New results and questions on the geometry of numbers

Lorenzo Sauras-Altuzarra

Fermat numbers

Fermat

- Let n be an integer exceeding one.
- The n-th **Fermat number** is $2^{2^n} + 1$.
- For example:
  - $2^{2^2} + 1 = 17$.
  - $2^{2^3} + 1 = 257$.
  - $2^{2^4} + 1 = 65537$.
  - $2^{2^5} + 1 = 4294967297$.
  - $2^{2^6} + 1 = 18446744073709551617$.
  - $2^{2^7} + 1 = 340282366920938463463374607431768211457$.

Factorization of Fermat numbers

Goldbach

Lenstra

- Fermat numbers are so large, that it is a mathematical and computational challenge to find their factors.
- Currently, only $2^{2^2}+1$, ..., $2^{2^{11}}+1$ are fully factored.
- For example, $2^{2^5}+1 = 641 \cdot 6700417$.
- Finding a new factor of some Fermat number is big news. At the present time, only 370 factors of Fermat numbers are known.
- **Theorem (Goldbach)**: Fermat numbers are pairwise coprime (in other words, Fermat numbers do not share factors with each other).
- The main procedure to find factors of Fermat numbers is **Lenstra's Elliptic Curve Method**.

The problem for my doctoral thesis

Euler

Lucas

- **Theorem (Euler & Lucas)**: the factors of the n-th Fermat number have the form $m2^{n+2}+1$.
- For example, $641 = 5 \cdot 2^{5+2}+1 \mid 2^{2^{\mathbf{5}}}+1$.
- So let m be an integer exceeding one.
- **Main problem**: when does $m2^{n+2}+1$ factor the n-th Fermat number?
- In order to tackle this problem, it is essential to analyze concrete proofs of divisibility (e.g. proofs of the fact that $5 \cdot 2^{5+2}+1 \mid 2^{2^{\mathbf{5}}}+1$ or $1071 \cdot 2^{6+2}+1 \mid 2^{2^{\mathbf{6}}}+1$).

A sufficient condition

Baaz

Kraïtchik

- **Theorem (Baaz)**: a sufficient condition for the main problem is

$$m2^{n+2}+1=m^{2r}+2^{2^n-2r(n+2)}$$

  for some non-negative integer r.
- This result was obtained by applying **Baaz's generalization method**, a new technique on extractive proof theory, to a proof by Kraïtchik of the fact that $5\cdot 2^{5+2}+1$ factors $2^{2^{\mathbf{5}}}+1$.

A necessary condition

- **Observation**: $1071^{2\cdot 4} + 2^{2^{\mathbf{6}} - 2\cdot 4\cdot(6+2)} = 1071^{2^{\mathbf{3}}} + 1$.
- The **dyadic valuation** of a given number, which is denoted by ν_2, is the exponent of two in its prime factorization.
- For example, $\nu_2(12) = \nu_2(2^2 \cdot 3) = 2$.
- **Theorem (with Wang)**: a necessary condition for the main problem is

$$m2^{n+2} + 1 \mid \left(m^{2j-1}\right)^{2^{n-\nu_{\mathbf{2}}(n+\mathbf{2})}} + 1$$

  for any positive integer j.
- For example, $5 \cdot 2^7 + 1$ factors $(5^{2j-1})^{2^{\mathbf{5}}} + 1$ for any positive integer j.
- We have more related results in preparation (some ones are already proved and other ones are yet conjectural), and we are trying to unify them in a single general statement.

Another necessary condition

- **Theorem (with Wang)**: a necessary condition for the main problem, provided that $m2^{n+2}+1$ is prime, is

$$\begin{cases} (bc-ad)^2 = 1 \\ c^2+d^2 = m2^{n+2}+1 \\ c^2+d^2 = 2^{2^n} - (ac+bd)^2 \end{cases}$$

  for some integers a, b, c, d.
- For example,

$$\begin{cases} (1\cdot 25 - 6\cdot 4)^2 = 1 \\ 25^2+4^2 = 5\cdot 2^{5+2}+1 \\ 25^2+4^2 = 2^{2^{\mathbf{5}}} - (6\cdot 25 + 1\cdot 4)^2 \end{cases}.$$

- This result was obtained by applying Baaz's generalization method to a proof of the fact that $1071\cdot 2^{6+2}+1$ factors $2^{2^{\mathbf{6}}}+1$, due to the participant of the Mersenne Forum whose nickname was Literka.

A first result of geometric nature

Brînzănescu

Harcos

- The **special linear group**, which is denoted by $\mathrm{SL}(2,\mathbb{Z})$, is the group of square matrices of order two, integer entries and determinant one.
- **Observation (Brînzănescu)**: the first condition from the previous theorem resembles the definition of the special linear group.
- A **Gaussian integer** is a complex number whose real and imaginary parts are both integers.
- **Theorem (with Harcos)**: a prime p divides m^2+1 if and only if there exist Gaussian integers u and v such that $v\bar{v} = p \mid m^2 - \Re(uv)^2$ and

$$\begin{bmatrix} \Im(u) & \Re(u) \\ -\Im(v) & \Re(v) \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Z}).$$

A more general sufficient condition

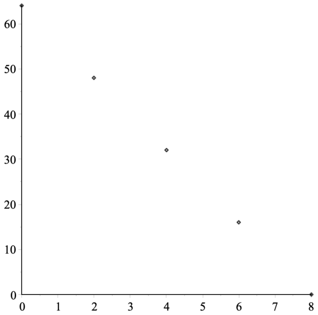
Bennett

- **Theorem**: a sufficient condition for the main problem is

$$m2^{n+2} + 1 \mid m^{2r} + 2^{2^n - 2r(n+2)}$$

  for some non-negative integer r.
- This result was obtained by applying Baaz's generalization method to another proof of the fact that $5 \cdot 2^{5+2} + 1$ factors $2^{2^{\mathbf{5}}} + 1$, due to Bennet & Kraïtchik.

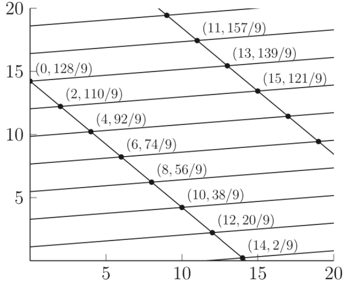
- **Observation**: the pairs of exponents from Baaz's result $(2r, 2^n - 2r(n+2))$ are collinear, see for example $\{(2r, 2^n - 2r(n+2))\}_{r=0}^{4}$.



- The **cover** of two integers a and b exceeding one, which is denoted by $\mathcal{C}(a, b)$, is the set

$$\left\{(x, y) \in \mathbb{Q}^2_{\geq 0} : \frac{a^x + b^y}{ab + 1} \in \mathbb{Z}\right\}.$$

- A (bi-dimensional) **point-lattice** is a set of the form $\langle \vec{u}, \vec{v} \rangle_{\mathbb{Z}}$ (i.e. of the form $\{i\vec{u} + j\vec{v} : i, j \in \mathbb{Z}\}$), where $(\vec{u}, \vec{v})$ is a $\mathbb{Q}$-basis of the vector space $\mathbb{Q}^2$.
- **Conjecture**: every cover is the first quadrant of a shifted point-lattice.
- For example, take a look to this subset of $\mathcal{C}(116503103764643, 2^{7+2})$.



Some partial answers for the conjecture on covers

Schoof

Sarkar

Tichy

- Thanks to an anonymous referee, we knew that covers were infinite as long as they were non-empty.
- **Euler's totient function**, which is denoted by φ, gives the number of smaller positive integers that are coprime with a given positive integer.
- For example, $\varphi(8) = 4$ because the smaller positive integers that are coprime with 8 are 1, 3, 5 and 7.
- **Theorem (Schoof)**: if a and b are any two integers exceeding one, then

$$\left(\begin{bmatrix} 1 \\ -1 \end{bmatrix} + \left\langle \begin{bmatrix} -2 \\ 2 \end{bmatrix}, \begin{bmatrix} \varphi(ab+1) \\ 0 \end{bmatrix} \right\rangle_{\mathbb{Z}} \right) \cap \mathbb{Q}^2_{\geq 0} \subseteq \mathcal{C}(a, b).$$

- In particular, Schoof's result shows that covers are non-empty.
- Another interesting (but more technical) partial answer was obtained by Sarkar.
- Tichy posed several concrete questions on Schoof's lattice whose resolution might approach us to the proof of the conjecture.

- **Theorem**: a necessary and sufficient condition for the main problem is

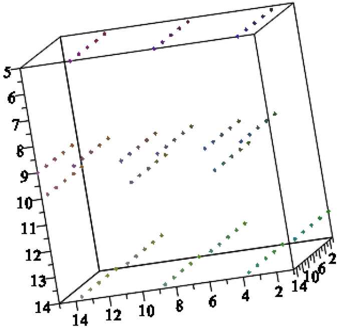
$$\mathbb{Q}^2_{\geq 0} \cap \left(\begin{bmatrix} 1 \\ -1 \end{bmatrix} + \left\langle \begin{bmatrix} -2 \\ 2 \end{bmatrix}, \begin{bmatrix} 2\lfloor \alpha(n) \rfloor - 1 \\ 2\alpha(n) - 2\lfloor \alpha(n) \rfloor + 1 \end{bmatrix} \right\rangle_{\mathbb{Z}} \right) \subseteq \mathcal{C}(m, 2^{n+2})$$

where $\alpha(n) = 2^{n-1}/(n+2)$.

- 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. $\dfrac{(5)^0 + (2^7)^{32/7}}{5 \cdot 2^7 + 1} = \dfrac{2^{2^5} + 1}{5 \cdot 2^7 + 1} \in \mathbb{Z}$.

- **Observation**: for other numbers of dimensions there are also interesting patterns: for example, a subset of $\left\{(x, y, z) \in \mathbb{Q}^3_{\geq 0} : \frac{2^x + 3^y + 5^z}{2 \cdot 3 \cdot 5 + 1} \in \mathbb{Z}\right\}$ looks as follows.



A connection with another theory

Parisse

Pillai

- **Observation (Parisse)**: the definition of cover resembles the **Pillai equation** (i.e. the Diophantine equation $a^x - b^y = c$).
- And indeed, we have for instance that

$$\left\{(x,y) \in \mathbb{Q}^2_{\geq 0} : \frac{2^x - 3^y}{2 \cdot 3 + 1} \in \mathbb{Z}\right\} = \mathbb{Q}^2_{\geq 0} \cap \left(\begin{bmatrix} 1 \\ 2 \end{bmatrix} + \left\langle \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} -2 \\ 2 \end{bmatrix} \right\rangle_{\mathbb{Z}} \right).$$

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

Towards a general statement

- **Problem**: given a point A of $\mathbb{Z}^n_{>1}$, 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?