Primitive Sixth Root of Unity and Problem 6 of the 42nd International Mathematical Olympiad

Chan Heng Huat
Department of Mathematics
National University of Singapore
Singapore 117543

Primitive Sixth Root of Unity and Problem 6 of the 42nd International Mathematical Olympiad

We begin our story with the last problem of the 42nd International Mathematical Olympiad:

Proposition 1 (Problem 6). *Let a, b, c, d be integers with $a > b > c > d > 0$. Suppose that*

(1) $$ac + bd = (b + d + a - c)(b + d - a + c).$$

Then $ab + cd$ is not prime.

An elegant solution of the above problem can be found in [3, p. 55-56].

Since the expressions $ab + cd$ and $ac + bd$ are similar, it is natural to ask for a factorization of $ab + cd$ similar to (1). My attempt to find such a factorization leads me to the following table:

a	b	c	d	$ab + cd$	$(ab + cd, b^2 - c^2)$
8	7	3	0	56	8
8	7	5	0	56	8
11	9	5	1	104	15
11	9	6	1	105	21
...	...	...	...	...	...

As usual, (m, n) denote the greatest common divisor of m and n. Note that the table shows that $1 < (ab + cd, b^2 - c^2) < ab + cd$ and this motivates us to formulate the following modification of Proposition 1:

Proposition 2 (Problem 6 (modified)).

Let a, b, c, d be integers with $a \geq b > c > d \geq 0$ and $(a, c) = 1$. Suppose that

$$ac + bd = (b + d + a - c)(b + d - a + c).$$

Then

$$1 < (ab+cd, b^2-c^2) < ab+cd.$$

It is easy to see that Proposition 2 implies Proposition 1. It suffices only to show that $(a,c)=1$. Suppose $(a,c)=r>1$. Then $a=ur, c=vr$ and $ab+cd=r(ub+vd)$. If $ab+cd$ is prime then r must be prime and $ub+vd=1$. Since $u,v,b,d>0$, this is impossible. Now that $(a,c)=1$, we conclude from our result that $ab+cd$ is not a prime since we have found a non-trivial divisor of $ab+cd$, namely, $(ab+cd, b^2-c^2)$.

Before we prove Proposition 2, we need a few Lemmas.

Lemma 3. [4, p. 12]

If n, n_1, and n_2 are natural numbers, $n|n_1n_2$ and $n \not| n_1$, $n \not| n_2$ then

$$\delta = \frac{n_1}{\left(n_1, \dfrac{n_1n_2}{n}\right)}$$

divides n and $1<\delta<n$.

Proof. Now

$$\frac{n_1}{\delta} = \left(n_1, \frac{n_1n_2}{n}\right).$$

Therefore,

$$\frac{n_1}{\delta} \in \mathbf{N}.$$

Hence,

$$n_1 = \frac{n_1}{\delta}k, \frac{n_1n_2}{n} = \frac{n_1}{\delta}l,$$

with $(k,l)=1$. Hence, $k=\delta$, (i.e. $(\delta,l)=1$) and $n_2\delta = nl$. Since $(\delta,l)=1$, $\delta|n$. Therefore δ is a divisor of n. If $\delta=1$ then $n_2=nl$ and therefore, $n|n_2$, a contradiction. If $\delta=n$ then $n|n_1$, again a contradiction. Hence $1<\delta<n$.

Lemma 4. *If k,l are integers such that $k^2+kl+l^2=1$, then*

$$(k,l) = (1,-1), (-1,1), (1,0), (0,1), (-1,0), (0,-1).$$

Proof. From the hypothesis, we conclude that

$$4k^2+4kl+4l^2=4.$$

This implies that

$$(2k+l)^2+3l^2=4.$$

The solutions to this final equation are the six given solutions.

Remarks. The six solutions correspond to the six units in the ring of integers $\mathbf{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. For more details, see [2, p.8, Ex. 12].

Proof of Proposition 2.

To prove the claim, we first observe that the condition (1) is equivalent to

$$(2) \qquad a^2 - ac + c^2 = b^2 + bd + d^2 =: n.$$

We may deduce from (2) that

$$(3) \qquad n^2 = (ab+cd)^2 + (ad-bc-cd)^2 + (ab+cd)(ad-bc-cd)$$

$$(4) \qquad = (ad+bc)^2 + (ab-cd-bc)^2 + (ab-cd-bc)(ad+bc),$$

and

$$(5) \qquad (ab+cd)(ab-cd-bc) = (b^2-c^2)(b^2+bd+d^2).$$

We claim that if $n|(ab+cd)$ then $n|(ad-bc-cd)$.

From (3), we find that

$$4n^2 = (2(ad-bc-cd)+ab+cd)^2 + 3(ab+cd)^2.$$

Since $n|(ab+cd)$, we find that

$$n^2|(2(ad-bc-cd)+ab+cd)^2.$$

Using the fact that $a^2|b^2$ implies that $a|b$ (see [1, p. 22, Ex. 12]), we conclude that

$$n|(2(ad-bc-cd)+ab+cd).$$

This implies that

$$n|2(ad-bc-cd)$$

since $n|(ab+cd)$. Since $\gcd(a,c)=1$, $n=a^2-ac+c^2$ must be odd (by looking at the parity of a and c). This shows that $n|(ad-bc-cd)$.

Now let $ab+cd=kn$ and $ad-bc-cd=ln$. Then we obtain

$$n^2 = k^2n^2 + l^2n^2 + lkn^2,$$

or

$$(6) \qquad 1 = k^2 + kl + l^2.$$

By Lemma 4, the integral solutions to (6) are

$$(k,l) = (1,-1), (-1,1), (1,0), (0,1), (-1,0), (0,-1).$$

Now, $ab+cd>0$ implies that second, fourth, fifth and sixth solutions are inadmissible. If $ad-bc-cd=0$, then $ad=c(b+d)$. Since $(a,c)=1$, we deduce that $c|d$. This is impossible since $c>d$. Hence the third solution is also inadmissible. We therefore conclude that

$$(7) \qquad ab+cd=n \quad \text{and} \quad ad-bc-cd=-n.$$

Adding up these two equations, we conclude that

$$a(b+d)=bc,$$

which is again impossible since $ab>bc$. Hence $n \nmid (ab+cd)$.

Primitive Sixth Root of Unity and Problem 6 of the 42nd International Mathematical Olympiad

Primitive Sixth Root of Unity and Problem 6 of the 42nd International Mathematical Olympiad

If $n|(ab-cd-bc)$ then from (4) and similar argument as above, we conclude that $n|(ad+bc)$ and that

$$ad+bc=n \quad \text{and} \quad ab-cd-bc=-n.$$

This gives

$$ab+ad=cd,$$

and that $a|d$, a contradiction. Hence $n \not| (ab-cd-bc)$.

By (5) and Lemma 3, with $n_1 = ab+cd, n_2 = ab-cd-bc$ and $n = b^2+bd+d^2$, we conclude that

$$1 < \frac{ab+cd}{(ab+cd, b^2-c^2)} < b^2+bd+d^2.$$

Hence,

$$(ab+cd, b^2-c^2) < ab+cd.$$

It remains to show that $(ab+cd, b^2-c^2) > 1$. If $(ab+cd, b^2-c^2) = 1$ then the number

$$\delta = \frac{ab+cd}{(ab+cd, b^2-c^2)} = ab+cd$$

is a divisor of b^2+bd+d^2. But $b^2+bd+d^2 < ab+ab+cd = 2(ab)+cd < 2(ab+cd)$, implies that $n = b^2+bd+d^2 = ab+cd$. However, we have seen previously (see (7)) that $ab+cd = n$ leads to a contradiction. Hence, $(ab+cd, b^2-c^2) > 1$ and our proof is complete.

Concluding Remarks.

1. Expression (3) follows from the fact that x^2+xy+y^2 is the norm of the element $x+y\omega \in \mathbf{Q}(\sqrt{-3})$, where $\omega = \frac{1+\sqrt{-3}}{2}$. Since the norm of $a-c\omega$ and $b+d\omega$ is n, the norm of $(a-c\omega)(b+d\omega)$ must be n^2. Calculating the norm explicitly, we find that the first identity holds.

2. Proposition 2 and its proof are inspired by the proof given in [3, p. 55-56] and [4, p. 225]. It is by coincidence that I turn to page 225 of W. Sierpiński's book and realize that the problem there is related to the IMO's problem.

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1986.
[2] D. A. Marcus, *Number Fields*, Springer-Verlag, New York, 1977.
[3] Mathematical Medley, vol. 29, no. 1, June 2002.
[4] W. Sierpiński, *Elementary Theory of Numbers*, North-Holland, Poland, 1988 (Revised and enlarged by A. Schinzel).