Diophantine equations $f(x) = g(y)$ with infinitely many rational solutions x, y

Rob Tijdeman

Leiden University

Joint work with Lajos Hajdu

Specialisation and Effectiveness in Number Theory
Banff, Canada
29 August - 3 September 2022

Main questions

Let $a_0, a_1, \ldots, a_k \in \mathbb{Q}$, distinct, $a_0 \neq 0$. Put

$$f(x) = a_0(x - a_1) \cdots (x - a_k).$$

Let $g(y) \in \mathbb{Q}[y]$.

1. For which f, g does equation

$$f(x) = g(y)$$

have infinitely many rational solutions x, y?

2. What do we know if g has also only simple rational roots?

More precise main question

Equation $f(x) = g(y)$ has infinitely many rational solutions *with a bounded denominator* if there is a $\Delta \in \mathbb{Z}$ such that $f(x) = g(y)$ has infinitely many solutions with $(\Delta x, \Delta y) \in \mathbb{Z}^2$.

For which f, g does the equation $f(x) = g(y)$ have infinitely many solutions $(x, y) \in \mathbb{Q}^2$ with a bounded denominator?

Avanzi and Zannier (2001):
If $f(x) = g(y)$ with $\gcd(\deg(f), \deg(g)) = 1$ and $\deg(f), \deg(g) > 6$ has infinitely many rational solutions, then infinitely many of them have a bounded denominator.

Earlier results (1). The equation

$$x(x+d)\cdots(x+(k-1)d) = by^\ell, k > 2, \ell > 1$$

Siegel (1926): If $\ell > 2$, then only finitely many integral solutions.

Schinzel (1967): If $\ell = 2$, then only finitely many integral solutions.

Erdös and Selfridge (1975): No integral solutions if $d = 1, b = 1$.

Erdös (1951) $k \geq 4$, Györy (1998) $k = 2, 3$:
No integral solutions if $d = 1, b = k!$, except for $\binom{50}{3} = 140^2$.

Euler; (Györy, Hajdu, Saradha, 2004); (Bennett, Bruin, Györy, Hajdu, 2006); (Györy, Hajdu, Pintér, 2009):
No integral solutions if $b = 1, k \leq 34$.

Earlier results (2). The equation

$$(x + d_1 d) \cdots (x + d_k d) = b_0 y^\ell + b_\ell$$

Many results by Saradha, Shorey and coauthors.

(Saradha, Shorey), (Hanrot, Saradha, Shorey), (Bennett), 2001-2004: The only solutions with $d = b_0 = 1, b_\ell = 0$ and only one term is missing from AP are $\frac{4!}{3} = 2^3, \frac{6!}{5} = 12^2, \frac{10!}{7} = 720^2$.

Hajdu and Papp (2020): Only finitely many solutions x, y, ℓ if only one term is missing from a finite AP and $k > 6$.

Question 2.

(Mordell, 1963), (Boyd and Kisilevsky, 1972), (Saradha and Shorey, 1990), Mignotte, Saradha, Shorey (1996), (Hajdu and Pintér, 2000): All solutions are known for the equation
$x(x+1)\cdots(x+k-1) = y(y+1)\cdots(y+\ell-1)$
for $(k,\ell) = (2,3),(3,4),(4,6),\ell/k \in \{2,3,4,5,6\}$.

(Mordell, 1963), (Avanesov, 1966), (Pintér, 1995), (De Weger, 1996), (Stroeker and De Weger, 1999), (Bugeaud, Mignotte), (Stoll and Tengely, 2008), (Blokhuis, Brouwer, De Weger, 2017)
All solutions of $\binom{m}{k} = \binom{n}{\ell}$ are known for
$(k,\ell) = (3,4),(2,3),(2,4),(2,6),(2,8),(3,6),(4,6),(4,8),(2,5)$,
for $m \leq 10^6$ and for binomial coefficient is $< 10^{60}$.

Beukers, Shorey and Tijdeman (1999): The equation
$x(x+d_1)\cdots(x+(k-1)d_1) = y(y+d_2)\cdots(y+(\ell-1)d_2)$
has only finitely many positive integral solutions x, y
except when $(k,\ell) = (2,4)$ and $d_1 = 2d_2^2$. Then
$(y^2+3d_2y)(y^2+3d_2y+2d_2^2) = y(y+d_2)(y+2d_2)(y+3d_2)$.

Preliminaries

We call polynomials $f, f_1 \in \mathbb{Q}[x]$ *similar* if there exist $a, b \in \mathbb{Q}$, $a \neq 0$ such that $f(x) = f_1(ax + b)$. Notation $f \simeq f_1$.
This induces an equivalence relation in $\mathbb{Q}[x]$.
If f has only simple rational roots, then f_1 has only simple rational roots; in every such equivalence class there is a polynomial with integer roots.
Similar f, f_1 represent the same rational numbers for rational x's.

If $f \simeq f_1$ and $g \simeq g_1$, then we call the equations $f(x) = g(y)$ and $f_1(x) = g_1(y)$ *equivalent*.
It suffices to study a representative from each class of equations.

Let $\varphi(x) \in \mathbb{Q}[x]$.
Then every solution of $f(x) = g(y)$ is a solution of $\varphi(f(x)) = \varphi(g(y))$.

The Bilu-Tichy Theorem

Theorem (Bilu, Tichy, 2000)

Let $f(x), g(x) \in \mathbb{Q}[x]$ be non-constant polynomials. Then the following two statements are equivalent.

(I) *The equation $f(x) = g(y)$ has infinitely many rational solutions x, y with a bounded denominator.*

(II) *We have $f = \varphi(F(\kappa))$ and $g = \varphi(G(\lambda))$, where $\kappa(x), \lambda(x) \in \mathbb{Q}[x]$ are linear polynomials, $\varphi(x) \in \mathbb{Q}[x]$, and $F(x), G(x)$ form a* standard pair *over $\mathbb{Q}$ such that the equation $F(x) = G(y)$ has infinitely many rational solutions with a bounded denominator.*

Note that $F(\kappa) \sim F, G(\lambda) \sim G$. (We often identify them.)
(II) implies (I) is trivial.
Notation: $k = \deg(f), \ell = \deg(g), m = \deg(F), n = \deg(G), t = \deg(\varphi)$.
Therefore $k = mt, \ell = nt$.

There are five kinds of (unordered) standard pairs.

Standard pairs

Kind	Standard pair (F, G unordered)	Parameter restrictions
First	$(x^q, ax^p v(x)^q)$	$0 \leq p < q$, $(p,q) = 1$, $p + \deg(v) > 0$
Second	$(x^2, (ax^2 + b)v(x)^2)$	-
Third	$(D_m(x, a^n), D_n(x, a^m))$	$\gcd(m, n) = 1$
Fourth	$(a^{-m/2} D_m(x, a), -b^{-n/2} D_n(x, b))$	$\gcd(m, n) = 2$
Fifth	$((ax^2 - 1)^3, 3x^4 - 4x^3)$	-

Standard pairs. Here
a, b are non-zero rational numbers,
m, n, q are positive integers,
p is a non-negative integer,
$v(x) \in \mathbb{Q}[x]$ is a non-zero, but possibly constant polynomial.
$D_m(x, b)$ is a *Dickson polynomial*.

Dickson polynomials

Let b be a non-zero rational number and m be a positive integer. Then the m-th *Dickson polynomial* is defined by

$$D_m(x,b) := \sum_{i=0}^{\lfloor m/2 \rfloor} d_{m,i} x^{m-2i} \quad \text{where } d_{m,i} = \frac{m}{m-i}\binom{m-i}{i}(-b)^i.$$

Some properties are:

$D_m(x,b) = xD_{m-1}(x,b) - bD_{m-2}(x.b)$,

$D_m(x + \frac{b}{x}, b) = x^m + \left(\frac{b}{x}\right)^m$,

$D_{mn}(x,b) = D_m(D_n(x,b), b^n) = D_n(D_m(x,b), b^m)$,

$\sum_{m=0}^{\infty} D_m(x,b)z^m = (2 - xz)/(1 - xz + bz^2)$,

$D_m(2x,1) = 2T_m(x)$, where $T_m(x) = \cos(m \arccos x)$.

Earlier applications of the Bilu-Tichy theorem

Kulkarni and Sury (2003): The number of solutions of the equation $(x+1)(x+2)\cdots(x+k) = g(y)$ is finite with exception of three explicitly given classes in which there can be infinitely many solutions.

Hajdu, Papp and Tijdeman (2022): The number of solutions of the equation $(x+d_1d)\cdots(x+d_kd) = g(y)$, for $g(y) \in \mathbb{Q}[y]$ of degree $\ell \geq 2$ and $d, k, K, d_1, d_2, \ldots, d_k \in \mathbb{Z}$ with $0 \leq d_1 < d_2 < \cdots < d_k < K$, $k > 2$, is finite under the assumption that $K - k \leq cK^{2/3}$ with c an explicit constant, provided that g does not belong to two explicitly given classes in which there can be infinitely many solutions.

Standard pairs of the fifth kind

A standard pair of the fifth kind is $(F, G) = ((\alpha x^2 - 1)^3, 3x^4 - 4x^3)$.

Suppose f has only simple rational roots.

Then f' has only simple real roots.

Since $f = \varphi(F)$ we have $f' = \varphi'(F) \cdot F'$.

Therefore F' has only simple real roots.

This is not the case for standard pairs of the fifth kind.

Thus we can exclude the standard pairs of the fifth kind.

Standard pairs of the third and fourth kind

Third kind: $(F(x), G(x)) = (D_m(x, a^n), D_n(x, a^m))$ and $\gcd(m, n) = 1$.
Fourth kind: $(F(x), G(x)) = (a^{-m/2} D_m(x, a), -b^{-n/2} D_n(x, b))$ and $\gcd(m, n) = 2$ and an extra condition.

Crucial relation: $D_{mn}(x, b) = D_m(D_n(x, b), b^n) = D_n(D_m(x, b), b^m)$.

Therefore, for $F(x) = D_m(x, b^n)$, $G(x) = D_n(x, b^m)$ the equation $F(x) = G(y)$ has infinitely many solutions $(x, y) = (D_n(z, b), D_m(z, b))$.

Questions:
When does $\varphi(cD_m(x, b) + d)$ have simple rational roots?

For $t = 1$ (i.e. $\deg(\varphi) = 1$):
When does $cD_m(x, b) + d$ have simple rational roots?
We can take $c = 1$.

Question for $t = 1$

Theorem

Assume that with some rational numbers u, b with $ub \neq 0$ we have

$$D_m(x, b) + u = (x - w_1) \cdots (x - w_m), \tag{1}$$

where $D_m(x, b)$ is the m-th Dickson polynomial with parameter b and $w_1, \ldots, w_m \in \mathbb{Q}$ are distinct. Then $m \in \{1, 2, 3, 4, 6\}$.

Theorem

Let $m \in \{3, 4, 6\}$. For any $w_1, w_2 \in \mathbb{Q}$ we can define $w_3, \ldots, w_m, b, u \in \mathbb{Q}$ such that (1) *holds. On the other hand, this provides the only solutions of equation* (1).

Conclusion for the third and fourth kind

$m = \deg(F), n = \deg(G), t = \deg\varphi, \deg(f) = mt, \deg(g) = nt.$

Theorem

Standard pairs of the third kind:
Then $m \in \{1,2,3,4,6\}$ or $n \in \{1,2\}$.
Here m and n should be coprime and every t is possible.

Standard pairs of the fourth kind:
Then $m \in \{2,4,6\}$ or $n = 2$.
Here $\gcd(m,n) = 2$ and every t is possible.

Theorem

There are no solutions if both f and g have only simple rational roots.

PTE-sets

Suppose $f(x) = \varphi(F(x)) = (F(x) - p_1)\cdots(F(x) - p_t)$ has only single integral roots.
Then $p_1, p_2, \ldots, p_t$ are distinct.
We call such sets $F(x) - p_i \ \ (i = 1, 2, \ldots, t)$ with only simple integral roots PTE-sets.

$t = 2$: 'ideal Prouhet-Tarry-Escott pairs'.
Known to exist for $m \leq 12, m \neq 11$. Open problem.

Theorem

For $m = \deg(F) \in \{2, 3, 4, 6\}$ there exist PTE-sets for any $t \in \mathbb{Z}_{>0}$.

PTE-sets are useful to construct equations $f(x) = g(y)$ with infinitely many integer solutions with f, g having only simple integral roots.

PTE's of degree 6

Lemma. *Let N be the product of r primes of the form* $\equiv 1 \pmod 6$. *Then N can be written as* $x^2 + xy + y^2$ *for positive integers* x, y *in* 2^r *ways.*

We take $(r = 3): \quad 7 \cdot 13 \cdot 19 = 1729 = x^2 + xy + y^2$ for $(x, y) = (40, 3), (37, 8), (32, 15), (25, 23)$.

Hence $G(y) = y^6 - 2 \cdot 1729 y^4 + 1729^2 y^2$ has simple rational roots when 26625600, 177422400, 508953600 or 761760000 is subtracted, since the corresponding polynomials equal

$$(y^2 - 40^2)(y^2 - 3^2)(y^2 - 43^2), (y^2 - 37^2)(y^2 - 8^2)(y^2 - 45^2),$$

$$(y^2 - 32^2)(y^2 - 15^2)(y^2 - 47^2), (y^2 - 25^2)(y^2 - 23^2)(y^2 - 48^2).$$

A PTE-quadruple of degree 6.

Standard pairs of the first or second kind

$(F(x), G(x))$ or $(G(x), F(x)) =$

First kind: $(x^q, ax^p v(x)^q)$ with $0 \leq p < q$, $(p, q) = 1$ and $p + \deg(v) > 0$.

Second kind: $(x^2, (ax^2 + b)v(x)^2)$.

If $q > 2$, then $x^q + d$ cannot have simple roots.
Thus $\deg(F) \leq 2$ or $\deg(G) \leq 2$.

It follows that $\deg(f) \mid 2\deg(g)$ or $\deg(g) \mid 2\deg(f)$.

If $F(x) = x$, then $F(x) = G(y)$ has trivial solutions $(x, y) = (G(y), y)$.
Same if $\deg(G) = 1$.

In case of the second kind a Pell equation plays a role.

An example of the first kind

Let $f(x) = (x^2 - (249 \cdot 1591 \cdot 1840)^2)(x^2 - (656 \cdot 1305 \cdot 1961)^2)$ and $g(y)) =$
$(y - 249^2)(y - 1591^2)(y - 1840^2)(y - 656^2)(y - 1305^2)(y - 1961^2)$.

The equation $f(x) = g(y)$ has infinitely many integral solutions $(x, y) = (a(a^2 - 1729), a^2)$ for $a \in \mathbb{Z}$.

Observe that here both f and g have simple integral roots.

Here $F(x) = x^2, G(y) = y(y - 1729)^2$, $t = 2$ and $\varphi(z) = (z - (249 \cdot 1591 \cdot 1840)^2)(z - (656 \cdot 1305 \cdot 1961)^2)$.

(40,3), (37,8) satisfy $x^2 + xy + y^2 = 1729$.
We considered triples (40, 3, -43), (37, 8, -45)
$43^2 - 40^2 = 249, 40^2 - 3^2 = 1591, 43^2 - 3^2 = 1840.$

An example of the second kind

Consider the Pell equation $x^2 = 2y^2 - 1$ with solutions $(1,1),(7,5),(41,29),\ldots$. Take $t = 3$,

$$F(x) = x^2, \;\; G(y) = 2y^2 - 1, \;\; \varphi(z) = (z - 1^2)(z - 7^2)(z - 41^2).$$

Then we have

$$f(x) = (x^2 - 1^2)(x^2 - 7^2)(x^2 - 41^2), \;\; g(y) = 2^3(y^2 - 1^2)(y^2 - 5^2)(y^2 - 29^2).$$

So $f(x)$ and $g(y)$ both have simple integral roots.
Further, every solution of $x^2 = 2y^2 - 1$ is a solution of $f(x) = g(y)$.
Here t can be chosen arbitrarily.

Application

Theorem

For every positive integer N there exist only finitely many pairs of disjoint blocks A and B of size at most N with the property that for some k, ℓ with $1 \le k < \ell$ and $k \nmid 2\ell$, there exist distinct elements $a_1, \ldots, a_k \in A$ and distinct elements $b_1, \ldots, b_\ell \in B$ such that $a_1 \cdots a_k = b_1 \cdots b_\ell$.

Example with $k \nmid \ell$. Recall example of the first kind.
$f(x) = (x^2 - (249 \cdot 1591 \cdot 1840)^2)(x^2 - (656 \cdot 1305 \cdot 1961)^2)$ and
$g(y)) =$
$(y - 249^2)(y - 1591^2)(y - 1840^2)(y - 656^2)(y - 1305^2)(y - 1961^2)$.
The equation $f(x) = g(y)$ has infinitely many integral solutions $(x, y) = (a(a^2 - 1729), a^2)$ for $a \in \mathbb{Z}$. Let $N = 2 \cdot 656 \cdot 1305 \cdot 1961$.

For any x the numbers $x \pm 249 \cdot 1591 \cdot 1840$ and $x \pm 656 \cdot 1305 \cdot 1961$ are in an interval of length N and so do, for any y, the numbers $y - 249^2, y - 1591^2, y - 1840^2, y - 656^2, y - 1305^2, y - 1961^2$.

Literature

R.M. Avanzi, U.M. Zannier, Acta Arith. **99** (2001), 227-256.

F. Beukers, T.N. Shorey, R. Tijdeman, Number Theory in Progress, de Gruyter, 1999, pp. 11- 26.

Yu. Bilu, R. Tichy, Acta Arith. **95** (2000), 261-288.

L. Hajdu, Á. Papp, Monatsh. Math. **193** (2020), 637-655, **195** (2021), 377.

L. Hajdu, Á. Papp, R. Tijdeman, Ramanujan J. **58** (2022), 1075-1093.

L. Hajdu, R. Tijdeman, The Diophantine equation $f(x) = g(y)$ for polynomials with simple rational roots, in preparation.

L. Hajdu, R. Tijdeman, N. Varga, Diophantine equations for Littlewood polynomials, in preparation.