ON A SET OF FIXED POINTS RELATED TO BOTH FERMAT AND MERSENNE PRIMES

José Manuel Rodríguez Caballero
Département de Mathématiques, Université du Québec á Montréal, Montréal, Québec, Canada
rodriguez_caballero.jose_manuel@uqam.ca

Received: 12/21/17, Revised: 4/24/18, Accepted: 6/24/18, Published: 6/29/18

Abstract
Motivated by a sequence of polynomials from Hodge Theory, we define an arithmetical function $f(n)$ and we prove that its fixed points are related to both Fermat and Mersenne primes.

1. Introduction

For any integer $n \geq 1$, consider the polynomial

$$E\left(X^{[n]};q\right) := \left(q^n - q^{n-1}\right) \sum_{\substack{d|n \\ d \equiv 1 \pmod 2}} \left(q^{\gamma_n(d)} - q^{1-\gamma_n(d)}\right), \tag{1}$$

where $\gamma_n(d) := \frac{1}{2}\left(\frac{2n}{d} - d + 1\right)$. From a Hodge-theoretic point of view [4], $E\left(X^{[n]};q\right)$ is E-polynomial of the Hilbert scheme $X^{[n]}$ of n points on the algebraic torus $X := \mathbb{C}^\times \times \mathbb{C}^\times$. The quotient $E\left(X^{[n]};q\right)/(q-1)^2$ is a polynomial whose coefficients are nonnegative integer, named *Kassel-Reutenauer q-analog of the sum of divisors* [2].

Several number-theoretic properties of these polynomials where studied in the author's Master Memoir [1]. Also, the coefficients of $E\left(X^{[n]};q\right)$ are related to well-matched parentheses [3].

If q is a prime power [5, 6] then $E\left(X^{[n]};q\right)$ is the number of ideals I of the algebra $\mathbb{F}_q[x,y,x^{-1},y^{-1}]$ such that the quotient $\mathbb{F}_q[x,y,x^{-1},y^{-1}]/I$, viewed as a vector space over $\mathbb{F}_q$, has dimension n. Furthermore, the sequence $\left(C_n(q)\right)_{n\geq 1}$ evaluated at some roots of unity [7] can be expressed as the Fourier coefficient of certain η-products.

It follows from (1) that

$$E\left(X^{[n]};q\right) = q^{2n} - q^{2n-1} - (-1)^{\kappa(n)}\, q^{f(n)+1} + R_n(q),$$

for some polynomial $R_n(q)$ whose degree is at most $f(n)$, where $\kappa(n)$ and $f(n)$ are the arithmetical functions defined below.

For each integer $n \geq 1$, define the arithmetical function

$$\kappa(n) := \begin{cases} 0, & \text{if } n = 2^k \text{ for some } k \in \mathbb{Z}_{\geq 0}; \\ \min M_n, & \text{otherwise;} \end{cases}$$

where $M_n := \left\{d, \frac{2n}{d} : \quad d|n, \, d > 1 \text{ and } d \equiv 1 \pmod 2\right\}$. Let $f(n)$ be the arithmetical function given by

(i) $f\left(2^k\right) := 0$ for all $k \in \mathbb{Z}_{\geq 0}$;

(ii) $\frac{n}{\kappa(n)} - \frac{f(n)}{\kappa(n)+1} = \frac{1}{2}$, for all $n \in \mathbb{Z}_{\geq 1}$, provided that $n \neq 2^k$ for all $k \in \mathbb{Z}_{\geq 0}$.

The values of $\kappa(n)$ and $f(n)$, for $1 \leq n \leq 25$, are given in the following table.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\kappa(n)$	0	0	2	0	2	3	2	0	2	4	2	3	2	4	2
$f(n)$	0	0	3	0	6	6	9	0	12	10	15	14	18	15	21

The first polynomials $E\left(X^{[n]}; q\right)$ are

$$\begin{aligned}
E\left(X^{[1]}; q\right) &= q^2 - 2q + 1, \\
E\left(X^{[2]}; q\right) &= q^4 - q^3 - q + 1, \\
E\left(X^{[3]}; q\right) &= q^6 - q^5 - q^4 + 2q^3 - q^2 - q + 1, \\
E\left(X^{[4]}; q\right) &= q^8 - q^7 - q + 1, \\
E\left(X^{[5]}; q\right) &= q^{10} - q^9 - q^7 + q^6 + q^4 - q^3 - q + 1, \\
E\left(X^{[6]}; q\right) &= q^{12} - q^{11} + q^7 - 2q^6 + q^5 - q + 1, \\
E\left(X^{[7]}; q\right) &= q^{14} - q^{13} - q^{10} + q^9 + q^5 - q^4 - q + 1, \\
E\left(X^{[8]}; q\right) &= q^{16} - q^{15} - q + 1, \\
E\left(X^{[9]}; q\right) &= q^{18} - q^{17} - q^{13} + q^{12} + q^{11} - q^{10} - q^8 + q^7 + q^6 - q^5 - q + 1.
\end{aligned}$$

We recall that a prime number $p = 2^m + 1$, with $m \in \mathbb{Z}_{\geq 1}$, is called *Fermat prime*. Similarly, a prime number $p = 2^m - 1$, with $m \in \mathbb{Z}_{\geq 1}$, is called *Mersenne prime*. Furthermore, n is a *fixed point* of f if $f(n) = n$. The goal of this paper is to prove the following elementary result.

Theorem 1. *The function $f(n)$ has infinitely many fixed points if and only if at least one of the following statements holds:*

(i) there are infinitely many Fermat primes;

(ii) there are infinitely many Mersenne primes.

2. Proof of the Main Result

We proceed to prove the main result of this paper.

Proof of Theorem 1. Notice that, by definition of f, an integer $n \in \mathbb{Z}_{\geq 1}$ is a fixed point of f if and only if

$$\kappa(n)\ (\kappa(n)+1) = 2n. \tag{2}$$

Suppose that $n = \frac{p(p+1)}{2}$, where $p = 2^m - 1$ is a Mersenne prime and $m \in \mathbb{Z}_{\geq 1}$. Then $\kappa(n) = p < p+1 = 2^m = \frac{2n}{p}$. The left hand side of (2) becomes $\kappa(n)\ (\kappa(n)+1) = p\,(p+1)$, which coincides with its right hand side $2n = p\,(p+1)$. Hence, n is a fixed point of f.

Suppose that $n = \frac{(p-1)p}{2}$, where $p = 2^m+1$ is a Fermat prime and $m \in \mathbb{Z}_{\geq 1}$. Then $\kappa(n) = 2^m = \frac{2n}{p} = p-1 < p$. The left hand side of (2) becomes $\kappa(n)\ (\kappa(n)+1) = (p-1)\,p$, which coincides with its right hand side $2n = (p-1)\,p$. Hence, n is a fixed point of f.

Now, suppose that n is a fixed point of f. The equation (2) implies that $\kappa(n) \neq 0$. So, $n \neq 2^k$ for all $k \in \mathbb{Z}_{\geq 0}$, i.e. n has an odd divisor greater than 1.

Suppose that $\kappa(n)$ is an odd prime number. Let d be the largest odd divisor of $\kappa(n)+1$. Notice that $2d$ divides $\kappa(n)+1$. The obvious inequality $2d \leq \kappa(n)+1$ implies that $d \leq \frac{\kappa(n)+1}{2} < \kappa(n)$. In virtue of the extremal property of μ, we conclude that $d = 1$, i.e. $\kappa(n)+1 = 2^m$, for some $m \in \mathbb{Z}_{\geq 1}$. Hence, $n = \frac{(p-1)p}{2}$, where p is a Mersenne prime.

Suppose that $\kappa(n)$ is not an odd prime number. By definition of κ we have $\kappa(n) = 2^m$, for some $m \in \mathbb{Z}_{\geq 1}$. Let d be the largest divisor of $\kappa(n)+1$ satisfying $d < \kappa(n)+1$. So, $d < \kappa(n)$, because d is odd and $\kappa(n)$ even. In virtue of the extremal property of μ, we conclude that $d = 1$, i.e. $\kappa(n)+1$ is prime. Hence, $n = \frac{p(p+1)}{2}$, where p is a Fermat prime.

We have shown that there is a bijection between the set fixed points of $f(n)$ and the set of both Fermat and Mersenne primes. Therefore, there are infinitely many fixed points of $f(n)$ if and only if the set of both Fermat and Mersenne primes is infinite. □

Acknowledgments. This paper was written at LaBRI (Laboratoire Bordelais de Recherche en Informatique) during a scientific travel to France supported by an ERASMUS+ scholarship. The ISM (Institut des Sciences Mathématiques) contributed to the financial support of the author by means of a scholarship. The author would like to thank Srečko Brlek, Christophe Reutenauer, Christian Kassel, Pierre Castéran and the anonymous reviewers.

References

[1] J. M. R. Caballero, *Propriétés arithmétiques du E-polynôme du schéma de Hilbert de n points dans le tore bidimensionnel*, Master Memoir, Université du Québec à Montréal, Montréal, QC, Canada, 2018.

[2] J. M. R. Caballero, On Kassel–Reutenauer q-analog of the sum of divisors and the ring $\mathbb{F}_3[X]/X^2\mathbb{F}_3[X]$, *Finite Fields Appl.* **51** (2018), 183–190.

[3] J. M. R. Caballero, Symmetric Dyck Paths and Hooleys Δ-function. In: Brlek, S, Dolce, F., Reutenauer, C., Vandomme, E., eds. *Combinatorics on Words: 11th International Conference, Words 2017*, Vol. 10432, Springer, Montréal, QC, Canada, 2017, 252–261.

[4] T. Hausel, E. Letellier, and F. Rodriguez-Villegas, Arithmetic harmonic analysis on character and quiver varieties II, *Advances in Mathematics* **234** (2013), 85–128.

[5] C. Kassel and C. Reutenauer, Complete determination of the zeta function of the Hilbert scheme of n points on a two-dimensional torus (2016), arxiv.org/pdf/1610.07793.

[6] C. Kassel and C. Reutenauer, Counting the ideals of given codimension of the algebra of Laurent polynomials in two variables (2015), arxiv.org/pdf/1505.07229

[7] 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.