A FINITE RING POLYNOMIAL

B. Sury

Stat-Math Unit, Indian Statistical Institute, Bangalore, 560 059, India

sury@isibang.ac.in

Received: 1/1/04, Revised: 9/28/04, Accepted: 10/22/04, Published: 10/25/04

Abstract

For any finite commutative ring A with unity, the polynomial

$$S_A(x) = \prod_{a \in A} (x - a)$$

was considered in [1] as an analogue of the sine function and studied with reference to Kronecker's Jugendtraum. A question posed there was whether, for $A = \mathbb{Z}/n\mathbb{Z}$, the additivity

$$S_A(x + y) = S_A(x) + S_A(y)$$

holds if, and only if, n is a prime. We prove this very easily and show, more generally, that if additivity holds for A, then A has characteristic a prime and, further, for the ring A which is the direct sum of r copies of $\mathbb{Z}/p\mathbb{Z}$ for a prime p, we have

$$S_A(x) = (x^p - x)^{p^{r-1}}.$$

For any finite commutative ring A with unity, consider the polynomial

$$S_A(x) = \prod_{a \in A} (x - a).$$

This finite analogue of the sine function was studied in [1] where the question was posed for $A = \mathbb{Z}/n\mathbb{Z}$ as to whether the additivity

$$S_A(x + y) = S_A(x) + S_A(y)$$

holds if, and only if, n is a prime. This is extremely easy to prove and here we observe, more generally, the following :

Theorem. *Let A be any finite commutative ring with unity having cardinality n and let $S_A(x) \in A[x]$ be defined to be $\prod_{a \in A}(x-a)$. If*

$$S_A(x+y) = S_A(x) + S_A(y)$$

holds, then A has characteristic a prime. In particular, for $\mathbb{Z}/n\mathbb{Z}$, additivity holds if, and only if, n is prime.
Further, for the ring A which is the direct sum of r copies of $\mathbb{Z}/p\mathbb{Z}$ for a prime p, we have

$$S_A(x) = (x^p - x)^{p^{r-1}}.$$

In particular, additivity holds in all these cases.

Proof. Let us start by observing that $S_A(x) = x^n + f(x)$ where f is a polynomial consisting of terms in x, of degree smaller than n.
Thus $S_A(x+y)$ contains the terms $\binom{n}{r}x^r y^{n-r}$ for $1 \leq r < n$ which, if nonzero, contribute to $S_A(x+y) - S_A(x) - S_A(y)$. Thus, additivity forces all the binomial coefficients $\binom{n}{r}$ to be zero in A for all $1 \leq r < n$.
If $n = \prod_{i=1}^{k} p_i^{l_i}$ for different primes p_i, then since $\left(\begin{array}{c} n \\ p_i^{l_i} \end{array}\right)$ is coprime to p_i and since $n = \binom{n}{1}$ is itself zero, we obtain that $\frac{n}{p_i^{l_i}}$ is zero in A. But these k numbers do not have a common factor, which gives a contradiction unless there is only one prime.
Let us write $n = p^l$. Then the binomial coefficient $\left(\begin{array}{c} p^l \\ p^{l-1} \end{array}\right)$ is zero in A. This number is of the form pd for some $(p,d) = 1$; hence we once again obtain, by using $p^l = 0 = pd$, that $p = 0$ in A. This proves the first assertion and answers question 1 of [1] affirmatively.

Now, we proceed further and consider rings which are direct sums of a finite number of copies of $\mathbb{Z}/p\mathbb{Z}$ and show that in these cases, the function $S_A(x) = (x^p - x)^{p^{r-1}}$.
Let us consider $A = \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ first so as to make the pattern clear.
Now $S_A(x) = \prod_{0 \leq i,j < p}(x - (i,j))$. Further, it is trivial to see that the corresponding function of $\mathbb{Z}/p\mathbb{Z}$ is

$$x(x-1)\cdots(x-p+1) = x^p - x.$$

In other words, the k-th symmetric polynomials σ_k in the natural numbers $1, 2, \cdots, p-1$ are multiples of p for $1 \leq k < p-1$.
Note that, for this ring A,

$$(x-(0,0))(x-(1,1))\cdots(x-(p-1,p-1)) = x(x-1_A)(x-2(1_A))\cdots(x-(p-1)1_A)$$

where 1_A is the unity of A.
Hence

$$x(x-1_A)(x-2(1_A))\cdots(x-(p-1)1_A) = x^p - (\sigma_1)1_A x^{p-1} + \cdots - (\sigma_{p-2})1_A x^2 - x = x^p - x.$$

Thus, we have the subproduct

$$S_0(x) := (x-(0,0))(x-(1,1))\cdots(x-(p-1,p-1)) = x^p - x.$$

Now, we claim that the product $S_A(x)$ can be broken up into p products each of which equals the above subproduct $S_0(x)$.
It is clear that the product of the $p-1$ factors

$$S_i(x) = (x-(0,i))(x-(1,i+1))\cdots(x-(p-1,i-1)),$$

for $i = 1,2,\cdots,p-1$, when multiplied by $S_0(x)$, give $S_A(x)$. We claim that $S_i = S_0$ for all i.
Clearly, $S_i(x) = S_0(y)$ where $y = x-(0,i)$. Therefore,

$$S_i(x) = y^p - y = (x-(0,i))^p - (x-(0,i)) = x^p - x.$$

Hence, we have proved, for $A = \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$, that $S_A(x) = (x^p - x)^p$.

For general r, the proof is essentially the same as that given for $r = 2$, taking

$$S_0(x) = (x-(0,\cdots,0))(x-(1,\cdots,1))\cdots(x-(p-1,\cdots,p-1))$$

except that there are now p^{r-1} subproducts in the obvious manner. In fact, $\mathbb{Z}/p\mathbb{Z}$ acts on A by

$$j.(i_1,\cdots,i_r) = (i_1-j,\cdots,i_r-j)$$

and S_0 is an orbit of the action. Since each orbit clearly has p elements, there are p^{r-1} orbits. Note that for any orbit S_i, the subproduct equals $x^p - x$ as seen before.
Hence, it follows that for the direct sum A of r copies of $\mathbb{Z}/p\mathbb{Z}$, we have $S_A(x) = (x^p - x)^{p^{r-1}}$. This proves the theorem.

It may also be interesting to study this function for finite noncommutative rings, where we fix any order of the elements for defining the product.

References

[1] **N. Kurokawa, Eva-Marie Muller-Stuler, H. Ochiai, and M. Wakayama**, *Kronecker's Jugendtraum and ring sine functions*, J. Ramanujan Math. Soc., Vol. 17 (2002) 211-220.

Acknowledgments

It is a pleasure to thank Professor H. N. Ramaswamy who drew my attention to this question and gave me a copy of the paper of Kurokawa et. al.