IMO Training Programme UCD March 24 2018.

Thomas J. Laffey.

Algebraic and number-theoretic techniques related to IMO problems.

Problem 1. Let $a > b > c > d > 0$ be integers satisfying $ac + bd = (b + d + a - c)(b + d - a + c)$. Prove that $ab + cd$ is not prime.

Solution: Multiplying out

$$ac + bd = (b + d + a - c)(b + d - a + c) \text{ gives}$$

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

that is

$$a^2 - ac + c^2 = b^2 + bd + d^2 \quad \ldots (1).$$

So the problem reduces to using (1) in some way to show that $ab + cd$ is not a prime number. If we could find a factorization involving $ab + cd$ and other terms, we might be able to use the fact that $ab + cd$ is bigger than similar looking expressions such as $ac + bd$, $ad + bc$, ... since $a > b > c > d$.

The rearrangement inequality states that if

$$x_1 \geq x_2 \geq \cdots \geq x_n \quad \text{and}$$
$$y_1 \geq y_2 \geq \cdots \geq y_n$$

and σ is any permutation of $\{1, 2, \cdots, n\}$, then

$$x_1 y_1 + x_2 y_2 + \cdots + x_n y_n \geq$$

$$x_1 y_{\sigma(1)} + x_2 y_{\sigma(2)} + \cdots + x_n y_{\sigma(n)} \geq$$

$$x_1 y_n + x_2 y_{n-1} + \cdots + x_{n-1} y_2 + x_n y_1$$

For example $3 > 2 > 1$
$5 > 4 > 2$

Then $3 \times 5 + 2 \times 4 + 1 \times 2 = 25$ is the biggest number we can get by multiplying each number in the first list by a corresponding number in the second list and adding, and

$$3 \times 2 + 2 \times 4 + 1 \times 5 = 19$$

is the smallest.

Notice that if $x > y$ and $u > v$, then

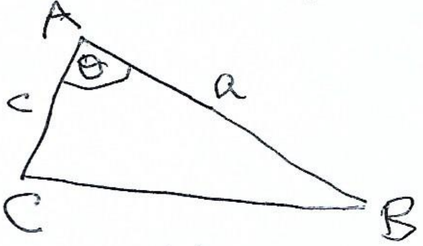
$$(xu + yv) - (xv + yu) =$$
$$(x - y)(u - v) > 0.$$

The result is proved by repeatedly using swops like this.

[For detailed discussion on this topic, see its Wikipedia page].

Going back to Problem 1, we ask if the product $ab + cd$ or, say, $a^2 - ac + c^2$ arises in some other context'.

Does $a^2 - ac + c^2$ remind you of the cosine rule



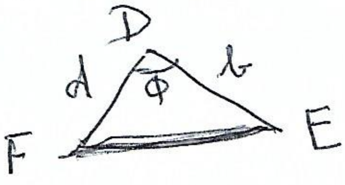
$$|BC|^2 = a^2 + c^2 - 2ac\cos\theta$$

$$= a^2 + c^2 - ac \quad \text{if } \cos\theta = 1/2,$$

that is, if $\theta = 60°$.

Now, look at $b^2 + bd + d^2$.

$$|FE|^2 = b^2 + d^2 - 2bd\cos\phi$$

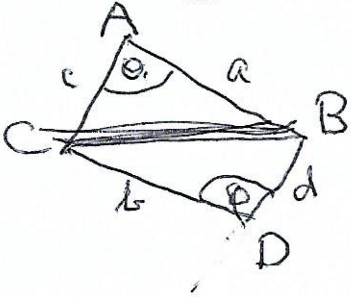


$$= b^2 + d^2 + bd, \text{ if } \cos\phi = -\tfrac{1}{2},$$

that is $\phi = 120°$.

Notice that $\theta + \phi = 180°$ and that $|BC| = |FE|$ by equation (1)

This suggests making a cyclic quadrilateral



$\theta = 60°$, $\phi = 120°$.

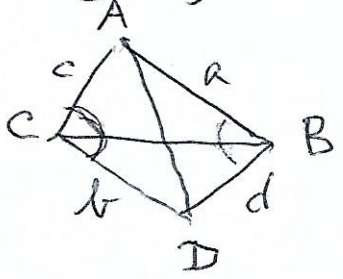
Now we can interpret $ab + cd$. Recall Ptolemy's Theorem. It states that if $ABDC$ (as in the picture on last page), is a cyclic quadrilateral, then $|AB||CD| + |AC||BD| = |AD||BC|$,

that is

$$\begin{aligned} ab + cd &= |AD||BC| \\ &= |AD|(a^2 - ac + c^2)^{1/2} \ldots (2) \end{aligned}$$

If we have a formula for $|AD|$, then we might be able to get a contradiction to the statement that $ab + cd$ is prime.

To calculate $|AD|$ is straightforward.



Apply the cosine rule on the two triangles ABD, ACD:

$$|AD|^2 = a^2 + d^2 - 2ad \operatorname{Cos} \angle ABD,$$

$$|AD|^2 = b^2 + c^2 - 2bc \operatorname{Cos} \angle ACD.$$

Since $ABDC$ is a cyclic quadrilateral,

$$\angle ABD + \angle ACD = 180^\circ, \quad \text{so}$$

$$\operatorname{Cos} \angle ABD = - \operatorname{Cos} \angle ACD.$$

So to get the cosines to cancel out, we multiply the first equation for $|AD|^2$ by bc and the second by ad and add. This gives

$$\begin{aligned} |AD|^2 (bc + ad) &= (a^2 + d^2) bc + (b^2 + c^2) ad \\ &= (ab + cd)(ac + bd) \ldots (3) \end{aligned}$$

Squaring equation (2) gives

$$(ab+cd)^2 = |AD|^2 \ (a^2-ac+c^2) \quad , \text{ so}$$

$$(ab+cd)^2(ad+bc) = |AD|^2(ad+bc)(a^2-ac+c^2)$$

$$= (ab+cd)(ac+bd)(a^2-ac+c^2),$$

using (3).

Hence

$$(ab+cd)(ad+bc) = (ac+bd)(a^2-ac+c^2) \quad \ldots(4).$$

Now, if $ab+cd$ is a prime number, it must divide one of the factors in the right-hand-side of (4), since the factors in (4) are all integers.

But $a > b > c > d$, so $ab+cd > ac+bd$

and $2(ab+cd) > 2ab+cd > b^2+bd+d^2 \ldots (5)$

Since $a^2-ac+c^2 = b^2+bd+d^2$, ~~then~~ if $ab+cd$ is prime, $ab+cd$ must divide b^2+bd+d^2 and therefore must equal b^2+bd+d^2, using (5). But then (4) says $ad+bc = ac+bd$,

So $(a-b)(d-c) = 0$, which is false.

This contradicts the supposition that $ab+cd$ is prime. Hence $ab+cd$ is not prime, as required

---

The geometrical interpretation gives a natural way to find equation (4). But of course, one might arrive at (4) by trial and error searching, guessing and checking etc. For example, seeing the given factorization of $\underline{ac+bd}$ and the problem relating to $\underline{ab+cd}$, and a^2-ac+c^2 turning up in expanding the given information, one would be tempted to consider products of $ab+cd$, $ac+bd$, $ad+bc$ and a^2-ac+c^2 and hope to get some equations. In the IMO, one has time to try out many different approaches and most students who solved this problem arrived at the factorization (4) by such trial and error methods. Some South Korean students used a different approach. The polynomial $a^2-ac+c^2 = (a+\omega c)(a+\bar{\omega} c)$, where ω is the complex number $\frac{-1+i\sqrt{3}}{2}$, $\bar{\omega} = \frac{-1-i\sqrt{3}}{2}$, where $i=\sqrt{-1}$. Here $\bar{\omega} = \frac{1}{\omega}$, $\omega^2+\omega+1=0$, $\omega^3=1$. Let $E = \{a+c\omega \mid a, c \text{ integers}\}$. Then E is an integral domain (like the set of integers): E is closed under addition, subtraction and multiplication and addition and multiplication are associative and commutative and satisfy distributive laws, $0, 1 \in E$ and if $\alpha, \beta \in E$ with $\alpha\beta = 0$, then either $\alpha = 0$ or $\beta = 0$. E is called Eisenstein ring (Eisenstein visited Dublin in 1843, around the time he invented his ring). There are exactly six elements $x \in E$ such that their inverse $\frac{1}{x}$ is also in E. These form $G = \{1, -1, \omega, -\omega, \bar{\omega}, -\bar{\omega}\}$ and G is a group under multiplication - the group of sixth roots of unity in the complex number field $\mathbb{C}$. There is a concept of prime in E. Every prime number $p \equiv 2 \bmod 3$ turns out to be a prime in E also, but a prime $p \equiv 1 \bmod 3$ factors as the product of two primes $a + c\omega$, $a + c\bar{\omega}$ in E, so $p = (a+c\omega)(a+c\bar{\omega}) = a^2 - ac + c^2$. The prime 3 also factors in E as $(2+\omega)(2+\bar{\omega})$ Starting from the equation $a^2 - ac + c^2 = b^2 + bd + d^2$ and how it factors into a product of primes in E gives another approach to finding the factorization (4).

An analogue of the Eisenstein ring is the ring $\mathbb{Z}[i]$ of Gaussian integers.

$\mathbb{Z}[i]$ is the set of all complex numbers of the form $z=a+bi$, where a, b are integers and $i=\sqrt{-1}$. Writing $\bar{z}=a-bi$ ($\bar{z}$ is called the complex conjugate of z), we have $z\bar{z}=a^2+b^2$ and $\overline{z_1 z_2}=\bar{z}_1\bar{z}_2$ for all $z, z_1, z_2 \in \mathbb{C}$. There is also a concept of prime in $\mathbb{Z}[i]$. Every ordinary prime number $p \equiv 3 \bmod 4$ remains a prime in $\mathbb{Z}[i]$ but a prime number $p \equiv 1 \bmod 4$ can be written as $p=a^2+b^2$ for some $a, b \in \mathbb{Z}$, (This result was first proved by Fermat Thus $p=(a+ib)(a-ib)$. Corresponding to G in E, $H=\{1,-1,i,-i\}$ is a group of order 4 and $1,-1,i,-i$ are the only elements x in $\mathbb{Z}[i]$ such that $\frac{1}{x}$ is also in $\mathbb{Z}[i]$. Both $\mathbb{Z}[i]$ and E are unique factorization domains - when one writes a element $z \neq 0$ as a product of primes in E (or $\mathbb{Z}[i]$), the product is unique up to multiplication by elements of G (or H). $\mathbb{Z}[i]$ is often used in solution to the (harder) IMO number theory questions

Ptolemy's Theorem and its corollaries are often applicable to IMO geometry problems about quadrilaterals and other polygons. Similarly, the theorems of Ceva and Menelaus are often applicable in problems about collinearity and concurrence.

The book Geometry Revisited by Coxeter and Greitzer is a great source for results of this type.

Some exercises

1. Find (with proof) all positive integers n such that $n + s(n) = 2001$, where $s(n)$ is the sum of all the digits of n.

2. Prove that for any positive real numbers a, b, c,

$$\frac{a}{10b+11c} + \frac{b}{10c+11a} + \frac{c}{10a+11b} \geqslant \frac{1}{7}.$$

3. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be the four roots of the equation $x^4 - 18x^3 + kx^2 + 90x - 2000 = 0$, where k is a constant. If $\alpha_1\alpha_2 = 50$, find the value of k.

4. For each positive integer n, let A_n be the (unique) positive integer which satisfies

$$(\sqrt{3}+1)^{2n} \leq A_n < (\sqrt{3}+1)^{2n} + 1$$

Prove that A_n is divisible by 2^{n+1}.