Recent results on the geometry of numbers

Lorenzo Sauras-Altuzarra

25th Central European Number Theory Conference, Sopron, 2023

TECHNISCHE UNIVERSITÄT WIEN
Vienna University of Technology

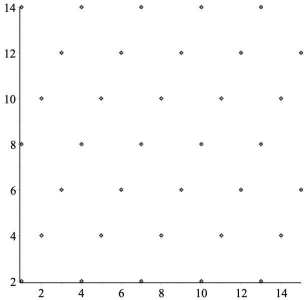
The Pillai equation

- Consider integers $a > 1$, $b > 1$ and $c \neq 0$.
- The associated **Pillai equation** is the Diophantine equation $a^x - b^y = c$.
- **Theorem (G. Pólya, 1918)**:

  the Pillai equation has only finitely many solutions on the positive integers.
- Let $\mathcal{D}(a,b) = \{(x,y) \in \mathbb{Q}^2_{\geq 0} : \exists k \in \mathbb{Z}\ a^x - b^y = (ab+1)k\}$.
- Note that $\mathcal{D}(a,b) = \left\{(x,y) \in \mathbb{Q}^2_{\geq 0} : \dfrac{a^x - b^y}{ab+1} \in \mathbb{Z}\right\}$.

The Pillai equation

- For example, $\mathcal{D}(2,3) = \mathbb{Q}^2_{\geq 0} \cap \left(\begin{bmatrix} 1 \\ 2 \end{bmatrix} + \left\langle \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} -2 \\ 2 \end{bmatrix} \right\rangle_{\mathbb{Z}} \right)$.



In particular, $\dfrac{2^{11} - 3^4}{2 \cdot 3 + 1} = 281$ and $\begin{bmatrix} 11 \\ 4 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \end{bmatrix} + 4 \begin{bmatrix} 1 \\ 2 \end{bmatrix} - 3 \begin{bmatrix} -2 \\ 2 \end{bmatrix}$.

- **Conjecture (2023)**: $\mathcal{D}(a,b)$ is the first quadrant of some shifted point-lattice.

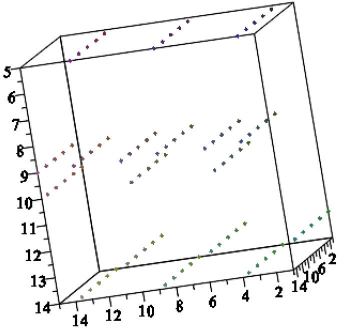
- Let $\mathcal{C}(a,b) = \left\{ (x,y) \in \mathbb{Q}^2_{\geq 0} : \dfrac{a^x + b^y}{ab+1} \in \mathbb{Z} \right\}$ (the **cover** of a and b).
- **Conjecture (2022)**: $\mathcal{C}(a,b)$ is also the first quadrant of some shifted point-lattice.
- **Theorem (R. Schoof, pers. comm., 2023)**:

  $\mathcal{C}(a,b)$ is an infinite set (in particular, it is not empty).

Towards a general statement

- We can consider further generalizations:

for example, a subset of $\left\{(x, y, z) \in \mathbb{Q}^3_{\geq 0} : \dfrac{2^x + 3^y + 5^z}{2 \cdot 3 \cdot 5 + 1} \in \mathbb{Z}\right\}$ looks as follows.



Towards a general statement

- Consider a point A of $\mathbb{Z}^n$.

- **Problem (2023)**: when does a set of the form

$$\left\{ P \in \mathbb{Q}^n_{\geq 0} : \frac{\pm A_1^{P_1} \pm A_2^{P_2} \pm \ldots \pm A_n^{P_n}}{A_1 A_2 \ldots A_n \pm 1} \in \mathbb{Z} \right\},$$

  where the '$\pm$' signs are independent,

  equal the first orthant of some shifted point-lattice?

Application: Fermat numbers

- Now, consider also integers $f > 1$, $m > 1$ and $n > 2$; and let $\alpha(n) = 2^{n-1}/(n+2)$.
- The n-th **Fermat number** is $2^{2^n} + 1$.
- **Theorem (É. Lucas, 1878)**: If f divides $2^{2^n} + 1$, then $\dfrac{f-1}{2^{n+2}} \in \mathbb{Z}$.
- **Theorem (M. Baaz, 1999)**:

  if $m2^{n+2} + 1 = m^{2r} + 2^{2^n - 2r(n+2)}$, for some integer $r \leq \lfloor \alpha(n) \rfloor$,

  then $m2^{n+2} + 1$ divides $2^{2^n} + 1$.
- For example, if $m = n = 5$, then, by setting $r = 2$,

  $5 \cdot 2^7 + 1 = 5^4 + 2^4$, $2 = \lfloor \alpha(5) \rfloor$ and $5 \cdot 2^7 + 1 \mid 2^{2^5} + 1$.

- **Theorem (2022) (geometric characterization of the factors of Fermat numbers)**:

  $m2^{n+2}+1$ divides $2^{2^n}+1$ if and only if

  $$\mathbb{Q}^2_{\geq 0} \cap \left(\begin{bmatrix} 1 \\ -1 \end{bmatrix} + \left\langle \begin{bmatrix} -2 \\ 2 \end{bmatrix}, \begin{bmatrix} 2\lfloor \alpha(n) \rfloor - 1 \\ 2\alpha(n) - 2\lfloor \alpha(n) \rfloor + 1 \end{bmatrix} \right\rangle_{\mathbb{Z}} \right) \subseteq \mathcal{C}(m, 2^{n+2}).$$

- For example, $\mathbb{Q}^2_{\geq 0} \cap \left(\begin{bmatrix} 1 \\ -1 \end{bmatrix} + \left\langle \begin{bmatrix} -2 \\ 2 \end{bmatrix}, \begin{bmatrix} 3 \\ 11/7 \end{bmatrix} \right\rangle_{\mathbb{Z}} \right) \subseteq \mathcal{C}(5, 2^7)$.

  In particular, $(0, 32/7) \in \mathcal{C}(5, 2^7)$; i.e. $\dfrac{(5)^0 + (2^7)^{32/7}}{5 \cdot 2^7 + 1} = \dfrac{2^{2^5}+1}{5 \cdot 2^7 + 1} \in \mathbb{Z}$.

Additional result: generalized Fermat numbers

- Consider, in addition, integers $g > 1$ and $j > 0$.
- Recall that ν_2 denotes the dyadic valuation.
- The n-th **generalized Fermat number**, with respect to g, is $g^{2^n} + 1$.
- **Theorem (with J. Wang, 2022)**:

  if f divides $2^{2^n} + 1$, then f also divides $\left(\left(\frac{f-1}{2^{n+2}}\right)^{2j-1}\right)^{2^{n-\nu_2(n+2)}} + 1.$

- For example, $5 \cdot 2^7 + 1$ divides both $2^{2^5} + 1$ and $(5^{2j-1})^{2^5} + 1$.