A Short Solution of a Problem in Combinatorial Geometry

MARC NOY
Dept. Matemàtica Aplicada II
Universitat Politècnica de Catalunya
08028 Barcelona, Spain

The solution of the classical problem: Into how many regions is a circle divided if n points on its circumference are joined by chords with no three concurrent? is well known to be

$$\binom{n}{4}+\binom{n}{2}+1$$

and can be found in many references. It appears in [2] as problem 47, although the two solutions provided are quite involved. Because the first values of n yield 1, 2, 4, 8, 16, and the next one 31, it appears in [1] as one of several examples of patterns that seem to appear in a sequence of numbers, but turn out not to be correct. The solution there considers the circle as a planar map with $V=n+\binom{n}{4}$ vertices—the original n points and an intersection of chords for each choice of 4 of those points. There are 4 ends of edges at each intersection and $n+1$ at each point, so that $E=\frac{1}{2}n(n+1)+2\binom{n}{4}$ and Euler's formula $R=E-V+1$ gives the result.

In this note we offer a direct combinatorial proof without any algebraic calculation. Imagine that we draw the chords one after another, keeping count of the number of regions created each time. Starting with one region, the whole circle, the first chord creates one more region. Any subsequent chord will create one new region, plus as many more as the number of intersections it produces with the chords previously

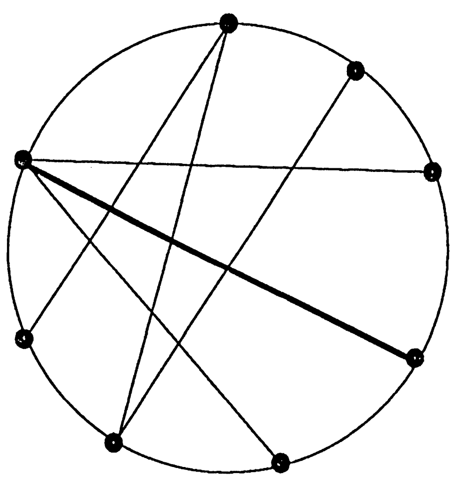

FIGURE: Adding the thick chord creates 4 new regions.

drawn (see FIGURE). This number will of course depend on the particular chord selected but at the end there will be one new region for every chord and one for every intersection. The number of chords is $\binom{n}{2}$ and the number of intersections is $\binom{n}{4}$ as before. Hence the number of regions is $1+\binom{n}{2}+\binom{n}{4}$.

REFERENCES

1. R. K. Guy, The strong law of small numbers, *Amer. Math. Monthly* (1988), 697–712.
2. A. M. Yaglom and I. M. Yaglom, *Challenging Mathematical Problems with Elementary Solutions*, Vol. I, Dover Publications, Mineola, NY, 1987.

On the Order of a Product in a Finite Abelian Group

DIETER JUNGNICKEL
Universität Augsburg
D-86135 Augsburg, F.R. Germany

The following result from elementary group theory is included in virtually every course in abstract algebra:

LEMMA 1. *Let a and b be two elements of a finite abelian group G with orders m and n, respectively. If m and n are co-prime, then the product ab has order mn.*

Lemma 1 can be used to find elements of increasingly larger order in G. This has many interesting applications, both theoretic and algorithmic. One usually applies Lemma 1 to show that G is cyclic if, and only if, its exponent agrees with its order; this result in turn is used to show that a finite subgroup of the multiplicative group of a field is cyclic. (See, e.g., Jacobson [**1**, Theorems 1.4 and 2.18] or van der Waerden [**5**, §§42 and 43].) Lemma 1 is also the basis of the standard algorithm (due to Gauss) for determining primitive elements for finite fields (i.e., generators for the multiplicative groups) and then primitive polynomials, see e.g. Jungnickel [**3**, §2.5]. These are important tasks if one actually wants to perform arithmetic in finite fields, which in turn is fundamental for applications, e.g. in cryptography. See [**3**] (and the references cited there) for more information on this topic.

In some of my algebra classes, students asked the quite natural question: What happens in the situation of Lemma 1 if one drops the hypothesis that m and n are co-prime.* Trivially, $(ab)^{\operatorname{lcm}(m,n)}=1$, so that the order of ab satisfies

$$o(ab) \mid \operatorname{lcm}(m,n). \tag{1}$$

Usually, some student suggests that one should actually have equality in (1). Though this might seem a reasonable conjecture, it is not difficult to find counterexamples. Here is a simple series of such examples.

*I do not know of any textbook treating this question. Weak versions of some of the results below (i.e., Corollary 1, the special case $f=d$ of Lemma 3 and the corresponding construction) were already obtained in [**2**].