SOLUTION TO PROBLEM 5.2 (C)

CHRISTOPHER J. HILLAR

Abstract. We present a solution to the following problem: Let $a_1, \ldots, a_n \in \mathbb{C}$ and suppose that $S(k) = \sum_{i=1}^{n} {a_i}^k \in \mathbb{Z}$ for all $k \in \mathbb{P}$. Then,

$$\prod_{i=1}^{n} (t - a_i) \in \mathbb{Z}[t].$$

1. Newton Polynomials and Symmetric Functions

The problem above gives a converse to the following fact. Let α be an algebraic integer (a root of a monic polynomial, $g(t) \in \mathbb{Z}[t]$), then if $a_1, \ldots, a_n \in \mathbb{C}$ are the conjugates of this polynomial (all its roots), then $S(k) \in \mathbb{Z}$. This is an easier implication since the polynomial $f(x_1, \ldots, x_n) = \sum_{i=1}^{n} {x_i}^k$ is symmetric and thus can be written (over $\mathbb{Z}$) in terms of the elementary symmetric polynomials. Substituting $(a_1, \ldots, a_n)$ for $(x_1, \ldots, x_n)$ in f gives us the result (as the coefficients of g are the elementary symmetric polynomials evaluated at $(a_1, \ldots, a_n)$).

We will first prove that $g(t) = \prod_{i=1}^{n} (t - a_i)$ is a polynomial in $\mathbb{Q}[t]$. This will follow from Newton's famous identities relating the coefficients of $g(t)$ to the values of $S(k)$.

Theorem 1.1. (Newton's Identities) Let $a_1, \ldots, a_n \in \mathbb{C}$ and let

$$g(t) = \prod_{i=1}^{n} (t - a_i) = t^n + p_{n-1}t^{n-1} + \ldots + p_0.$$

Then,

$$S(k) + p_{n-1}S(k-1) + \ldots + p_{n-k+1}S(1) + kp_{n-k} = 0 \quad \text{for} \quad k < n$$
$$S(k) + p_{n-1}S(k-1) + \ldots + p_1 S(k-n+1) + p_0 S(k-n) = 0 \quad \text{for} \quad k \geq n$$

For clarity, we write a few of these identities down:

$$S(1) + p_{n-1} = 0, \ S(2) + p_{n-1}S(1) + 2p_{n-2} = 0.$$

Proof. For simplicity, we define $S(0) = n$. We will prove the claim by evaluating $g'(t)$ in two ways. Notice that on the one hand we have

$$g'(t) = nt^{n-1} + (n-1)p_{n-1}t^{n-2} + \ldots + p_1.$$

On the other hand, since $g(t) = \prod_{i=1}^{n} (t - a_i)$ we have

$$g'(t) = \sum_{i=1}^{n} \frac{g(t)}{(t - a_i)}$$

Department of Mathematics, University of California, Berkeley, CA 94720. (chillar@math.berkeley.edu).

Viewing this expression as a Laurent series (in the variable t), we may expand

$$\frac{1}{(t-a_i)} = (1/t)\sum\nolimits_{j=0}^{\infty}(a_i/t)^j$$

So then,

$$\begin{aligned} g'(t) &= (g(t)/t)\sum\nolimits_{i=1}^{n}\sum\nolimits_{j=0}^{\infty}(a_i/t)^j \\ &= (g(t)/t)\sum\nolimits_{j=0}^{\infty}\sum\nolimits_{i=1}^{n}(a_i/t)^j \\ &= t^{n-1}\left(\sum\nolimits_{j=0}^{\infty} p_{n-j}t^{-j}\right)\left(\sum\nolimits_{j=0}^{\infty} S(j)t^{-j}\right) \end{aligned}$$

in which $p_n = 1$ and $p_i = 0$ for $i < 0$. Writing this last expression more constructively, we have

$$g'(t) = t^{n-1}\sum\nolimits_{k=0}^{\infty} t^{-k}\sum\nolimits_{i=0}^{k} S(i)p_{n-k+i}$$

Equating coefficients of both series for $g'(t)$, we arrive at

$$\sum\nolimits_{i=0}^{k} S(i)p_{n-k+i} = (n-k)p_{n-k}.$$

Since $S(0)p_{n-k} = np_{n-k}$, the formulas in the theorem drop out. □

Using Newton's identities, we have $p_{n-1} = -S(1) \in \mathbb{Z}$, $2p_{n-2} = -S(2) - p_{n-1}S(1) \in \mathbb{Z}$, and in general, $n!p_i \in \mathbb{Z}$ for all $i = 0, \ldots, n-1$. This not only proves that $g(t) \in \mathbb{Q}[t]$, but also much more. Since each of a_i is algebraic over $\mathbb{Q}$ and $n!p_i \in \mathbb{Z}$, there is a constant c_n (only depending on n) such that each of $c_n a_i$ is an algebraic integer (we can actually choose $c_n = (n!)^n$). We will now prove that, in fact, each a_i is an algebraic integer. This will prove the claim that $g(t) \in \mathbb{Z}[t]$ since then we can express each p_i as an elementary symmetric polynomial in the a_i. Since algebraic integers form a ring and the only elements of $\mathbb{Q}$ that are algebraic integers are elements of $\mathbb{Z}$ we must have $p_i \in \mathbb{Z}$.

Let $r \in \mathbb{P}$ and notice that $a_1^r, \ldots, a_n^r$ satisfy the hypothesis that $\sum_{i=1}^{n}\left({a_i}^r\right)^k \in \mathbb{Z}$ for all $k \in \mathbb{P}$. Whence, $\prod_{i=1}^{n}\left(t - {a_i}^r\right) \in \mathbb{Q}[t]$ and that, moreover, each of $c_n a_i^r$ ($r = 1, 2, \ldots$) is an algebraic integer. We will now show that $\{1, a_i, a_i^2, \ldots\}$ is a finitely generated $\mathbb{Z}$-module which will finally prove that each a_i is an algebraic integer and complete the proof. Let ϑ denote the ring of algebraic integers of $\mathbb{Q}(a_i)$. By well-known results in number theory, this ring is a finitely generated $\mathbb{Z}$-module and hence $(1/c_n)\vartheta$ is a finitely generated $\mathbb{Z}$-module. The $\mathbb{Z}$-module generated by $\{1, a_i, a_i^2, \ldots\}$ is contained in $(1/c_n)\vartheta$, and hence is finitely generated (since any submodule of a finitely generated module over a principal ideal domain is finitely generated), completing the proof.