 140, 2)$.

Consequences

- **Erdős-Selfridge theorem** on equation (1), $(b = 1)$,
- **Erdős-Gy theorem** on equation (2), $(b = k!)$,
- **complete solution** of (3) with $P(b) < p^{(k)}$

Extensions of Theorem C

- to the case $P(b) \leq p^{(k)}$: **Saradha** ($k \geq 9$), **Hanrot, Saradha, Shorey** ($6 \leq k \leq 8$), **Bennett** ($k \leq 5$)
- to the case $P(b) \leq p_k$, p_k is the *k-th prime* ($p_k > p^{(k)}$ if $k > 3$): **Pintér and Gy** ($k \leq 5$)

Conjecture 1 (Pintér and Gy, 2005)

For $k \geq 3$ and $n > 2$, equation (3) has no non-trivial solution with $P(b) \leq p_k$.

More general equations

$$m(m+d)\cdots(m+(k-1)d) = y^n; \qquad (4)$$

$$m(m+d)\cdots(m+(k-1)d) = by^n; \qquad (5)$$

m, k, d, b, y, n positive integers with $k \geq 3$, $n \geq 2$, $\gcd(m, d) = 1$ and $P(b) \leq k$. Assume that $\mathbf{d > 1}$.

1 Finiteness results

Darmon, Granville (1995): for (4), $k \geq 3$, $n \geq 4$

Gy, Hajdu, Saradha (2004): for (5), $k \geq 3$, $n \geq 2$, $k + n > 6$

Tijdeman (1989): $k + n > 6$ necessary

2 Resolution of (4) **and** (5) **for fixed d**

many **deep results: Shorey, Saradha, Tijdeman,**...

Saradha, Shorey (2001, 2005) complete solution of (5) for $k \geq 4$, $1 < d \leq d_0(n)$, n prime, $d_0(n)$ explicitly given for $n = 2, 3, 5, 7$, $n \geq 11$

In what follows, consider equations (4) and (5) for **fixed** k

3 Resolution of (4) and (5) for fixed k

Equation (4):

- *infinitely many solutions* for $k = 2$ and $(k, n) = (3, 2)$
- *no solution for* $(k, n) = (4, 2)$ **(Euler)**, and for $(k, n) = (5, 2), (3, 3), (3, 4)$ and $(3, 5)$ **(Obláth, 1951)**

For **arbitrary** $n > 2$, the first result:

Gy (1999): *if* $k = 3$, $n > 2$ *and* $P(b) \leq 2$, (5) *has no solution*

$\Longrightarrow$ *for* $k = 3$, $n > 2$, (4) *has no solution*

Theorem D (Gy, Hajdu, Saradha, 2004, $4 \leq k \leq 5$; Bennett, Bruin, Gy, Hajdu, 2006, $6 \leq k \leq 11$)

(5) *has no solution for* $3 < k \leq 6$, $P(b) \leq 2$ *and* $6 < k \leq 11$, $P(b) \leq 3$

$\Longrightarrow$ *for* $4 \leq k \leq 11$, (4) *has no solution*

Bennett (2008): for $k = 5, 6$ and $n \geq 7$, the same result with $P(b) \leq 3$

The proofs required different methods according as $n = 2, 3, 5$ or $n \geq 7$. Since 2006, considerable progress has been made.

n=2

Theorem E (Hirata-Kohno, Laishram, Shorey, Tijdeman, 2007; Tengely 2008)

(i) *if* $n = 2$, $d > 1$, $5 \leq k \leq 100$, *then* (5) *has no solution*

(ii) *if* $n = 2$, $k \leq 109$, *then* (4) *has no solution*

n=3

Theorem F (Hajdu, Tengely, Tijdeman, 2009)

(i) *if* $n = 3$, $8 \leq k < 32$, $P(b) < k$, *then* (5) *has no solution*

(ii) *if* $n = 3$, $k < 39$, *then* (4) *has no solution*

n > 3 prime

Theorem G (Gy, Hajdu, Pintér, 2009)

(i) (5) *has no solution if* $n > 3$ *prime and* $12 \leq k \leq 22$, $P(b) \leq 7$ *or* $22 < k \leq 34$, $P(b) \leq \frac{k-1}{2}$

(ii) (4) *has no solution if* $n > 3$ *prime and* $12 \leq k \leq 34$

Theorems D, E, F, G + Gy ($k = 3$) $\Rightarrow$ MAIN RESULT:

Theorem H

Let $3 \leq k \leq 34$.

(i) *if $(k, n) \neq (3, 2)$ and $P(b) \leq 2$, then (5) has no solution*

(ii) *if $(k, n) \neq (3, 2)$, then (4) has no solution*

Remark for $(k, n) = (3, 2)$, $b = 1$ and for $(k, n) = (3, 2), (4, 2)$, $P(b) = 3$, there are infinitely many solutions

Corollary 1 (to Theorem H (ii))

Let $2 \leq k \leq 34$, $n \geq 2$ with $(k, n) \neq (2, 2)$. Then the superelliptic equation

$$x(x+1)\cdots(x+k-1) = w^n$$

in positive **rationals** *x, w has no solution.*

Conjecture 2

(i) *if $(k, n) \neq (3, 2)$ and $P(b) \leq 2$, then (5) has no solution*

(ii) *if $(k, n) \neq (3, 2)$, then (4) has no solution*

For $b = 1$, (ii) is a more precise version of a conjecture of **Erdős**.

For $\mathbf{n} = \mathbf{5}$, a further extension has been recently obtained

Theorem I (Hajdu and Kovács, 2011)

(i) *if* $n = 5$ *and* $3 \leq k \leq 36$, *then equation* (5) *has the only solution* $(m, k, d) = (2, 3, 7)$

(ii) *if* $n = 5$ *and* $3 \leq k \leq 54$, *then equation* (4) *has no solution*

k $\geq$ **3** fixed, **n** $\geq$ **2** prime

$$m(m+d)\dots(m+(k-1)d) = by^n \qquad (5)$$

$$\Updownarrow$$

$$m + id = a_i x_i^n, \; P(a_i) \leq k, \; i = 0, \dots, k-1 \qquad (6)$$

a_i n-th power free, finitely many and effectively determinable such $(a_0, \dots, a_{k-1})$

1. if for some $i, j < k-1$, $P(a_i a_{i+1} \dots a_{i+j}) \leq j+1$ holds, then replace k by $j+1$ in (5)
2. (5) $\Longrightarrow$ generalized Fermat's equations

Possibilities

1 for $p, q, r \geq 0$, $m + pd$, $m + qd$ are $m + rd$ are linearly dependent $\Longrightarrow$

$$AX^n + BY^n = CZ^n \tag{7}$$

with $\gcd(X, Y, Z) = 1$ and $P(ABC) \leq k$.

2 for $p < q \leq r < s \leq k - 1$ with $p + s = q + r$,

$$(m+qd)(m+rd)-(m+pd)(m+sd) = (qr-ps)d^2$$

$$\Longrightarrow AX^n + BY^n = CZ^2 \tag{8}$$

$\gcd(X, Y, Z) = 1$, $P(AB) \leq k$, $|C| \leq (k-1)^2$

X, Y, Z with $XYZ \neq 0, \pm 1$, *non-trivial* solutions

Resolution of equations 4 and 5 (proofs of Theorems D to I)

case n = 2: quadratic residues, reduction to elliptic curves, MAGMA, Chabauty method

case n = 3: Selmer's classical results on equations $AX^3 + BY^3 = CZ^3$, Chabauty method

case n = 5: classical and new results of Dirichlet, Lebesgue, Dénes, Gy, Bennett, Bruin and Hajdu on equations $AX^5 + BY^5 = CZ^5$, genus 2 curves and Chabauty method

case n $\geq$ 7 prime, **main tool**: application of the **modular method** to ternary equations

(7) $AX^n + BY^n = CZ^n$ and (8) $AX^n + BY^n = CZ^2$.

The following **ternary equations** were used in **Gy** (**Gy**, $k = 3$), **Gy, Hajdu, Saradha** (**GyHS**, $4 \leq k \leq 5$), **Bennett, Bruin, Gy, Hajdu** (**BBGyH**, $6 \leq k \leq 11$), **Gy, Hajdu, Pintér** (**GyHP**, $12 \leq k \leq 34$):

$\mathbf{3 \leq k \leq 34}$, in **Gy**, **GyHS**, **BBGyH** and **GyHP**,

$$X^n + Y^n = 2^\alpha Z^n, \quad \alpha \geq 0$$

has no non-trivial solutions ($\alpha = 0$, **Wiles**, $1 \leq \alpha < n$ **Darmon-Merel and Ribet**)

$\mathbf{4 \leq k \leq 34}$, in **GyHS, BBGyH and GyHP** the following results of **Bennett and Skinner (2004)** were used: the equations $X^n + 2^\alpha Y^n = 3^\beta Z^2$, $\alpha \neq 1$; $X^n + Y^n = CZ^2$, $C \in \{2, 6\}$; $X^n + 5^\alpha Y^n = 2Z^2$, $n \geq 11$ if $\alpha > 0$; $AX^n + BY^n = Z^2$, $AB = 2^\alpha p^\beta$, $p \in \{11, 19\}$ have no non-trivial solutions

$\mathbf{6 \le k \le 11}$, in **BBGyH** the authors *proved and utilized* that $X^n + 2^\alpha Y^n = Z^2$ with $p \mid XY$ for $p \in \{3, 5, 7\}$ and five further new ternary equations have no non-trivial solutions.

To extend the results concerning equations (4) and (5) from $k \le 11$ to $12 \le k \le 34$, more than 50 new ternary equations had to be solved in **GyHP**. Denote by $rad(m) = \prod_{p \mid m} p$ the *radical* of m.

GyHP gave explicitly a set $\mathcal{S}$ of 54 pairs (a, b) with $a, b \geq 1$ integers such that *if* $n > 31$ *prime, A, B, C coprime positive integers with $(rad(AB), C) \in \mathcal{S}$ and p a prime such that $11 \leq p \leq 31$ and $p \nmid AB$, then the equation*

$$AX^n + BY^n = CZ^2$$

has no non-trivial solutions X, Y, Z with $p \mid XY$, unless, possibly, for 60 *tuples* $(n, rad(AB), C, p)$ (which are listed explicitly)

For k $\geq$ 12, one of the **main difficulties**: the *number of systems of equations, i.e. the number of* $(a_o, \ldots, a_{k-1})$ *grows so rapidly with* k *that practically it is impossible to handle the different cases as before for* $k \leq 11$

For k $\geq$ 12, fundamentally new ideas were needed: *efficient* and *iterated combination* of our procedure for *solving* the arising *new ternary equations* (corresponding to the pairs in $\mathcal{S}$) with several **sieves** based on the ternary equations already solved. For $n \leq 31$ *local sieves* worked.

Main novelty in the case $\mathbf{k \geq 12}$:

we **algorithmized** our proof $\Longrightarrow$ use of a **computer**. Algorithm works for *larger k* as well, but there are *limits*: computation of modular forms of higher and higher level and computational time itself.

Thank you
for your attention!