We investigate Problem 6 of the International Mathematical Olympiad of this year This article presents two solutions.

The first one, like the solution of Problem 2, does not make use of any special idea, and does not require anything beyond high-school mathematics, but it starts with a surprising step that might look discouraging at the first sight.

The second solution requires much more mathematical background. It uses as extension of the set of integers, the theory of the so-called Eulerian integers. This is the price for revealing the most probable origin of the problem.

Problem 6. *Let a, b, c, d be integers, such that $a > b > c > d > 0$. Given that*

$$ac + bd = (b + d + a - c)(b + d - a + c), \tag{6}$$

show that $ab + cd$ is not a prime number.

By rearranging equation (6), we have

$$a^2 - ac + c^2 = b^2 + bd + d^2. \tag{7}$$

Let us use this form from now on.

Solution 1: Substitute.

The proof is indirect. Assume that $ab + cd = p$, where p is a prime. We have the simultaneous equations

$$a^2 - ac + c^2 = b^2 + bd + d^2, \quad ab + cd = p. \tag{8}$$

The number of unknowns and equations can be reduced by expressing some appropriate expression out of one equation and substituting it into the other. In order to make calculations more convenient, let us consider everything modulo p.

According to the second equation, $ab \equiv -cd \pmod{p}$. Multiply equation (7) by b^2, and substitute $-cd$ for ab:

$$\begin{aligned} 0 = b^2(b^2 + bd + d^2 - a^2 + ac - c^2) = b^4 + b^3d + b^2d^2 - (ab)^2 + ab \cdot bc - b^2c^2 \equiv \\ \equiv b^4 + b^3d + b^2d^2 - (cd)^2 - cd \cdot bc - b^2c^2 = (b + c)(b - c)(b^2 + bd + d^2) \pmod{p}. \end{aligned}$$

The resulting expression is a product of three factors, one of which is equal to the quantity in equation (7). It follows from the congruence that one of the three factors $b + c$, $b - c$ and $b^2 + bd + d^2$ is divisible by p, as we assumed that p was a prime. The numbers $b + c$ and $b - c$ are positive and less than $ab + cd = p$, and thus cannot be divisible by p. There remains the only possibility that $b^2 + bd + d^2$ is divisible by p. As

$$0 < b^2 + bd + d^2 < ab + ab + cd < 2(ab + cd) = 2p,$$

the number $b^2 + bd + d^2$ can only be divisible by p if it equals p. Hence the simultaneous equations to solve are

$$a^2 - ac + c^2 = b^2 + bd + d^2 = ab + cd = p. \tag{9}$$

No it is easy to show the contradiction. Consider equation (9) modulo a (as a is the largest one of the unknowns). It follows that $c(c-d) = ab+ac-a^2$ is divisible by a. But that is impossible, as a and c are relative primes (or otherwise $ab + cd$ could not be a prime), and $0 < c - d < a$.

Solution 2: With a little help from Euler.

It is clear to anyone who has read about them that equation (7) is closely related to Eulerian integers.

Let ϱ be a complex third root of unity. The complex numbers of the form $x + y\varrho$, where x and y are integers, are called Eulerian integers. Eulerian integers form a lattice of regular triangles in the complex plane (*Figure 1*).

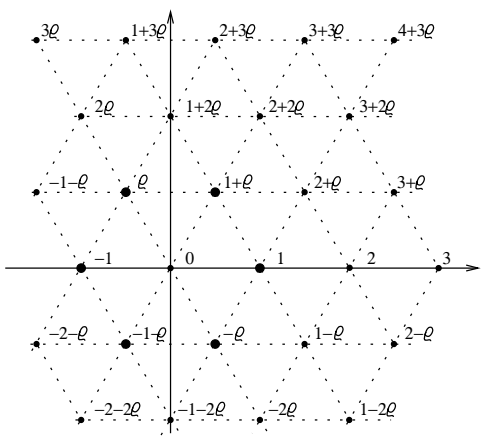

Figure 1

This number set has several remarkable and useful properties. Leonhard Euler also used these numbers when he proved Fermat's last theorem for the exponent 3. Let us briefly summarize the most important concepts and theorems related to Eulerian integers that will be needed in the proof.

Addition, subtraction and multiplication of Eulerian integers are defined in the natural way. Remember that $\varrho^2 = -\varrho - 1$:

$$(x + y\varrho) \pm (u + v\varrho) = (x \pm u) + (y \pm v)\varrho;$$
$$(x + y\varrho)(u + v\varrho) = xu + (xv + yu)\varrho + yv\varrho^2 = (xu - yv) + (xv + uy - yv)\varrho.$$

The commutative, associative and distributive properties of addition and multiplication of integers or real numbers are also valid for Eulerian integers. The properties of the numbers 0 and 1 also remain valid: for example if 0 is added to any Eulerian integer, the sum equals the original number, or 0 times any Eulerian integer is 0.

The *conjugate* of an Eulerian integer $\alpha = x + y\varrho$ is the number $\overline{\alpha} = x + y\varrho^2 = (x - y) - y\varrho$.

There is a very important quantity called the norm of an Eulerian integer. The norm of an Eulerian integer $\alpha = x + y\varrho$ is denoted by $N(\alpha)$ and defined as follows:

$$N(\alpha) = \alpha \cdot \overline{\alpha} = x^2 - xy + y^2.$$

The norm is always a non-negative integer, and 0 is the only number whose norm is 0.

The norm is clearly equal to the square of the modulus of the complex number. Thus the norm of a product is the product of the norms of the factors:

$$N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta).$$

An Eulerian integer α is a *factor* of an Eulerian integer β if there exists an Eulerian integer γ such that $\alpha\gamma = \beta$. It follows from the multiplicativity of the norm that if $\alpha \mid \beta$ then $N(\alpha) \mid N(\beta)$. (The latter divisibility is meant in the set of rational integers.)

There are six Eulerian integers whose norm is 1. They are called *units* and marked in *Figure 1.* The units divide all Eulerian integers.

Two Eulerian integers are said to be associate if they are obtained from each other by multiplication with a unit, that is, by rotation about 0 through a multiple of 60°.

A non-unit Eulerian integer π is said to be *irreducible* if its only factors are the units and itself.

A non-unit and non-zero Eulerian integer π is said to be a *prime* if $\pi \mid \alpha\beta$ implies $\pi \mid \alpha$ or $\pi \mid \beta$ for any Eulerian integers α, β. In order to distinguish the primes in the system of Eulerian integers from real primes, let us call them *Eulerian primes.*

The most important theorems of the theory of Eulerian integers are the following

1. Irreducible Eulerian integers are the same as Eulerian primes.

2. The fundamental theorem of number theory is valid for Eulerian integers, too: Every non-zero and non-unit Eulerian integer can be expressed as a product of Eulerian primes and units, and the representation is unique up to associates, that is, in any two representations, the corresponding factors are associates of each other.

3. The real primes of the form $3k + 2$ are also Eulerian primes. The primes of the form $3k + 1$ can be reduced to the product of two non-associate Eulerian primes (e.g. $7 = (3 + \varrho)(2 - \varrho)$). The prime factor decomposition of 3 is $3 = -\varrho^2(1 - \varrho)^2$.

The theorems show that there is a close relationship between the prime factors of an Eulerian integer α and the prime factors of $N(\alpha)$. The square of each prime factor $3k + 2$ of α occurs in the prime factor decomposition of $N(\alpha)$, and so do the norms of all the other prime factors, which are either 3 or primes of the form $3k + 1$.

For example, let $\alpha = 10 + 8\varrho$. Its resolution into Eulerian primes is $2 \cdot (2 + \varrho)(3 + \varrho)$ and that of its norm is $N(\alpha) = N(2) \cdot N(2 + \varrho) \cdot N(3 + \varrho) = 2^2 \cdot 3 \cdot 7$.

Conversely, the prime factors of $N(\alpha)$ „almost determine" the prime factors of α. All prime factors $3k + 2$ of $N(\alpha)$ are also prime factors of α (with half the exponent), and each factor of 3 in the resolution of $N(\alpha)$ is the norm of the Eulerian prime $1 - \varrho$. The prime factors $3k + 1$ of $N(\alpha)$ are also norms of prime factors of α, but there are two possible Eulerian primes in each case, even if associates are not considered different.

Back to the problem: let $\alpha = a + c\varrho$ and $\beta = b - d\varrho$. According to the given condition, $a^2 - ac + c^2 = b^2 + bd + d^2$, that is, $N(\alpha) = N(\beta)$. We have to prove that $ab + cd$, that is, the „real part" of $\alpha\beta = (ab + cd) + (bc + cd - ad)\varrho$, cannot be a prime.

As $N(\alpha) = N(\beta)$, the prime factors of the two Eulerian integers are „almost the same". They have some prime factors in common, and the remaining factors are pairwise conjugate. This can be put as follows:

$$\alpha = \varepsilon_1 \cdot \pi_1 \cdots \pi_k \cdot \mu_1 \cdots \mu_l \quad \text{and} \quad \beta = \varepsilon_2 \cdot \pi_1 \cdots \pi_k \cdot \overline{\mu}_1 \cdots \overline{\mu}_l, \tag{10}$$

where $\pi_1, \ldots, \pi_k$ and $\mu_1, \ldots, \mu_l$ are Eulerian primes and ε_1, ε_2 are units.

Let $\gamma = \pi_1 \cdot \ldots \cdot \pi_k$ and $\delta = \mu_1 \cdot \ldots \cdot \mu_l$ as above. Then

$$\alpha = \varepsilon_1 \gamma \delta \quad \text{and} \quad \beta = \varepsilon_2 \gamma \overline{\delta}.$$

(It may happen that there are only common or only different prime factors in α and β; then, of course $\gamma = 1$, or $\delta = 1$.)

Consider now the number

$$\alpha\beta = (ab + cd) + (bc + cd - ad)\varrho = \varepsilon_1 \varepsilon_2 \gamma^2 \cdot N(\delta). \tag{11}$$

This number is divisible by $N(\delta)$, and thus $ab + cd$ and $bc + cd - ad$ are also divisible by $N(\delta)$. What remains to prove is that neither $N(\delta) = 1$ nor $ab + cd = N(\delta)$ is possible.

If $N(\delta) = 1$, that is $\delta = 1$, then α and β are associates, which means that they can be obtained from each other by a few 60° rotations about 0. The number of these rotations is determined by the arguments of α and β.

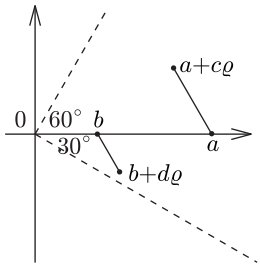

Figure 2

It follows from the condition $a > b > c > d > 0$ that the argument of α is between 0° and 60°, and that of β is between -30° and 0° (*Figure 2*). Thus the difference of the arguments is between 0° and 90°, and hence the angle of rotation is exactly 60°, that is $\alpha = (1 + \varrho)\beta$. But then,

$$\alpha = a + c\varrho = (1 + \varrho)(b - d\varrho) = (b + d) + b\varrho,$$

which is impossible, as $b > c$. Thus the assumption $N(\delta) = 1$ leads to a contradiction.

If $ab + cd = N(\delta)$, then by dividing equation (11) by $N(\delta)$ we get

$$\frac{\alpha\beta}{N(\delta)} = \frac{ab + cd}{N(\delta)} + \frac{ad + bc - cd}{N(\delta)} \cdot \varrho = \varepsilon_1 \varepsilon_2 \cdot \gamma^2.$$

This number, as shown by the right-hand side, is an Eulerian integer. Its argument is the sum of the arguments of α and β, which is between -30° and 60°, and its „real part" is $\dfrac{ab + cd}{N(\delta)} = 1$, by assumption. The only Eulerian integer satisfying this requirement is 1 (*Figure 3*), hence $\varepsilon_1 \varepsilon_2 \gamma^2 = 1$ and $\alpha\beta = N(\delta)$.

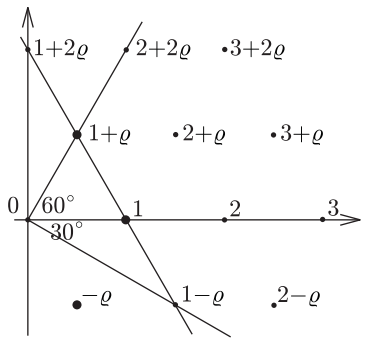

Figure 3

Thus the product of the numbers α and β is the positive real number $N(\delta)$. As $N(\alpha) = N(\beta)$, it follows that the two numbers are conjugates. But then

$$\alpha = a + c\varrho = \overline{\beta} = \overline{b - d\varrho} = b + d(1 + \varrho) = (b + d) + d\varrho,$$

which is impossible, as $c > d$. The assumption $ab + cd = N(\delta)$ also leads to a contradiction. This completes the proof.

Solution 2 not only proves the statement of the problem, but also provides a construction for finding appropriate numbers a, b, c, d with $a > b > c > d$ and

$$a^2 - ac + c^2 = b^2 + bd + d^2.$$

All we need to do is find Eulerian integers of the appropriate arguments.

For example, setting

$$\alpha = a + c\varrho = (4+\varrho)(3+\varrho) = 11 + 6\varrho, \quad \beta = b - d\varrho = (4+\varrho)\overline{(3+\varrho)} = 9 - \varrho,$$

$a = 11$, $b = 9$, $c = 6$ and $d = 1$, with

$$a^2 - ac + c^2 = b^2 + bd + d^2 = 91.$$

(Obviously, $ab + cd = 105$ is not a prime.)