# An Integral Polynomial

B. SURY
Tata Institute of Fundamental Research
Bombay 400005, India

On many occasions, we find ourselves surprised when some general formula being used for some specific purpose suddenly seems to yield something totally different. For instance, we discover while looking at the so-called Weyl dimension formula for the compact group $SU(n)$ that, for any $n$ integers $a_1 < a_2 < \cdots a_n$ the fraction

$$\prod_{i>j} \frac{a_i - a_j}{i - j}$$

occurs as the dimension of some representation of this group. As a result, we see the unexpected fact that the fraction given above is always an integer. We would like to derive this fact by an elementary method. Surprisingly enough, this does not seem to be very easy to prove. For one thing, an induction argument invariably fails. Even more surprising is the fact that we can give an elementary proof of the following more general fact (whereas the proof itself cannot be applied directly to show the weaker result that the above fraction is an integer!).

THEOREM. *For any integers* $a_1 < a_2 < \cdots < a_n$

$$P(X) := \prod_{n \geq i > j \geq 1} \frac{X^{a_i - a_j} - 1}{X^{i-j} - 1} \in \mathbf{Z}[X].$$

Of course, by L'Hôpital's rule then

$$P(1) = \prod_{i>j} \frac{a_i - a_j}{i - j} \in \mathbf{Z},$$

which was our original assertion. As we will see, we can deduce more from the proof of the theorem.

*Proof.* Writing $X^r - 1 = \prod_{d/r} \Phi_d(X)$, where $\Phi_d$ is the $d$th cyclotomic polynomial ([**1**], Theorem 3.4) we have

$$P(X) = \prod_{i>j} \frac{\prod_{d/(a_i - a_j)} \Phi_d(X)}{\prod_{d/(i-j)} \Phi_d(X)}.$$

Fix any positive integer $d$. Since $\Phi_d$ is irreducible ([**1**], Theorem 3.7), we need only show that the power of $\Phi_d(X)$ occurring in the denominator is at the most the power occurring in the numerator. For $0 \leq i \leq d-1$, we let $r_i$ denote the number of $a$'s that are in the residue class $i$ modulo $d$. Similarly, we denote by $s_i$ the corresponding numbers when $\{a_1, \dots, a_n\}$ is replaced by $\{1, \dots, n\}$. Then $\Sigma r_i = \Sigma s_i = n$. Moreover, if we write $n = qd + r$, $0 \leq r < d$, then it is clear that $s_0 = q = s_i$ for $r < i < d$ and $s_j = q + 1$ for $0 < j \leq r$. The power of $\Phi_d$ dividing $\prod_{i>j}(X^{a_i - a_j} - 1)$ equals

$$\frac{1}{2} \sum_{i=0}^{d-1} r_i(r_i - 1) = \frac{1}{2} \sum_{i=0}^{d-1} r_i^2 - \frac{n}{2}.$$

It is reasonable to guess that $\Sigma_{i=0}^{d-1} r_i^2$ is minimum when the $r_i$ are almost equal. To see that this is indeed true, we write $r_i = s_i + t_i$, with $t_i \in \mathbf{Z}$. Then, $\Sigma t_i = 0$. Now, if

$r=0$ i.e. if $d/n$, then $s_i=q$ for all $0\le i<d$ and $\Sigma r_i^2=\Sigma(q+t_i)^2=dq^2+\Sigma t_i^2\ge dq^2=\Sigma s_i^2$. If $r>0$, then

$$\begin{aligned}\sum r_i^2 &= (q+t_0)^2+\sum_{i=1}^{r}(q+1+t_i)^2+\sum_{i=r+1}^{d-1}(q+t_i)^2\\ &=(d-r)q^2+r(q+1)^2+\sum_{i=0}^{d-1}t_i^2+2\sum_{i=1}^{r}t_i\\ &\ge (d-r)q^2+r(q+1)^2=\sum s_i^2,\end{aligned}$$

provided $\Sigma_{i=0}^{d-1}t_i^2+2\Sigma_{i=1}^{t}t_i\ge 0$. But, if $I=\{i:1\le i\le r,\ t_i=-1\}$, then

$$\begin{aligned}\sum_{i=0}^{d-1}t_i^2+2\sum_{i=1}^{r}t_i &\ge \sum_{0\le i\le d-1,\, t>0}t_i^2+\sum_{1\le i\le r,\, t_i<0}\left(t_i^2+2t_i\right)\\ &\ge \sum_{0\le i\le d-1,\, t_i>0}t_i^2+\sum_{1\le i\le r,\, t_i=-1}t_i(t_i+2)\\ &= \sum_{0\le i\le d-1,\, t_i>0}t_i^2-|I|\\ &\ge \sum_{0\le i\le d-1,\, t_i>0}\left(t_i^2-t_i\right)\ge 0\end{aligned}$$

since $\Sigma_{0\le i\le d-1,\, t_i>0}t_i\ge |I|$ by the equality $\Sigma_{i=0}^{d-1}t_i=0$ where $|I|$ is the cardinality of $I$. This completes the proof of the theorem.

If we look at the proof carefully, we can guess at the following result.

**Bonus result** Let $k$ be any natural number and let $a_1,\dots,a_n$ be integers such that the number of $a_i$'s in each residue class modulo $k$ is the number of $i$'s in that class. Then

$$\prod_{i\ne j}\frac{\prod_{a_i\equiv a_j(k)}(a_i-a_j)}{\prod_{i\equiv j(k)}(i-j)}\in\mathbf{Z}.$$

In particular, if $k=1$, we need no restriction on the $a_i$'s.

We notice that the above expression equals $P(e^{2\pi i/k})$. Consequently, $P(e^{2\pi i/k})$ is an algebraic integer as well as a rational number, which forces it to be a rational integer.

**Remark** We notice that in the proof of the theorem, the cyclotomic polynomials $\Phi_d(X)$ could be replaced by any irreducible polynomials $T_d(X)$ with integer coefficients. Then our argument goes through without change to show that

$$T(X)=\prod_{i>j}\frac{\prod_{d/(a_i-a_j)}T_d(X)}{\prod_{d/(i-j)}T_d(X)}\in\mathbf{Z}[X].$$

For instance, for each $d$, if we choose $T_d(X)$ to be the constant polynomial 2, we would get

$$\sum_{i>j}\tau(a_i-a_j)\ge\sum_{i>j}\tau(i-j),$$

where $\tau(n)$ is the number of divisors of $n$.

**Acknowledgements.** I would like to thank the referee for his/her detailed comments that helped in improving the exposition. I am also indebted to Amit Roy and Rajan for their assistance.

## REFERENCE

1. Niven, *Irrational Numbers*, The Carus Mathematical Monographs, MAA, Washington, DC, 1956.