A discrete approach to a result concerning a contour integral

Navid Safaei

1 Introduction

The following result is a standard application of the residue theorem and can be found in essentially every book on Complex Analysis:

Theorem 1.1. *If $P(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ is a polynomial with complex coefficients, then*

$$\frac{1}{2\pi}\int_0^{2\pi} |P(e^{i\theta})|^2 d\theta = |a_0|^2 + |a_1|^2 + \cdots + |a_n|^2.$$

The usual proof of this result goes as follows:

$$\frac{1}{2\pi}\int_0^{2\pi} |P(e^{i\theta})|^2 d\theta = \frac{1}{2i\pi}\oint_{|z|=1} |P(z)|^2 \frac{dz}{z} =$$

$$\frac{1}{2\pi i}\oint_{|z|=1} P\left(z\right)\overline{P}(z^{-1})\frac{dz}{z} = \left|a_0\right|^2 + \ldots . + \left|a_n\right|^2,$$

where $\bar{P}(X) = \overline{a_n}X^n + \cdots + \overline{a_0}$ (note that $\overline{P(z)} = \overline{P}(\overline{z})$ for all $z \in \mathbf{C}$, and $\overline{z} = z^{-1}$ when $|z| = 1$). The last equality in the above chain (the only non tautological one) is a consequence of the residue theorem.

Even though this proof is straightforward (with the right tools in our hands!), the use of rather serious theorems of Complex Analysis makes it hard to digest for a high-school student. The purpose of this article is to present a discrete version of the previous argument, which gives a completely elementary proof of the result, and to discuss a few applications of the theorem to some fairly challenging problems from mathematical competitions.

2 Preliminaries

The goal of this small paragraph is to recall and prove the following very useful:

Proposition 2.1. *Let $z_1, z_2, \ldots, z_n$ be the roots of the polynomial $X^n - 1$, i.e. the nth roots of unity. If k is an integer, then $z_1^k + z_2^k + \cdots + z_n^k$ is equal to 0 when n does not divide k, and equal to n otherwise.*

Proof. By permuting $z_1, z_2, \ldots, z_n$, we may assume that $z_1 = e^{\frac{2i\pi}{n}}$ and $z_k = z_1^k$ for $1 \leq k \leq n$. Then for all integers k we have

$$z_1^k + z_2^k + \cdots + z_n^k = z_1^k + z_1^{2k} + \cdots + z_1^{nk} = z_1^k + (z_1^k)^2 + \cdots + (z_1^k)^n.$$

We recognize a geometric progression. If n divides k, then $z_1^k = 1$ and the sum is obviously equal to n. If not, then $z_1^k \neq 1$ and the formula for the sum of a geometric progression yields

$$z_1^k + (z_1^k)^2 + \cdots + (z_1^k)^n = z_1^k \frac{1 - z_1^{nk}}{1 - z_1^k} = 0,$$

since $z_1^{nk} = (z_1^n)^k = 1$. An alternative argument goes as follows: letting $S = z_1^k + z_2^k + \cdots + z_n^k$, we have

$$Sz_1^k = \sum_{i=1}^{n} (z_1 z_i)^k = \sum_{i=1}^{n} z_i^k = S,$$

the second equality being a consequence of the fact that the $z_1 z_i$'s are simply a permutation of the z_i's (since they are clearly n pairwise different roots of the polynomial $X^n - 1$). Thus $S(z_1^k - 1) = 0$ and $S = 0$ when n does not divide k (as then $z_1^k \neq 1$). The result follows. □

3 The main result

In this paragraph we prove the two key technical results, proposition 3.1 and corollary 3.1 below.

Proposition 3.1. *Let $P(X) = a_n X^n + \cdots + a_1 X + a_0$ be a polynomial with complex coefficients. Let $N > n$ be an integer and let $z_1, \ldots, z_N$ be the roots of the polynomial $X^N - 1$. Then*

$$\frac{1}{N} \sum_{i=1}^{N} |P(z_i)|^2 = |a_0|^2 + |a_1|^2 + \cdots + |a_n|^2.$$

Proof. For all $z \in \mathbf{C}$ with $|z| = 1$ we have (using that $\overline{z} = z^{-1}$)

$$|P(z)|^2 = P(z)\overline{P(z)} = |a_0|^2 + |a_1|^2 + \cdots + |a_n|^2 + \sum_{k=1}^{n} A_k z^{-k} + \sum_{k=1}^{n} B_k z^k$$

for some numbers $A_1, \ldots, A_n, B_1, \ldots, B_n \in \mathbf{C}$ depending on the coefficients $a_0, \ldots, a_n$ but not on z. Plugging in $z = z_1, \ldots, z_N$ and adding the resulting relations yields

$$\sum_{i=1}^{N} |P(z_i)|^2 = N(|a_0|^2 + \cdots + |a_n|^2) + \sum_{i=1}^{N} \sum_{k=1}^{n} A_k z_i^{-k} + \sum_{i=1}^{N} \sum_{k=1}^{n} B_k z_i^k.$$

On the other hand, we have

$$\sum_{i=1}^{N} \sum_{k=1}^{n} A_k z_i^{-k} = \sum_{k=1}^{n} A_k (\sum_{i=1}^{N} z_i^{-k}) = 0,$$

the last equality being a consequence of the more precise $\sum_{i=1}^{N} z_i^{-k} = 0$ for $1 \leq k \leq n$, itself a consequence of proposition 2.1. A similar argument shows that $\sum_{i=1}^{N} \sum_{k=1}^{n} B_k z_i^k = 0$, which combined with the previous discussion yields the desired result. □

Note that theorem 1.1 follows immediately from the previous proposition, by taking $N \to \infty$, since with the (somewhat abusive, since z_i depend on N) notations of the proposition

$$\lim_{N \to \infty} \frac{1}{N} \sum_{i=1}^{N} |P(z_i)|^2 = \frac{1}{2\pi} \int_0^{2\pi} |P(e^{i\theta})|^2 d\theta.$$

We end this section with a second key result, which is somewhat exotic but very useful, as we will see in the next section. It is a simple consequence of proposition 3.1.

If P is a polynomial with complex coefficients, we denote as in the introduction $\bar{P}$ the polynomial whose coefficients are the complex conjugates of the coefficients of P. In other words, if $P(X) = a_nX^n + \cdots + a_0$, then $\overline{P}(X) = \overline{a_n}X^n + \cdots + \overline{a_0}$. Also, for a polynomial $P(X) = a_nX^n + \cdots + a_0$ we write

$$S(P(X)) = |a_n|^2 + \cdots + |a_1|^2 + |a_0|^2.$$

We can then rewrite the proposition as the identity

$$S(P(X)) = \frac{1}{N}\sum_{i=1}^{N} |P(z_i)|^2$$

where z_i are the roots of the polynomial $X^N - 1$, where $N > n$ is any integer. We are now ready to state:

Corollary 3.1. *Let P, Q be polynomials with complex coefficients and let $m \geq \deg(Q)$. Then*

$$S(P(X) \cdot Q(X)) = S(X^m\overline{Q}(1/X) \cdot P(X)).$$

Proof. The hypothesis $m \geq \deg Q$ ensures that $R(X) = X^m\overline{Q}(1/X)$ is a polynomial with complex coefficients. Note that $|R(z)| = |Q(z)|$ for all z such that $|z| = 1$. In particular

$$\sum_{i=1}^{N} |R(z_i)P(z_i)|^2 = \sum_{i=1}^{N} |P(z_i)Q(z_i)|^2$$

when $z_1, \ldots, z_N$ are the roots of $X^N - 1$. The discussion preceding the corollary immediately yields $S(P(X) \cdot R(X)) = S(P(X) \cdot Q(X))$ (by taking N large enough). □

4 Applications

The goal of this paragraph is to explain how the two previous theoretical results yield unified and rather simple solutions to some fairly difficult problems about complex polynomials. Recall that

$$S(P(X)) = |a_0|^2 + \cdots + |a_n|^2\text{Ê} \quad \text{if} \quad P(X) = a_nX^n + \cdots + a_0 \in \mathbf{C}[X].$$

Problem 1 (Russian Olympiad 1995) Let P, Q be two monic polynomials with complex coefficients. Prove that

$$S(P(X) \cdot Q(X)) \geq |P(0)|^2 + |Q(0)|^2.$$

Solution Write $P(X) = a_nX^n + \cdots + a_0$ and $Q(X) = b_mX^m + \cdots + b_0$, with $a_n = b_m = 1$. Then, since P, Q are monic

$$P(X)X^m\overline{Q}(1/X) = (a_nX^n + \cdots + a_0)(\overline{b_0}X^m + \cdots + \overline{b_m}) = \overline{b_0}X^{n+m} + \cdots + a_0.$$

Using corollary 3.1, we deduce that

$$S(P(X)Q(X)) = S(P(X)X^m\overline{Q}(1/X)) \geq |a_0|^2 + |\overline{b_0}|^2 = |P(0)|^2 + |Q(0)|^2,$$

as desired.

Problem 2 (Taiwanese Olympiad) Let $P(X) = a_nX^n + \cdots + a_0$ be a polynomial with complex coefficients and roots $z_1, z_2, \ldots, z_n$. Let $j \in \{1, ..., n\}$ be such that $|z_1|, \ldots, |z_j| > 1$ and $|z_{j+1}|, ..., |z_n| < 1$. Prove that:

$$|z_1z_2 \ldots z_j| \le \sqrt{|a_0|^2 + |a_1|^2 + \cdots + |a_n|^2}.$$

Solution This is a special case of the previous problem. Indeed, define

$$Q(X) = (X - z_1) \ldots (X - z_j), \quad R(X) = (X - z_{j+1}) \ldots (X - z_n),$$

so that $P(X) = Q(X)R(X)$ and Q, R are monic. Problem 1 yields

$$|a_0|^2 + \cdots + |a_n|^2 = S(P(X)) = S(Q(X)R(X))$$

$$\ge |Q(0)|^2 + |R(0)|^2 \ge |Q(0)|^2 = |z_1 \ldots z_j|^2.$$

We conclude that

$$|z_1 \ldots z_j|^2 \le |a_n|^2 + \cdots + |a_0|^2,$$

finishing the proof.

Problem 3 (Chinese TST) Let $z_1, \ldots, z_n$ be the roots of a polynomial $P(X) = X^n + a_1X^{n-1} + \cdots + a_n$ with complex coefficients. If $\sum_{i=1}^n |a_i|^2 \le 1$, prove that $\sum_{i=1}^n |z_i|^2 \le n$.

Solution As we will see, this is a subtle variation and improvement of problem 2. Enumerate the roots of P such that $|z_1|, \ldots, |z_k| \le 1$ and $|z_{k+1}|, \ldots, |z_n| \ge 1$. The solution of problem 2 shows that

$$1 + |a_1|^2 + \cdots + |a_n|^2 \ge |z_{k+1} \ldots z_n|^2 + |z_1 \ldots z_k|^2.$$

To conclude, we use the following:

Lemma 4.1. *If $x_1, \ldots, x_m$ are real numbers, either all in $[0, 1]$ or all in $[1, \infty)$, then*

$$x_1 + \cdots + x_m \le m - 1 + x_1 \ldots x_m.$$

Proof. The result follows immediately from the identity

$$m - 1 + x_1 \ldots x_m - (x_1 + \cdots + x_m) = (1 - x_1)(1 - x_2) + (1 - x_1x_2)(1 - x_3)+$$

$$(1 - x_1x_2x_3)(1 - x_4) + \cdots + (1 - x_1 \ldots x_{m-1})(1 - x_m).$$

Of course, a more direct proof by induction on m is also possible. □

The previous lemma yields

$$|z_{k+1} \ldots z_n|^2 + |z_1 \ldots z_k|^2 \ge |z_1|^2 + \cdots + |z_n|^2 + 2 - n.$$

Using also the hypothesis, we finally obtain

$$2 \ge 1 + \sum_{i=1}^n |a_i|^2 \ge |z_1|^2 + \cdots + |z_n|^2 + 2 - n$$

hence $|z_1|^2 + \cdots + |z_n|^2 \le n$.

Note that the previous solution shows that for any complex monic polynomial $P(X) = X^n + a_1X^{n-1} + \cdots + a_n$ with roots $z_1, \ldots, z_n$ we have

$$\sum_{i=1}^n |z_i|^2 \le n - 1 + \sum_{i=1}^n |a_i|^2.$$

This will be useful in the next:

Problem 4 (American Mathematical Monthly) Let $P(X) = \sum_{k=0}^{n} a_k X^k$ be a monic polynomial with complex coefficients and roots $z_1, \dots, z_n$. Prove that

$$\frac{1}{n}\sum_{k=1}^{n} |z_k|^2 < 1 + \max_{1\le k\le n} |a_{n-k}|^2 .$$

Solution We have already remarked that

$$|z_1|^2 + \cdots + |z_n|^2 \le n - 1 + \sum_{i=0}^{n-1} |a_i|^2 \le n - 1 + n \max_{1\le k\le n} |a_{n-k}|^2$$

It follows that

$$\frac{1}{n}\sum_{k=1}^{n} |z_k|^2 \le 1 - \frac{1}{n} + \max_{1\le k\le n} |a_{n-k}|^2 \ < 1 + \max_{1\le k\le n} |a_{n-k}|^2$$

and this finishes the proof.

We end this article with a rather challenging problem.

Problem 5 (American Mathematical Monthly) Let $P(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0$ be a polynomial with complex coefficients. Prove that

$$\max_{|z|=1} |P(z)| \ge \sqrt{2|a_0 a_n| + \sum_{i=0}^{n} |a_i|^2}.$$

Solution If $a_0 = 0$, the result follows directly from proposition 3.1, since with the notations of that proposition we clearly have

$$\frac{1}{N}\sum_{i=1}^{N} |P(z_i)|^2 \le \max_{|z|=1} |P(z)|^2$$

and the left-hand side is precisely $\sum_{i=0}^{n} |a_i|^2$.

Suppose that $a_0 \neq 0$ from now on. Write $\frac{a_n}{a_0} = re^{i\theta}$ with $r > 0$ and $\theta \in \mathbf{R}$ and set $z_0 = e^{-i\theta/n}$, so that $\frac{a_n z_0^n}{a_0} = r > 0$ and $|z_0| = 1$. Defining

$$Q(X) := P(Xz_0) = \sum_{k=0}^{n} b_k X^k,$$

we observe that $|b_k| = |a_k z_0^k| = |a_k|$ for all k. Moreover, we have $b_n = a_n z_0^n = ra_0 = rb_0$. It suffices therefore to prove that

$$\max_{|z|=1} |Q(z)| \ge \sqrt{2r|b_0|^2 + \sum_{i=0}^{n} |b_i|^2}.$$

Let $z_1, \dots, z_n$ be the roots of the polynomial $X^n - 1$. Then clearly

$$n \max_{|z|=1} \hat{\mathrm{E}}|Q(z)|^2 \ge \sum_{i=1}^{n} |Q(z_i)|^2 = \sum_{i=1}^{n} (\sum_{k=0}^{n} b_k z_i^k)(\sum_{l=0}^{n} \overline{b_l} z_i^{-l})$$

$$= \sum_{i=1}^{n} \sum_{k,l=0}^{n} b_k \overline{b_l} z_i^{k-l} = \sum_{k,l=0}^{n} b_k \overline{b_l} \sum_{i=1}^{n} z_i^{k-l}.$$

Note that for $0 \leq k, l \leq n$ the number $k - l$ is a multiple of n precisely when $k = l$ or $(k, l) \in \{(n, 0), (0, n)\}$. Therefore proposition 2.1 shows that

$$\sum_{k,l=0}^{n} b_k \overline{b_l} \sum_{i=1}^{n} z_i^{k-l} = n(\sum_{k=0}^{n} |b_k|^2 + b_n \overline{b_0} + b_0 \overline{b_n}) = n(\sum_{k=0}^{n} |b_k|^2 + 2r|b_0|^2).$$

The result follows.

Navid Safaei, Sharif University of Technology, Tehran, Iran