On prime numbers of the form $2^n \pm k$

José Manuel Rodríguez Caballero

Université du Québec à Montréal, Montréal, QC, Canada
rodriguez_caballero.jose_manuel@uqam.ca

Abstract. Consider the set $K$ of integers $k$ for which there are infinitely many primes $p$ such that $p + k$ is a power of 2. The aim of this paper is to show a relationship between $K$ and the limits points of some set rational numbers related to a sequence of polynomials $C_n(q)$ introduced by Kassel and Reutenauer [2].

Keywords: Fermat primes, Mersenne primes, ideals, finite fields, local zeta function.

1 Introduction

Consider the group algebra $\mathbb{F}_q [\mathbb{Z} \oplus \mathbb{Z}]$, where $\mathbb{Z} \oplus \mathbb{Z}$ is the free abelian group of rank 2. An ideal $I$ of $\mathbb{F}_q [\mathbb{Z} \oplus \mathbb{Z}]$ is said of codimension $n$ if $\mathbb{F}_q [\mathbb{Z} \oplus \mathbb{Z}] / I$ is an $n$-dimensional vector space over $\mathbb{F}_q$. The ideals of codimension $n$ of $\mathbb{F}_q [\mathbb{Z} \oplus \mathbb{Z}]$ are the $\mathbb{F}_q$-points of the Hilbert scheme $H^n := \text{Hilb}^n \left( \mathbb{A}^1_{\mathbb{F}_q} \setminus \{0\} \times \mathbb{A}^1_{\mathbb{F}_q} \setminus \{0\} \right)$ of $n$ points on the two-dimensional torus (i.e., of the affine plane minus two distinct straight lines). Let $Z_{H^n / \mathbb{F}_q}(t)$ be the local zeta function of $H^n$. The evaluation at $t = 0$ of the logarithmic derivative of $Z_{H^n / \mathbb{F}_q}(t)$ will be denoted $C_n(q)$. From a combinatorial point of view, $C_n(q)$ counts the ideals of $\mathbb{F}_q [\mathbb{Z} \oplus \mathbb{Z}]$ having codimension $n$.

Kassel and Reutenauer obtained an explicit expression for $C_n(q)$ in terms of the partitions of $n$ (see [2]) and in terms of the divisors of $n$ (see [3]). Furthermore, using the generating function

$$\prod_{m \geq 1} \frac{(1 - t^m)^2}{(1 - q^m)(1 - q^{-1}t^m)} = 1 + \sum_{n \geq 1} \frac{C_n(q)}{q^n} t^n,$$

a connection between $C_n(q)$ and modular forms was given in [4].

For any prime power $q$, consider the set of rational numbers $\Omega_q := \left\{ \frac{C_n(q)}{q^n} : n \in \Phi \right\}$, where $\Phi := \left\{ 2^h p : h \geq 0 \text{ and } p \text{ odd prime} \right\}$. Our main result is the following theorem.

Let $K$ be the set of $k \in \mathbb{Z}$ for which there are infinitely many prime numbers $p$ such that $p + k$ is a power of 2. For any prime power $q$, define the set $\Omega_q$.
\[ K_q := \left\{ \text{sign}(k) \frac{(q - 1)(q^{|k|} - 1)}{q^{|k|+1}/2} : \ k \in K \right\} \cup \{-\infty, +\infty\}, \]

where sign(k) is the sign of k, i.e. sign(k) = 1 if k > 0, sign(k) = -1 if k < 0 and sign(k) = 0 for k = 0. The aim of this paper is to prove the following result.

**Theorem 1.** For any prime power q, the set of limit points of \( \Omega_q \) is \( K_q \).

## 2 Proof of the main result

Given an integer \( k \geq 1 \), define the set

\[ E_k := \left\{ \frac{p(p + k)}{2} : \ p \ \text{odd prime and} \ p + k \ \text{power of} \ 2 \right\} \cap \mathbb{Z}. \]

Define the arithmetical functions \( \psi(n) \) and \( \beta(n) \) considering two cases according to the existence or not of a nontrivial odd divisor of \( n \). If \( n \) is a power of \( 2 \), then \( \psi(n) := 0 \) and \( \beta(n) := -n \). If \( n = 2^h p_1 p_2 ... p_r \), with \( p_1 \leq p_2 \leq ... \leq p_r \) odd primes and \( r \geq 1 \), then

\[ \psi(n) := \min \left\{ 2^{h+1}, p_1 \right\}, \]
\[ \beta(n) := \frac{1}{2} \left( \frac{2n}{\psi(n)} - \psi(n) - 1 \right). \]

**Lemma 2.** For all \( n \in E_k \),

\[ \beta(n) = \frac{|k| - 1}{2}, \]
\[ (-1)^{2n/\psi(n)} = \text{sign}(k). \]

**Proof.** Take \( n \in E_k \). By definition, \( 2n = p(p + k) \), where \( p \) is an odd prime number and \( p + k = 2^h \) with \( h \geq 1 \) (the case \( h = 0 \) is excluded in virtue of the inclusion \( E_k \subseteq \mathbb{Z} \)). Notice that we cannot have \( k = 0 \), because \( p \) is an odd prime.

Suppose that \( k > 0 \). It follows that \( \psi(n) = p \). So, \( (-1)^{2n/\psi(n)} = (-1)^{p+k} = 1 \).

Furthermore,

\[ \beta(n) = \frac{1}{2} \left( \frac{2n}{p} - p - 1 \right) = \frac{1}{2} ((p + k) - p - 1) = \frac{k - 1}{2}. \]

Suppose that \( k < 0 \). It follows that \( \psi(n) = p + k \). So, \( (-1)^{2n/\psi(n)} = (-1)^{p} = -1 \). Furthermore,

\[ \beta(n) = \frac{1}{2} \left( \frac{2n}{p + k} - (p + k) - 1 \right) = \frac{1}{2} (p - (p + k) - 1) = \frac{(-k) - 1}{2}. \]

The equalities (1) and (2) follows. \( \square \)
We will use the following result due to Kassel and Reutenauer (Theorem 1.1 in [3]).

**Theorem 3.** The polynomial $C_n(q)$ can be expanded as follows,

$$C_n(q) = c_{n,0} q^n + \sum_{i=1}^{n} c_{n,i} \left(q^{n+i} + q^{n-i}\right),$$

where the coefficients $c_{n,i}$ satisfy

$$c_{n,0} = \begin{cases} 2 (-1)^r & \text{if } n = \frac{r(r+1)}{2}, \\ 0 & \text{otherwise}, \end{cases}$$

$$c_{n,i} = \begin{cases} (-1)^r & \text{if } n = \frac{r(r+2i+1)}{2}, \\ (-1)^{r-1} & \text{if } n = \frac{r(r+2i-1)}{2}, \\ 0 & \text{otherwise}, \end{cases}$$

where $r \geq 1$ and $i \geq 1$ are integers.

**Proof.** The proof can be found in page 10 in [3].

The following lemma is equivalent to identity (9.2) in [1].

**Lemma 4.** For any integer $n \geq 1$,

$$\frac{C_n(q)}{q^n} = \left(1 - \frac{1}{q}\right) \sum_r (-1)^{r-1} q^{2n/r-r-1}/q^{r-2n/r-1}/2,$$

where $r$ runs over the odd divisors of $2n$.

**Proof.** Using by Theorem 3 we can express $\frac{C_n(q)}{q^n}$ as follows,

$$\frac{C_n(q)}{q^n} = \sum_r (-1)^{r-1} \left(q^{2n/r-r-1} - q^{r-2n/r+1}/2\right)$$

$$= \sum_r (-1)^{r-1} \left(q^{2n/r-r-1} - q^{r-2n/r-1}/2 q\right)$$

$$= \sum_r (-1)^{r-1} (1 - q) q^{r-2n/r-1}/2$$

$$= (q - 1) \sum_r (-1)^r q^{r-2n/r-1}/2,$$

where $r$ runs over divisors of $2n$ such that $r$ and $2n/r$ have opposite parity. Rearranging the terms,

$$\frac{C_n(q)}{q^n} = \left(1 - \frac{1}{q}\right) \sum_r (-1)^{2n/r} \left(q^{2n/r-r-1}/2 + 1 - q^{(2n/r-r-1)/2}\right)$$

$$= \left(1 - \frac{1}{q}\right) \sum_r q^{2n/r-r} - 1 \frac{q^{(2n/r-r-1)/2}}{q^{(2n/r-r-1)/2}}$$

$$= \left(1 - \frac{1}{q}\right) \sum_r q^{2n/r-r} - 1 \frac{q^{(2n/r-r-1)/2}}{q^{(2n/r-r-1)/2}},$$
Lemma 5. For any \( n \in E_k \),

\[
\frac{C_n(q)}{q^n} - \left(1 - \frac{1}{q}\right) q^n = \text{sign}(k) \frac{(q - 1) (q^{|k|} - 1)}{q^{(|k|+1)/2}} - \left(1 - \frac{1}{q}\right) \frac{1}{q^{n-1}}. \tag{3}
\]

Proof. Take \( n \in E_k \). We have \( n = \frac{p(p+k)}{2} \), for some odd prime number \( p \) such that \( p + k \) is a power of 2. In virtue of Lemma 4,

\[
\frac{C_n(q)}{q^n} = \left(1 - \frac{1}{q}\right) \frac{q^{2n-1} - 1}{q^{n-1}} + \left(1 - \frac{1}{q}\right) (-1)^{2n/\psi(n)} \frac{q^{2\beta(n)+1} - 1}{q^{\beta(n)}}. \tag{4}
\]

Applying Lemma 2 to (4) we obtain

\[
\frac{C_n(q)}{q^n} = \left(1 - \frac{1}{q}\right) \frac{q^{2n-1} - 1}{q^{n-1}} + \left(1 - \frac{1}{q}\right) \text{sign}(k) \frac{q^{|k|} - 1}{q^{(|k|+1)/2}}. \tag{5}
\]

The equality (5) can be easily transformed into (3). \( \Box \)

We proceed now with the proof of the main result of this paper.

Proof (of Theorem 1). Notice that \( K = \{ k \in \mathbb{Z} : E_k \text{ infinite} \} \) and \( \Phi = \bigcup_{k \in \mathbb{Z}} E_k \).

Take \( k \in K \). The set \( E_k \) is infinite. In virtue of Lemma 5

\[
\lim_{n \to +\infty} \left( \frac{C_n(q)}{q^n} - \left(1 - \frac{1}{q}\right) q^n \right) = \text{sign}(k) \frac{(q - 1) (q^{|k|} - 1)}{q^{(|k|+1)/2}}.
\]

Hence, \( \text{sign}(k) (1 - q^{-|k|}) \) is a limit point of the set \( \Omega_q \).

Consider a fixed prime number \( p \). For any power of 2 large enough, denoted \( 2^h \), we can construct \( n_h = \frac{p(p+k)}{2} \in E_{kh} \), with \( kh = 2^{h+1} - p > 0 \). So,

\[
\lim_{h \to +\infty} \left( \frac{C_{n_h}(q)}{q^{n_h}} - \left(1 - \frac{1}{q}\right) q^{n_h} \right) = \lim_{k \to +\infty} \text{sign}(k) \frac{(q - 1) (q^{|k|} - 1)}{q^{(|k|+1)/2}} = +\infty.
\]

Hence, \( +\infty \) is a limit point of the set \( \Omega_q \).

Consider a fixed power of 2, denoted \( 2^h \). For any prime number \( p \) large enough, we can construct \( n_p = \frac{p(p+k)}{2} \in E_{kp} \), with \( kp = 2^{h+1} - p < 0 \). So,

\[
\lim_{p \to +\infty} \left( \frac{C_{n_p}(q)}{q^{n_p}} - \left(1 - \frac{1}{q}\right) q^{n_p} \right) = \lim_{k \to -\infty} \text{sign}(k) \frac{(q - 1) (q^{|k|} - 1)}{q^{(|k|+1)/2}} = -\infty
\]

Hence, \( -\infty \) is a limit point of the set \( \Omega_q \).

Now, take a limit point \( \lambda \) of the set \( \Omega_q \). There is a sequence of integers in \( (n_j)_{j \geq 1} \) satisfying \( n_j \in \Phi \), \( \lim_{j \to +\infty} n_j = +\infty \) and
On prime numbers of the form $2^n \pm k$

$$\lim_{j \to +\infty} \left( \frac{C_{n_j}(q)}{q^{n_j}} - \left( 1 - \frac{1}{q} \right) q^{n_j} \right) = \lambda.$$ 

In virtue of Lemma [5]

$$\lambda = \lim_{j \to +\infty} \left( \frac{\text{sign}(k_j)}{q^{(k_j+1)/2}} \frac{(q-1)(q^{k_j+1}-1)}{q^{k_j+1}/2} - \left( 1 - \frac{1}{q} \right) \frac{1}{q^{n_j-1}} \right)$$

for some integers $k_j \in \mathbb{Z}$ satisfying $n_j \in E_{k_j}$ for all $j \geq 1$.

Suppose that the sequence $(k_j)_{j \geq 1}$ is bounded. There is a subsequence of $(k_j)_{j \geq 1}$ going to infinite. So, $\lim_{j \to +\infty} \frac{(q-1)(q^{k_j+1}-1)}{q^{(k_j+1)/2}} = +\infty$. Hence, $\lambda \in \{-\infty, +\infty\}$.

Suppose that the sequence $(k_j)_{j \geq 1}$ is bounded. There is some $k$ for which $n_j \in E_k$ for infinitely many $j \geq 1$. So, $k \in K$. Hence, $\lambda = \text{sign}(k) \frac{(q-1)(q^{k+1}-1)}{q^{(k+1)/2}}$.

Therefore, the set of limit points of $\Omega_q$ is precisely $K_q$. \qed

3 Final remarks

In virtue of Theorem[11] there are only finitely many Fermat and Mersenne primes if and only if there is a real number $\epsilon > 0$ such that for all $n \in \Phi$ large enough, the inequality

$$\left| \frac{C_n(2)}{2^n} - 2^{n-1} \right| > \frac{1}{2} + \epsilon$$

holds.

Acknowledgements

The author would like to thank Srečko Brlek and Christophe Reutenauer for useful comments.

References

1. N. J. Fine, “Basic hypergeometric series and applications” No. 27. American Mathematical Soc., 1988.
2. C. Kassel and C. Reutenauer, “Counting the ideals of given codimension of the algebra of Laurent polynomials in two variables”, [https://arxiv.org/abs/1505.07229](https://arxiv.org/abs/1505.07229) 2015.
3. C. Kassel and C. Reutenauer, “Complete determination of the zeta function of the Hilbert scheme of n points on a two-dimensional torus”, [https://arxiv.org/abs/1610.07793](https://arxiv.org/abs/1610.07793) 2016.
4. C. Kassel and C. Reutenauer, “The Fourier expansion of $\eta(z)\eta(2z)\eta(3z)/\eta(6z)$”, Archiv der Mathematik 108.5 (2017): 453-463.