

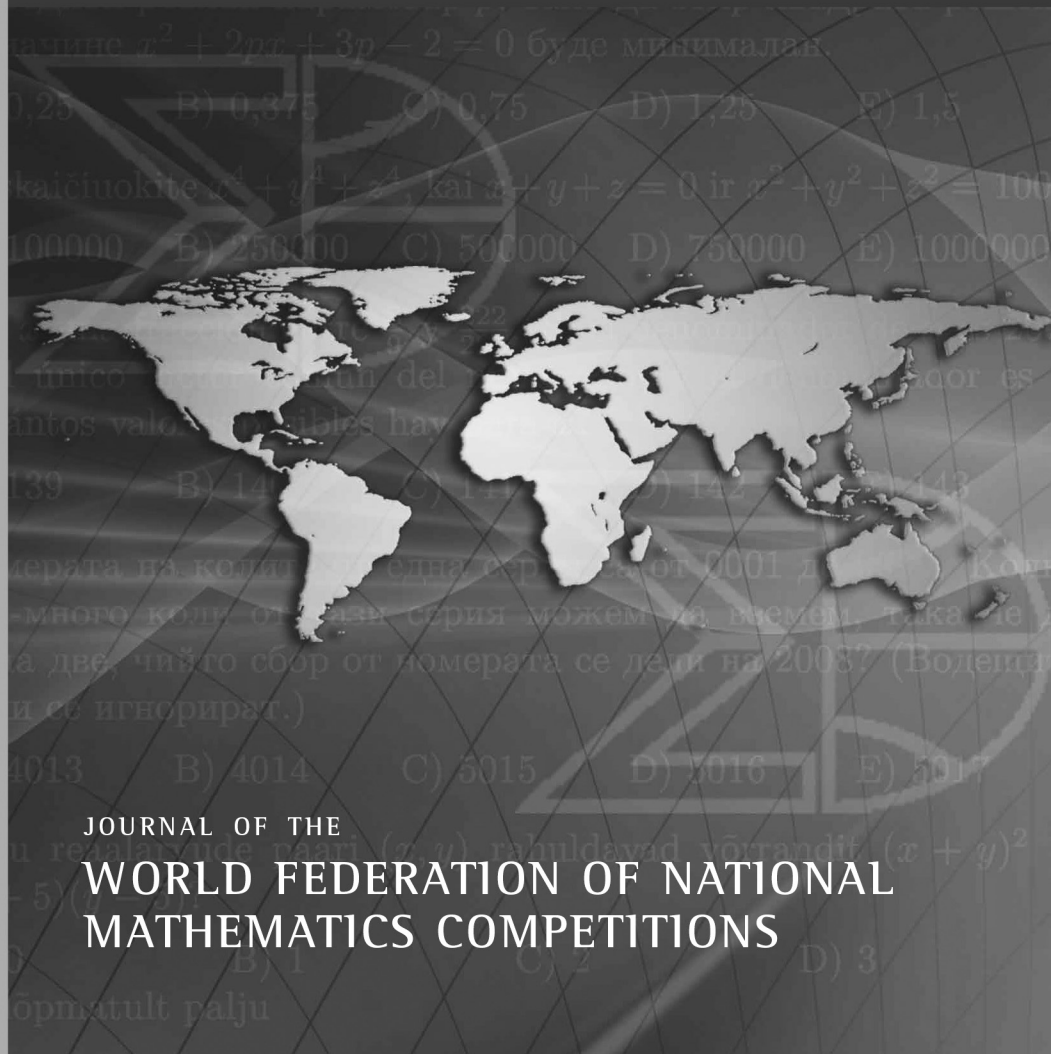
MATHEMATICS COMPETITIONS



JOURNAL OF THE
**WORLD FEDERATION OF NATIONAL
MATHEMATICS COMPETITIONS**



MATHEMATICS COMPETITIONS



JOURNAL OF THE
WORLD FEDERATION OF NATIONAL
MATHEMATICS COMPETITIONS



MATHEMATICS COMPETITIONS

Journal of the World Federation of National Mathematics Competitions
ISSN 1031-7503

Published biannually by
Australian Maths Trust
170 Haydon Drive
Bruce ACT 2617
Australia

Articles (in English) are welcome.
Please send articles to:
Professor María Elizabeth Losada
Universidad Antonio Nariño
Bogotá
Colombia
director.olimpiadas@uan.edu.co

The views expressed here are those of the authors and do not necessarily represent the views of the Australian Mathematics Trust.

Typesetting by
Rogelio F. CHOVET
rogelio@chovet.com

© 2020 Australian Mathematics Trust, AMTT Limited ACN 083 950 341

Contents

From the President	5
Editor's Page	6
From the Lifting the Exponent Lemma to Elliptic Curves with Isomorphic Groups of Points: How Olympiad Mathematics Influences Mathematical Research <i>Clemens Heuberger</i>	8
Using Inversion in Theorems from Classical Geometry and for Solving Problems <i>Kiril Bankov</i>	22
Some Polynomial Morsels from the Iranian Mathematical Olympiads <i>Navid Safaei</i>	36
<i>pqr</i> Inequality <i>Robert Bosch</i>	60
Remembering John Horton Conway <i>Peter James Taylor</i>	79
International Mathematics Tournament of Towns Selected Problems from the Spring 2019 Papers <i>Andy Liu</i>	82
The 60th International Mathematical Olympiad <i>Angelo Di Pasquale</i>	89

World Federation of National Mathematics Competitions

Executive

President:

Kiril Bankov
University of Sofia
Sofia, BULGARIA
kbankov@fmi.uni-sofia.bg

Senior Vice President:

Robert Geretschläger
BRG Kepler
Graz, AUSTRIA
robert@rgeretschlaeger.com

Vice Presidents:

Sergey Dorichenko
School 179
Moscow, RUSSIA
sdorichenko@gmail.com

Krzysztof Ciesielski
Jagiellonian University
Krakow, POLAND
Krzysztof.Ciesielski@im.uj.edu.pl

Publications Officer:

Maria Falk de Losada
Universidad Antonio Nariño
Bogota, COLOMBIA
mariadelosada@gmail.com

Secretary:

David Crawford
Leicester Grammar School
Leicester, UK
davidmc103@hotmail.com

*Immediate Past President
Chair, Award Committee:*

Alexander Soifer
University of Colorado
Colorado Springs, USA
asoifer@uccs.edu

Treasurer:

Peter Taylor
University of Canberra
Canberra, AUSTRALIA
pjt013@gmail.com

Past Presidents:

Maria Falk de Losada
Universidad Antonio Nariño
Bogotá, COLOMBIA
mariadelosada@gmail.com

Petar Kenderov
Bulgarian Academy of Sciences
Sofia, BULGARIA
vorednek@gmail.com

Regional Representatives

Africa:

Liam Baker
University of Stellenbosch
Stellenbosch, SOUTH AFRICA
bakerbakura@gmail.com

Asia:

M. Suhaimi Ramly
Ardent Educational Consultants Sdn. Bhd
Kuala Lumpur, MALAYSIA
msuhaimi@gmail.com

Europe:

Francisco Bellot Rosado
Royal Spanish Math Society
Valladolid, SPAIN
franciscobellot@gmail.com

Jaroslav Svrcek
Palacky University
Olomouc, CZECH REPUBLIC
jaroslav.svrcek@upol.cz

North America:

Alexander Soifer
University of Colorado
Colorado Springs, USA
asoifer@uccs.edu

Oceania:

Peter Taylor
University of Canberra
Canberra, AUSTRALIA
pjt013@gmail.com

South America:

Maria Falk de Losada
Universidad Antonio Nariño
Bogota, COLOMBIA
mariadelosada@gmail.com

For WFNMC Standing Committees please refer to “About WFNMC”
section of the WFNMC website <http://www.wfmc.org/>.

From the President

Dear readers of *Mathematics Competitions* journal!

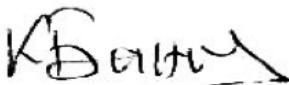
When I first wrote this greeting, I said that we were on the eve of the next edition of the most significant event in mathematics education – the 14th International Congress of Mathematics Education, “ICME-14”, which had been expected to be held in Shanghai, China. Now I have to say that the Congress has been postponed by one year. This is due to the global pandemic caused by the coronavirus disease. The congress organizers believe that even the postponement poses many challenges, but that this is the best decision in the current situation, and they have pledged to do everything possible to ensure a full-fledged and successful realization of this important congress.

I hope that the scientific program of ICME-14 will remain the same. For now, Topic Study Group TSG-46 “Mathematical Competitions and Other Challenging Activities” at ICME-14 designed to gather a group of participants who are interested in the specific features, trends and needs of “Competition Mathematics” is the place where the WFNMC members may bring ideas for discussion. Please check whether TSG-46 will ask for additional proposals, and if so, submit your contributions.

The traditional one-day mini-conference of WFNMC that usually takes place the day before the opening of the congress has also been postponed by one year. This is a good chance for those of you who were unable to send their proposals before, to do so now. Please take this opportunity and submit contributions for the mini-conference. As usual, papers presented at the mini-conference can be published in the journal *Mathematics Competitions*.

Due to the coronavirus disease, there are not many happenings in 2020, but it seems that the summer of 2021 will be full of exciting scientific events in the world of mathematics competitions. I am sure we are all looking forward to an enjoyable time next year.

My best regards,



Kiril Bankov
President of WFNMC

March, 2020

Editor's Page

Dear Competitions enthusiasts,
readers of our *Mathematics Competitions* journal!

Following the example of previous editors, I invite you to submit to our journal *Mathematics Competitions* your creative essays on a variety of topics related to creating original problems, working with students and teachers, organizing and running mathematics competitions, historical and philosophical views on mathematics and closely related fields, and even your original literary works related to mathematics.

Just be original, creative, and inspirational. Share your ideas, problems, conjectures, and solutions with all your colleagues by publishing them here.

We have formalized the submission format to establish uniformity in our journal.

Submission Format

Format: should be LaTeX, TeX, or Microsoft Word, accompanied by another copy in pdf.

Illustrations: must be inserted at about the correct place of the text of your submission in one of the following formats: jpeg, pdf, tiff, eps, or mp. Your illustration will not be redrawn. Resolution of your illustrations must be at least 300 dpi, or, preferably, done as vector illustrations. If a text is needed in illustrations, use a font from the Times New Roman family in 11 pt.

Start: with the title in BOLD 14 pt, followed on the next line by the author(s)' name(s) in italic 12 pt.

Main Text: Use a font from the Times New Roman family in 11 pt.

End: with your name-address-email and your website (if applicable).

Include: your high resolution small photo and a concise professional summary of your works and titles.

Please submit your manuscripts to María Elizabeth Losada at
director.olimpiadas@uan.edu.co

We are counting on receiving your contributions, informative, inspired and creative.

Best wishes,

María Falk de Losada
Acting Editor, Mathematics Competitions
Past President, WFNMC

From the Lifting the Exponent Lemma to Elliptic Curves with Isomorphic Groups of Points: How Olympiad Mathematics Influences Mathematical Research

Clemens Heuberger (clemens.heuberger@aau.at)

Institut für Mathematik Alpen Adria Universität Klagenfurt, Austria



Clemens Heuberger is Professor of Discrete Mathematics at the University of Klagenfurt, Austria. As a high school student, he competed in various mathematical contests. Since 2014, has served as the scientific director of the Austrian Mathematical Olympiad. He was awarded his PhD in number theory at Graz University of Technology in 1999.

Abstract

For several years, the so-called “Lifting the Exponent Lemma” has been considered to be part of the curriculum for contestants preparing for international mathematical competitions. However, it is hard to find it in the scientific literature. In this talk, we review the lemma and then report on a scientific paper which after translating the original question on elliptic curves to an elementary problem just boils down to suitably applying the lemma.

1 Introduction

About ten years ago, an idea which seems to have been folklore for quite some time became known as the “Lifting the Exponent Lemma” in the mathematical olympiad community [4, 1]. In this survey, we first recall the lemma including a sketch of the proof. We then proceed to an application in a recent mathematical olympiad problem in the second part of this survey. In the third part, we consider an application of the lemma in the scientific literature in particular in a study [2] concerning isomorphic point groups of elliptic curves. We will first introduce the necessary background to formulate the problem and then proceed to a characterisation of the problem by Wittmann in elementary terms. In the last part of the paper, we will then sketch the reduction of the elementary problem by means of olympiad mathematics to a question whose solution is essentially equivalent to the Lifting the Exponent Lemma.

2 Lifting the Exponent Lemma

In this section, we recall the Lifting the Exponent Lemma. As usual, we denote the p -adic valuation of an integer x (the exponent of p in the prime factor decomposition of x) by $v_p(x)$. For example,

$$v_2(2^4 \cdot 3) = 4; \quad v_3(2^4 \cdot 3) = 1; \quad v_5(2^4 \cdot 3) = 0.$$

Lemma 1 (Lifting the Exponent [1]). *Let p be a prime, $a \equiv b \not\equiv 0 \pmod{p}$ and $n \geq 1$. If $p = 2$ and n is even, additionally assume that $a \equiv b \pmod{4}$.*

Then

$$v_p(a^n - b^n) = v_p(a - b) + v_p(n).$$

We note that the lemma is incorrect without the additional condition for $p = 2$: take $p = 2$, $n = 2$, $a = 3$ and $b = 1$, then

$$v_2(3^2 - 1^2) = v_2(8) = 3 > 2 = v_2(3 - 1) + v_2(2).$$

Actually, the well-known fact that the square of any odd integer is congruent to 1 modulo 8 strikes once more.

Proof of Lemma 1. We proceed in three steps.

We first consider the case that n is coprime to p . We decompose $a^n - b^n$ as

$$a^n - b^n = (a - b) \sum_{j=0}^{n-1} a^j b^{n-1-j}. \quad (1)$$

By the assumption that $a \equiv b \pmod{p}$, we have

$$\sum_{j=0}^{n-1} a^j b^{n-1-j} \equiv \sum_{j=0}^{n-1} a^j a^{n-1-j} = \sum_{j=0}^{n-1} a^{n-1} = na^{n-1} \not\equiv 0 \pmod{p},$$

because a is coprime to p by assumption.

This implies that $\sum_{j=0}^{n-1} a^j b^{n-1-j}$ is not divisible by p and therefore, (1) implies that $v_p(a^n - b^n) = v_p(a - b)$. This is exactly the assertion of the Lifting the Exponent Lemma in this case.

We next consider the case when $n = p$. By assumption, we can write $a = b + cp^k$ where $k = v_p(a - b) \geq 1$ and c is coprime to p . Note that the additional assumption guarantees that $k \geq 2$ if $p = 2$. We compute $a^p - b^p$ modulo p^{k+2} by the binomial theorem:

$$\begin{aligned} a^p - b^p &= (b + cp^k)^p - b^p \\ &= \left(b^p + cp^{k+1}b^{p-1} + \frac{p(p-1)}{2}c^2p^{2k}b^{p-2} + \sum_{j=3}^p \binom{p}{j} c^j p^{jk} b^{p-j} \right) - b^p. \end{aligned}$$

As $jk \geq k + 2$ for $j \geq 3$ because of $k \geq 1$, we certainly have

$$a^p - b^p \equiv cp^{k+1}b^{p-1} + \frac{p(p-1)}{2}c^2p^{2k}b^{p-2} \pmod{p^{k+2}}.$$

If p is odd, then $(p-1)/2$ is an integer and the second summand is divisible by p^{2k+1} which is divisible by p^{k+2} . If $p = 2$, however, we have to use the assumption that $k \geq 2$ to see that p^{2k} is divisible by p^{k+2} . So, in any case, we have

$$a^p - b^p \equiv cb^{p-1}p^{k+1} \pmod{p^{k+2}}.$$

By assumption, cb^{p-1} is coprime to p . Therefore, $v_p(a^p - b^p) = k + 1 = v_p(a - b) + v_p(p)$, as required.

We now turn to the general case where $n = p^t m$ for some $t \geq 0$ and some integer m which is coprime to p . We prove the lemma by induction on t . For $t = 0$, the assertion has been shown in our first case. The induction step from t to $t + 1$ then follows from our second case together with the induction hypothesis:

$$\begin{aligned} v_p(a^{p^{t+1}m} - b^{p^{t+1}m}) &= v_p((a^{p^t m})^p - (b^{p^t m})^p) \\ &= v_p(a^{p^t m} - b^{p^t m}) + 1 = v_p(a - b) + t + 1. \end{aligned}$$

□

3 An Olympiad Problem

There are plenty of examples of olympiad problems which can be solved by the Lifting the Exponent Lemma, see [1, 4]. We add one recent problem of the Austrian Mathematical Olympiad to the list. In this case, using the Lifting the Exponent Lemma is optional.

Problem 1 (Austria, 2018, Final Round/6 (Walther Janous)).
Determine all digits z such that for each integer $k \geq 1$ there exists an integer $n \geq 1$ with the property that the decimal representation of n^9 ends with at least k digits z .

Solution. Answer: This is possible for $z \in \{0, 1, 3, 7, 9\}$.

For $z = 0$ we easily find $n = 10^\ell$ with an integer ℓ such that $9\ell \geq k$.

For $z \in \{2, 4, 6, 8\}$ the number n^9 is even and therefore n must be even, too, and hence n^9 must be divisible by 2^9 . However, numbers ending with 222, 444 or 666 are not divisible by 8, and numbers ending with 8888 are not divisible by 16. Therefore, there does not exist a solution for these values of z .

Similarly, for $z = 5$ the number n^9 is divisible by 5, therefore n itself is divisible by 5, too, and therefore, n^9 must be divisible by 5^9 . However, numbers ending with 55 are not divisible by 25.

For $z \in \{1, 3, 7, 9\}$, let $b := (zzz \dots z)_{10}$ with k digits z . We have to prove that there exists some integer n such that $n^9 \equiv b \pmod{10^k}$. We do this by proving that taking the ninth power is a surjective map from the set of primitive residue classes modulo 10^k to itself (a residue class modulo 10^k is said to be primitive if its elements are coprime to 10^k). As this is a finite set, the map is surjective if and only if it is bijective and if and only if it is injective. Thus we assume that $n^9 \equiv m^9 \pmod{10^k}$ for some m and n which are coprime to 10. This implies that $n^9 \equiv m^9 \pmod{10}$. By Euler's theorem, $n^4 \equiv 1 \pmod{10}$ and therefore $n \equiv m \pmod{10}$. The Lifting the Exponent Lemma implies that $k \leq v_p(n^9 - m^9) = v_p(n - m) + v_p(9) = v_p(n - m) + 2$ for $p \in \{2, 5\}$. This implies that $n \equiv m \pmod{10^k}$. We therefore proved that taking the ninth power is injective. \square

Of course, there are other solutions to this problem; in particular taking the r th power of $n^9 \equiv b \pmod{10^k}$ where r is the inverse residue of 9 modulo $\varphi(10^k)$. Another approach is via Hensel lifting.

In fact, the problem was solved by two students out of 24 participating in the final round of the Austrian Mathematical Olympiad; both students qualified for IMO and both obtained a bronze medal there.

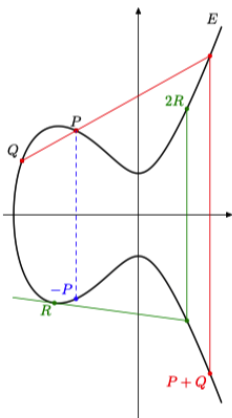


Figure 1: Elliptic curve $E: y^2 = x^3 + \frac{26}{9}x^2 + 1$ over \mathbb{R}

4 Elliptic Curves

As announced in the introduction, we will consider an application of the Lifting the Exponent Lemma to a problem on isomorphic point groups of elliptic curves. We collect the necessary background on elliptic curves in this section.

The simplest definition of an elliptic curve is to define it via its affine equation in Weierstrass form

$$y^2 = x^3 + ax^2 + bx + c$$

for given constants a , b and c where the cubic polynomial on the right side is assumed to have no multiple roots. An example of an elliptic curve over the reals is shown in Figure 1.

We define a special addition on this curve: For two (distinct) points P and Q on the curve, we take the line through P and Q , find its third intersection with the curve and reflect that point about the horizontal axis to obtain $P + Q$, see Figure 1.

To compute $R + R$, i.e., doubling a point, we take the tangent through R as the line.

It is obvious that this operation is commutative, i.e., $P + Q = Q + P$. When including a point 0 at infinity, we have $P + 0 = P$ and $-P$ is the reflection of P about the horizontal axis. It is far from obvious from this approach that the operation is in fact associative: $(P + Q) + R = P + (Q + R)$ for all points P , Q and R . See for instance Knapp's book [3] for an elementary proof. So the set of points together with the point at infinity form a commutative group.

There are many instances where elliptic curves are of interest within mathematics (for instance, the proof of Fermat's last theorem heavily relies on elliptic curves, among other topics), but elliptic curves also have applications, e.g., in cryptography. There, the essential feature is that scalar multiplication is considered to be a "one-way-function": for $n \in \mathbb{Z}$ and P on the curve, the multiple $nP = P + \dots + P$ (with n summands P) can be computed efficiently by at most $2 \log_2 n$ additions or doubling operations; the inverse operation (given nP and P , compute n), however, seems to be intractable in reasonable time. For these purposes, it is more convenient to consider elliptic curves over a finite field instead of the rationals.

Therefore, we will now replace the field of real numbers by a finite field \mathbb{F}_q with q elements for some prime power q , for instance the residue classes modulo some prime in \mathbb{Z} . For completeness be advised that if $1 + 1 = 0$ (e.g., integers modulo 2) or $1 + 1 + 1 = 0$ (e.g., integers modulo 3), the Weierstrass form has to be modified to the so-called long Weierstrass form.

A map φ between two elliptic curves E and E' is said to be a homomorphism if $\varphi(P + Q) = \varphi(P) + \varphi(Q)$ for all points P and Q on E . If E and E' coincide, we say that φ is an endomorphism of E .

5 Problem Formulation

We are now able to formulate the research question: Let q be the power of a prime, \mathbb{F}_q be a field with q elements and E and E' be elliptic curves over \mathbb{F}_q such that E and E' have the same number of points over \mathbb{F}_q .

The question then is to find all $k \geq 1$ such that the point groups of E and E' over the field extension \mathbb{F}_{q^k} are isomorphic, i.e., there exists a bijective homomorphism between E and E' .

An important step has been provided by Wittmann [5]. Its formulation, however, needs some more notation. The Frobenius endomorphism τ of an elliptic curve over \mathbb{F}_q is the map which sends a pair (x, y) to (x^q, y^q) . In fact, it is an endomorphism because of the well-known fact that the binomial coefficient $\binom{p}{j}$ is divisible by p for $0 < j < p$ and prime p ; in our case, we use the prime p of which q is a power.

It is a known, but non-trivial, result that for each point P of the curve, we have

$$\tau^2(P) - (q + 1 - n)\tau(P) + qP = 0$$

where n denotes the number of points on the curve. Of course, the additions and subtractions occurring in this equations are meant to be instances of our special operation on the elliptic curve. Thus we may identify the endomorphism τ of the curve with a root of the quadratic equation

$$\tau^2 - (q + 1 - n)\tau + q = 0;$$

we also denote this root by τ . A famous result by Hasse ensures that this root τ is never a real number. So we can write τ in the form $\tau = a + b\delta$ for suitable $a, b \in \mathbb{Z}$ and

$$\delta = \begin{cases} \sqrt{m} & \text{if } m \equiv 2 \text{ or } 3 \pmod{4}, \\ \frac{1+\sqrt{m}}{2} & \text{if } m \equiv 1 \pmod{4} \end{cases}$$

where $m < 0$ is squarefree.

The elliptic curve is said to be ordinary if $\gcd(q+1-n, q) = 1$. It is easily verified that this holds if and only if $\gcd(a, b) = 1$. The same theory which yields the result on the Frobenius endomorphism also ensures that in the case of an ordinary elliptic curve, every endomorphism of the curve fulfills a quadratic equation whose square-free part of the discriminant is the same m , so it can be represented as $a' + b'\delta$ for the same δ for suitable a' and b' . The smallest positive b' which occurs in this way is called the conductor g of the endomorphism ring.

The construction ensures that g divides b ; otherwise, a linear combination of τ and the endomorphism leading to g would contradict the minimality of g .

We are now able to state Wittmann's result.

Lemma 2 (Wittmann [5]). *Let E and E' be ordinary elliptic curves over \mathbb{F}_q with equal number of points with conductors of the endomorphism rings g and g' , respectively. Write the k th power of the complex number τ as $\tau^k = a_k + b_k\delta$ for suitable $a_k, b_k \in \mathbb{Z}$.*

Then the point groups of E and E' over \mathbb{F}_{q^k} are isomorphic if and only if

$$\gcd\left(a_k - 1, \frac{b_k}{g}\right) = \gcd\left(a_k - 1, \frac{b_k}{g'}\right). \quad (2)$$

Note that g and g' divide b_k for the same reason that g divides b .

We emphasise that Wittmann's result reduces the question to a gcd problem in terms of the known quantities g and g' involving the integers a_k and b_k arising from taking powers of $\tau = a + b\delta$. In particular, the problem is completely solved for *given* k because we can simply compute a_k and b_k and then compare the gcds. For *general* k , however, we need to invest more work. This work will no longer depend on the theory of

elliptic curves; instead, we will use olympiad methods including the Lifting the Exponent Lemma.

6 Sketch of the Solution Using Olympiad Methods

6.1 Rewriting in Terms of Primes

The first step consists in translating (2) in terms of p -adic valuations. It is clear that (2) is equivalent to

$$\forall p \text{ prime: } \min\left\{v_p(a_k - 1), v_p\left(\frac{b_k}{g}\right)\right\} = \min\left\{v_p(a_k - 1), v_p\left(\frac{b_k}{g'}\right)\right\}.$$

This trivially holds for those primes p for which $v_p(g) = v_p(g')$. We therefore restrict our attention to the set of primes

$$\mathcal{P} := \{p \text{ prime} \mid v_p(g) \neq v_p(g')\}. \quad (3)$$

So Wittmann's condition (2) is equivalent to

$$\forall p \in \mathcal{P}: \min\left\{v_p(a_k - 1), v_p\left(\frac{b_k}{g}\right)\right\} = \min\left\{v_p(a_k - 1), v_p\left(\frac{b_k}{g'}\right)\right\}.$$

As the second elements on both sides are now guaranteed to be different, the minima coincide if and only if they are equal to the first element. Thus (2) is equivalent to

$$\forall p \in \mathcal{P}: v_p(a_k - 1) \leq \min\left\{v_p\left(\frac{b_k}{g}\right), v_p\left(\frac{b_k}{g'}\right)\right\}.$$

We rewrite the valuations of quotients as differences of valuations and see that the condition is equivalent to

$$\forall p \in \mathcal{P}: v_p(a_k - 1) \leq v_p(b_k) - \max\{v_p(g), v_p(g')\}.$$

We summarise our findings in the following lemma.

Lemma 3. *With the notations of Lemma 2, the point groups of E and E' over \mathbb{F}_{q^k} are isomorphic if and only if*

$$\forall p \in \mathcal{P}: v_p(a_k - 1) \leq v_p(b_k) - s_p$$

where \mathcal{P} is defined in (3) and

$$s_p := \max\{v_p(g), v_p(g')\}.$$

6.2 Relation to a^k and b^k

Fix $p \in \mathcal{P}$. For simplicity, assume that $p \neq 2$. The goal of this section is to replace the quantities $v_p(a_k - 1)$ and $v_p(b_k)$ occurring in Lemma 3 by $v_p(a^k - 1)$ and $v_p(b^k)$. We first recall that by definition, we have

$$(a + b\delta)^k = a^k + b^k\delta.$$

We write $b = p^t c$ and $k = p^\ell m$ for suitable integers t, c, ℓ and m with $p \nmid cm$ and $\ell \geq 0$. Note that the fact that g and g' divide b and $v_p(g) \neq v_p(g')$ implies that $t \geq 1$. The fact that we are considering ordinary elliptic curves then implies that p does not divide a .

The binomial theorem implies that

$$\begin{aligned} a_k + b^k\delta &= (a + b\delta)^k = (a + p^t c\delta)^{p^\ell m} \\ &= a^k + p^{\ell+t} m c a^{k-1} \delta + \sum_{r=2}^k \binom{p^\ell m}{r} a^{k-r} p^{tr} c^r \delta^r. \end{aligned}$$

Careful counting of occurrences of factors p in the binomial coefficients $\binom{p^\ell m}{r}$ —see the original study [2] for the details, in particular some annoying boundary cases—shows that all coefficients of the last sum are divisible by $p^{\ell+t+1}$. We conclude that

$$\begin{aligned} a_k &\equiv a^k \pmod{p^{\ell+t+1}}, \\ b_k &\equiv p^{\ell+t} m c a^{k-1} \pmod{p^{\ell+t+1}}. \end{aligned}$$

As we know that $p \nmid mca^{k-1}$, this implies that

$$v_p(b_k) = \ell + t \text{ and } v_p(a_k - a^k) \geq \ell + t + 1. \quad (4)$$

Lemma 4. *Let $p \in \mathcal{P}$ be an odd prime. Then the condition*

$$v_p(a_k - 1) \leq v_p(b_k) - s_p \quad (5)$$

of Lemma 3 holds if and only if

$$v_p(a^k - 1) \leq v_p(b) + v_p(k) - s_p. \quad (6)$$

Note that the right side of (6) is non-negative because $g \mid b$ and $g' \mid b$ imply that $s_p \leq v_p(b)$.

Proof. We first consider the case that $v_p(a^k - 1) \geq \ell + t + 1$. Writing

$$a_k - 1 = (a_k - a^k) + (a^k - 1)$$

and using (4) then shows that both summands on the right side are divisible by $p^{\ell+t+1}$ which immediately implies that the left side is divisible by the same power of p . In other words,

$$v_p(a_k - 1) \geq \ell + t + 1 = v_p(b) + v_p(k) + 1 > v_p(b_k) \geq v_p(b_k) - s_p,$$

where (4) has been used in the second inequality. We conclude that neither (5) nor (6) holds in this case.

We now turn to the case that $v_p(a^k - 1) \leq \ell + t$. We again consider the decomposition

$$a_k - 1 = (a_k - a^k) + (a^k - 1).$$

The first summand on the right side is divisible by $p^{\ell+t+1}$ by (4), but the second is not. This implies that $v_p(a_k - 1) = v_p(a^k - 1)$ holds in this case. Combining this with (4) yields the assertion. \square

6.3 Using the Lifting the Exponent Lemma

In this section, we use the Lifting the Exponent Lemma to express the quantity $v_p(a^k - 1)$ in (6) to finally decide our question. We still assume that $p \in \mathcal{P}$ is odd.

Denote the order of a modulo p by e , i.e., e is the minimal positive exponent such that $a^e \equiv 1 \pmod{p}$.

If $e \nmid k$, then $a^k \not\equiv 1 \pmod{p}$ by standard properties of order and we have $v_p(a^k - 1) = 0$. Thus (6) is fulfilled in this case.

Otherwise, we can use the Lifting the Exponent Lemma and see that

$$v_p(a^k - 1) = v_p((a^e)^{k/e} - 1) = v_p(a^e - 1) + v_p\left(\frac{k}{e}\right) = v_p(a^e - 1) + v_p(k) - v_p(e).$$

Thus (6) is equivalent to

$$v_p(a^e - 1) - v_p(e) \leq v_p(b) - s_p.$$

Note that the order e of a modulo p divides $\varphi(p) = p - 1$ by Fermat's theorem; thus e must be coprime to p and thus $v_p(e) = 0$.

We conclude that for odd p , the condition (6) does *not* hold if and only if

$$e \mid k \text{ and } v_p(a^e - 1) > v_p(b) - s_p.$$

We summarise our findings (now also incorporating $p = 2$ for completeness, see [2]).

Theorem ([2]). *Let E and E' be ordinary elliptic curves over \mathbb{F}_q with equal number of points with conductors of the endomorphism rings g and g' , respectively, $\tau = a + b\delta$ for suitable $a, b \in \mathbb{Z}$ and $\mathcal{P} = \{p \text{ prime} \mid v_p(g) \neq v_p(g')\}$. Let $k \geq 1$ be an integer. If $2 \in \mathcal{P}$ and $v_2(b) = 1$, assume that k is odd.*

Then the point groups of E and E' over \mathbb{F}_{q^k} are not isomorphic if and only if

$$\exists p \in \mathcal{P} \setminus \{2\}: e := \text{ord}_p(a) \mid k \text{ and } v_p(a^e - 1) > v_p(b) - s_p$$

or

$$2 \in \mathcal{P} \text{ and } e := \text{ord}_4(a) \mid k \text{ and } v_2(a^e - 1) - v_2(e) > v_2(b) - s_2$$

or

$$2 \in \mathcal{P} \text{ and } v_2(k) = 0 \text{ and } s_2 = v_2(b).$$

The case of even k has been excluded from the statement of the theorem for ease of presentation; the case can however be decided, see [2].

References

- [1] Santiago Cuellar and Jose Alejandro Samper, *A nice and tricky lemma (lifting the exponent)*, *Mathematical Reflections* **3** (2007).
- [2] Clemens Heuberger and Michela Mazzoli, *Elliptic curves with isomorphic groups of points over finite field extensions*, *Journal of Number Theory* **181** (2017), 89-98.
- [3] Anthony W. Knapp, *Elliptic curves*, *Mathematical Notes*, vol. 40, Princeton University Press, Princeton, NJ, 1992.
- [4] Hossein Parvardi, *Lifting the exponent lemma (lte)*, 2011, <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.221.5543>.
- [5] Christian Wittmann, *Group structure of elliptic curves over finite fields*, *Journal of Number Theory* **88** (2017), no. 2, 335-344.

Using Inversion in Theorems from Classical Geometry and for Solving Problems¹

Kiril Bankov



Kiril Bankov prepares future mathematics teachers as a professor of mathematics education at the University of Sofia and the Bulgarian Academy of Sciences in Bulgaria. He graduated and received his PhD in mathematics at the same university. Prof. Bankov has been involved in mathematics competitions in Bulgaria for more than 20 years as an author of contest problems and as a member of juries. He was the Secretary of

World Federation of National Mathematics Competitions (WFNMC) from 2008 till 2012. In 2012 Kiril Bankov was elected as the Senior Vice President of WFNMC and in July 2018 he became the President.

1 Introduction

In this article, by the term *inversion* we mean a specific geometric transformation that is defined below. It is a powerful tool for solving problems, especially those that involve many circles. Using inversion, some of the circles may become lines. Roughly speaking, the inversion may transform problems for circles into problems for lines.

Definition. Let O be a point in the plane and r be a positive number. An *inversion* with center O and coefficient r is a transformation of the plane (except for point O) that transforms every point $M \neq O$ onto the point $M' \in \overrightarrow{OM}$ such that $OM \cdot OM' = r^2$ (Fig. 1). The circle ω with center O and radius r is called a *circle of inversion*. Points M and M' are called *inverse to each other*.

¹ This is a version of a talk for the section “Building Bridges between Problems of Mathematical Research and Competitions” of the 8-th Congress of WFNMC, Graz, July 2018.

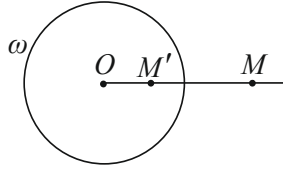


Fig. 1: Definition of inversion

The properties of inversion in a circle are studied in some geometry books, for example Bankov, Vitanov, 2003; Johnson, 1960, etc. The main properties of inversion are given below.

- (i). Inversion is a one-to-one correspondence between the plane without the center of the inversion and itself.
- (ii). If a point lies on the circle of inversion, it is inverse to itself.
- (iii). If a point is outside the circle of inversion, its inverse point is inside the circle of inversion, and vice versa, if a point is inside the circle of inversion, its inverse point is outside the circle of inversion.
- (iv). If a point M is outside the circle of inversion, its inverse point is the midpoint of the chord formed by the tangent points of the tangent lines from M to the circle of inversion (Fig. 2).

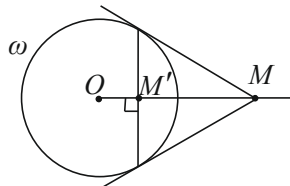


Fig. 2: Image of a point

(v). Let the points M, N be different from O and points O, M, N be non-collinear. If the inverse points of M and N are M' and N' respectively, then triangles OMN and $ON'M'$ are similar (Fig. 3) in such a way that $\angle OMN = \angle ON'M'$ and $\angle ONM = \angle OM'N'$.

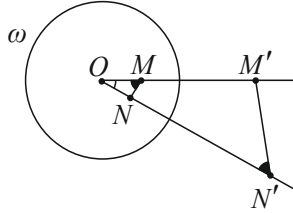


Fig. 3: Similar triangles

The so called inversion distance formula follows from property (v), namely

$$M'N' = \frac{r^2}{OM \cdot ON} \cdot MN$$

or equivalently

$$MN = \frac{r^2}{OM' \cdot ON'} \cdot M'N'.$$

(vi). A line passing through the center of inversion is transformed into itself.

(vii). A circle not passing through the center of inversion is transformed into a circle not passing through the center of inversion. The circle and its image are homothetic with center at the center of inversion.

(viii). A line not passing through the center of inversion is transformed into a circle passing through the center of inversion, and vice versa, a

circle passing through the center of inversion is transformed into a line not passing through the center of inversion.

It is easy to see that if k is a circle passing through the center of inversion and l is its inverse image (see property (viii) above), then the interior points of k are transformed to the one side of l , and the exterior points of k to the other side of l .

(ix). For any two circles without common point there is an inversion that transforms these circles into two concentric circles.

2 Lines and Circles

Lines and circles are different figures in Euclidean geometry, because they have different geometrical properties. Sometimes, because of property (viii) above, lines and circles are considered alike. Examples are presented below.

Here is a problem from the Federal Mathematics Competition in Germany, 1980.

Problem 1 Let M be a set of $2n + 3$ (n is a positive integer) points in the plane such that no three of them lie on a straight line and no four of them lie on a circle. Prove that there is a circle passing through three of the points of M that contains exactly n of the other points in its interior (and the other n are outside the circle).

Solution Let A and B be points of M , such that all other $2n + 1$ points of M lie on one and the same semi-plane with a boundary line AB . Since no four of the points of M lie on a circle, all angles $\angle AXB$, where $X \in M \setminus \{A, B\}$, are different. Arrange the points of $M \setminus \{A, B\}$ in a row

$P_1, P_2, P_3, \dots, P_{2n+1}$ in such a way that $\angle AP_1B < \angle AP_2B < \angle AP_3B < \dots < \angle AP_{2n+1}B$. The circle passing through the points A, B, P_{n+1} has the required property, because it contains the points $P_{n+2}, P_{n+3}, \dots, P_{2n+1}$ in its interior, but the points P_1, P_2, \dots, P_n are outside the circle.

The next problem looks similar but considers a line instead of a circle.

Problem 2 Let M be a set of $2n + 2$ (n is a positive integer) points on the plane such that no three of them lie on a straight line. Prove that there is a line passing through two of the points of M , such that exactly n of the other points lie on one side of the line (and the other n are on the other side of the line).

Solution Let p be a line passing through a point A of M , such that all other $2n + 1$ points of M are in one and the same semi-plane with boundary p . Start rotating p about A counterclockwise. Since no three of the points of M lie on a line, the rotating line p passes consecutively through the points $P_1, P_2, P_3, \dots, P_{2n+1}$ of $M \setminus \{A\}$. The line passing through the points A and P_{n+1} has the required property, because the points $P_{n+2}, P_{n+3}, \dots, P_{2n+1}$ are on one side of this line, but the points P_1, P_2, \dots, P_n are on the other side.

These two problems are equivalent. More interesting is to show that the statement of Problem 1 follows from the statement of Problem 2. Certainly, let M be a set of $2n + 3$ points on the plane such that no three of them lie on a straight line and no four of them lie on a circle. Choose a point O of M and consider inversion with center O and an arbitrary radius r . Denote by N the set of the inverse images of the remaining $2n + 2$ points of M . Since no three of them lie on a line,

according to the statement of Problem 2 there is a line p passing through two of the points of N , such that exactly n of the other points lie on one side of the line (and the other n are on the other side of the line). The reverse inverse image of p is a circle c that has the required property.

The same method is used to transform Miquel's theorem to the so-called Miquel's Six Circle Theorem (Bankov and Vitanov, 2003). These two theorems, cited below, are among a set of wonderful classical theorems in plane geometry. There are several theorems named after Auguste Miquel, a French mathematician from the 19th century. Only one of them can be found in Miquel's publications (Miquel, 1838), namely:

Theorem 1 (Miquel). Let $A_1A_2A_3$ be a triangle, with points P_1 , P_2 and P_3 on the lines A_2A_3 , A_1A_3 , and A_1A_2 respectively (Fig. 4). Then the three circumcircles of triangles $A_1P_2P_3$, $P_1A_2P_3$, and $P_1P_2A_3$ intersect in a single point P (called the Miquel point).

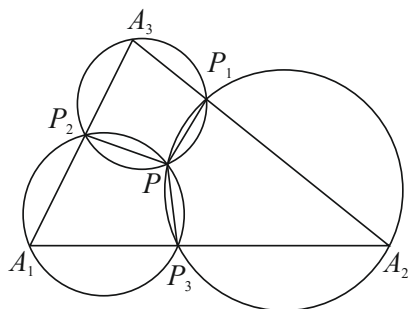


Fig. 4: Miquel's theorem

Proof. Let P be the point of intersection of the circumcircles of triangles $A_1P_2P_3$ and $P_1P_2A_3$ that is different from P_2 . Then $\angle PP_2A_1 = 180^\circ - \angle PP_3A_1$ or $\angle PP_2A_1 = \angle PP_3A_1$ (depending on the positions of the points A_1, P, P_2 , and P_3 on the circle). Both equations show that the angle between the lines A_1A_3 and PP_2 and the lines A_1A_2 and PP_3 are equal, i.e. $\angle(A_1A_3, PP_2) = \angle(A_1A_2, PP_3)$. In the same way, using the other circle, we obtain that $\angle(A_1A_3, PP_2) = \angle(A_2A_3, PP_1)$. Therefore $\angle(A_2A_3, PP_1) = \angle(A_1A_2, PP_3)$. It follows from this that either $\angle PP_1A_2 = 180^\circ - \angle PP_3A_2$ or $\angle PP_1A_2 = \angle PP_3A_2$. Any of these equations show that P lies on the circumcircle of triangle $P_1A_2P_3$.

Theorem 2 (Miquel's six circle theorem) Four points, A, B, C , and D are given on circle o . Four other circles k, l, m , and n pass through each adjacent pair of these points. Then the alternate intersections of these four circles at E, F, G and H lie on a common circle (or on a common line) (Fig. 5).

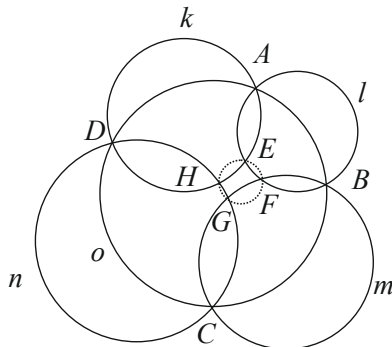


Fig. 5: Miquel's six circle theorem

These two theorems are equivalent. Here are arguments to show that Theorem 2 follows from Theorem 1. Consider the inversion with center A and an arbitrary coefficient r . The inverse images of the figures are denoted with the same letter with subindex 1. From property (viii) of inversion it follows that k_1 (the image of k) is a line containing the points D_1, H_1 , and E_1 (Fig. 6); l_1 is a line containing the points B_1, F_1 and E_1 ; o_1 is a line containing the points D_1, C_1 , and B_1 . Also m_1 is a circle containing the points B_1, F_1, G_1 , and C_1 ; and n_1 is a circle containing the points D_1, H_1, G_1 , and C_1 .

According to Theorem 1, points E_1, F_1, G_1 , and H_1 lie on a common circle. Therefore, points E, F, G and H also lie on a common circle (or on a common line).

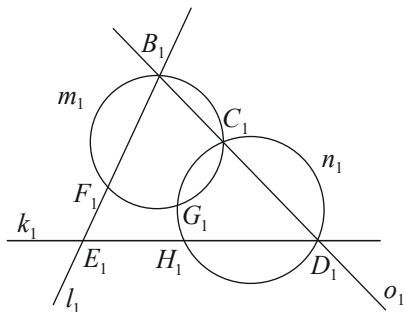


Fig. 6: Inversion of Fig. 5

The above reasoning shows how a suitable inversion may transform a problem concerning “many” circles to a problem that contains “fewer circles but more lines”. Assuming that problems for lines are easier to solve, the inverse transformation gives a solution to the original problem.

3 Two Famous Results from Plane Geometry

Miquel's theorems present classical results from plane geometry. Here are two other examples of beautiful geometrical theorems connected to the names of well-known mathematicians. The reason to bring attention to them is that inversion may help to prove them.

The first example is connected with the figure known as the *arbelos*. It consists of three collinear points A , B , and C , together with three semicircles with diameters AB , AC , and BC , as shown in Figure 7. It was named after a shoemaker's knife because its shape resembles it. Many interesting properties of the arbelos have been studied by mathematicians (Bankoff, 1974; Cadwell, 1966; Hood, 1961).

Here attention is brought to the statement that is believed to have been proven by Pappus.

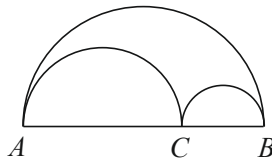


Fig. 7: Arbelos

Theorem (Pappus) Consider a chain of circles $c_1, c_2, \dots, c_n, \dots$ inscribed in an arbelos as shown in Figure 8. (Circle c_1 is tangent to the three semicircles of the arbelos, for $n > 1$, c_n is tangent to two of the semicircles of the arbelos and circle c_{n-1} .) For any $n = 1, 2, \dots$ denote by r_n the radius of c_n and by y_n the distance from the center of c_n to the baseline AB . Then $y_n = 2nr_n$, for $n = 1, 2, \dots, n > 1$

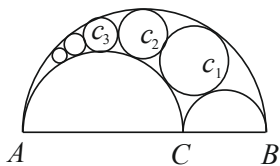


Fig. 8: Pappus' theorem

Nowadays the proof of the theorem is relatively easy if we consider the inversion with center A that transforms B in C (i.e. the radius of the inversion is $r = \sqrt{AB \cdot AC}$). The inversion transforms the semicircle with diameter AB into a ray with origin C that is perpendicular to AB . This inversion transforms the semicircle with diameter AC into a ray with origin B that is perpendicular to AB . It also transforms the semicircle with diameter BC into itself. Then the chain $c_1, c_2, \dots, c_n, \dots$ is transformed into a chain $c'_1, c'_2, \dots, c'_n, \dots$ of sequentially tangent equal circles that are tangent to the two rays as shown on Figure 9. If r'_n is the radius of c'_n and y'_n is the distance from the center of c'_n to the baseline AB , it is clear that $y'_n = 2nr'_n$. We can now use property (vii) of inversion that states that the circle and its inversion image are homothetic with center in the center of inversion to obtain the result.

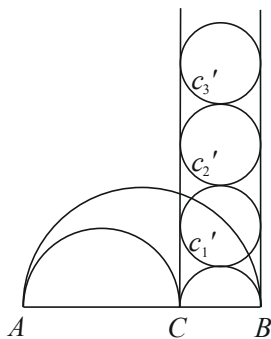


Fig. 9: Proof of Pappus' theorem

Pappus of Alexandria was one of the last great Greek mathematicians of antiquity. He lived in the fourth century. This means that Pappus could not have made use of this method, since inversion was discovered 15 centuries after he lived. In 1981 Bankoff (Bankoff, 1981) wrote an interesting essay on how Pappus could have proven this theorem.

The second example is connected to the Swiss mathematician of the 19th century Jakob Steiner. He considered two circles k_1 and k_2 , such that k_2 is in the interior of k_1 . In the area between the two circles a chain of touching circles c_1, c_2, \dots, c_n is such that each circle is tangent to k_1, k_2 , and both of its neighbors (Fig. 10). In some cases it is possible to find n such that c_n is tangent to k_1, k_2, c_{n-1} , and c_1 ; in some cases this is not possible. This depends on the radii of k_1, k_2 and their mutual position.

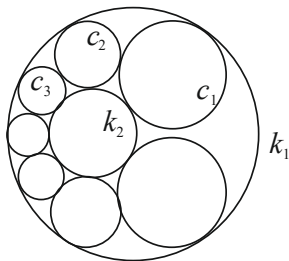


Fig. 10: Steiner's theorem

Theorem (Steiner) In the above configuration, let k_1, k_2 be circles such that there is a chain of circles c_1, c_2, \dots, c_n such that c_n is tangent to k_1, k_2, c_{n-1} , and c_1 . Then these chains are infinitely many. This means that for any circle t_1 that is tangent to k_1, k_2 , there is a chain of touching circles t_1, t_2, \dots, t_n such that each circle is tangent to k_1, k_2 , and both of its neighbors and t_n is tangent to k_1, k_2, t_{n-1} , and t_1 .

Steiner was more fortunate than Pappus because in his time inversion was well known. Apply property (ix) to find the inversion that transforms k_1, k_2 into two concentric circles k_1', k_2' . For k_1', k_2' the theorem is obvious. Then we use the inverse of this inversion.

The question that remains is under which conditions does there exist a chain of touching circles c_1, c_2, \dots, c_n such that c_n is tangent to k_1, k_2, c_{n-1} , and c_1 . We do not discuss this here. The answer can be found in Prassolov, 2006.

4 Inversion in Competition Problems

There are many examples of competition problems that can be solved using inversion (see, for example, Chapter 8 of Evan, 2016). This fact shows that the statement “geometry becomes less popular in school mathematics and in competitions” is only a myth.

The beauty of competition problems is that they do not directly refer to inversion in the statement of the problem. There is not much creativity in a situation like this: “A geometric construction and its image under certain inversion is given. Prove this and this.” In the problems that I refer to the inversion is not given. One should discover the inversion that may help and apply it. This needs a lot of creativity. Such problems are perfect examples of the beauty of geometry.

I will cite only two problems to give an opportunity to the reader to experience this beauty.

Problem 3 Four circles $k_1, k_2, k_3,$ and k_4 are given in such a way that k_1 is tangent externally to k_2 and k_4 in points A and D respectively, and k_3 is tangent externally to k_2 and k_4 in points B and C respectively. Prove that points $A, B, C,$ and D lie on a common circle.

Hint Consider inversion with center D and an arbitrary coefficient. The problem is transformed into the following easier problem: Let p and q be parallel lines, and A and C be points on p and q respectively. Let k_1 and k_2 be circles externally tangent in point B such that k_1 is tangent to p in A and k_2 is tangent to q in C . Prove that $A, B,$ and C lie on a common line.

Problem 4 (Russian Mathematical Olympiad, 1995) A semicircle with diameter AB and center O is given. A line intersects the semicircle at C and D , and line AB at M ($MB < MA, MD < MC$). Let K be the second point of intersection of the circumcircles of triangles AOC and DOB . Prove that $\angle MKO = 90^\circ$.

Hint Consider the inversion with center O and radius $r = OA = OB$. By property (ii) of inversion each of the points $A, B, C,$ and D is inverse to itself. The image of the circle through $A, O,$ and C is the line AC and the image of the circle through $D, O,$ and B is the line DB . Hence, the inversion point of K is the intersection K_1 of lines AC and DB . Also, the inverse point of M is the intersection M_1 of line AB with the circumcircle of triangle $\triangle OCD$. Then the image of line MK is the circumcircle of triangle $\triangle OM_1K_1$. According to property (v) of inversion $\angle MKO = 90^\circ$ if and only if $\angle K_1M_1O = 90^\circ$. To prove the last equation show that the circumcircle of triangle $\triangle OCD$ is the nine-point circle of $\triangle ABK_1$. (The nine-point circle for a triangle is the circle that contains the feet of the altitudes of the triangle and the midpoints of its sides.)

References

- [1] Bankoff, L. (1974). Are the Twin Circles of Archimedes really Twins? *Mathematics Magazine*, Mathematical Association of America, Vol. 47, No 4, pp 214-218.
- [2] Bankoff, L. (1981). How did Pappus do it? in *The Mathematical Gardner*, edited by David Klarner, Wadsworth International.
- [3] Bankov, K., and Vitanov, T. (2003). Geometry. Anubis (in Bulgarian).
- [4] Cadwell, J. (1966). Topics in Recreational Mathematics. Cambridge University Press. pp. 44-45.
- [5] Evan, C. (2016). Euclidean Geometry in Mathematical Olympiads. The Mathematical Association of America.
- [6] Hood, R. (1961). A Chain of Circles. *The Mathematics Teacher*, Vol. 54, No. 3, NCTM. pp. 134-137.
- [7] Johnson, R. (1960). Advanced Euclidean Geometry. Dover Publications, New York.
- [8] Miquel, A. (1838). Théorèmes de Géométrie, *Journal de Mathématiques Pures et Appliquées* 1: 485–487.
- [9] Prassolov, V. (2006). Problems on 2D Geometry. MCNMO, Moskow, chapter 28, problem 28.41, pp. 523-524. (in Russian).

Some Polynomial Morsels from the Iranian Mathematical Olympiads

Navid Safaei (navid_safaei@gsme.sharif.edu)

Sharif University of Technology, Tehran, Iran



Navid is a senior researcher at the Sharif University of Technology, Tehran, Iran. His main research interest is evolutionary theory for the socio-economic domain. He has been the head of the Mathematical Olympiad Department at Salam High schools complex since 2009. He has participated as instructor and problem proposer for the Iranian TST, since 2014. He has been involved in training curricula for mathematics competitions since 2005. He has written more than 20 books (in Persian) for high school mathematics including Calculus, Mathematics 9, 10, 11, published by Olgoo publication, Tehran, Iran.

Navid is a local organizer in Iran for European Mathematical Cup (EMC) and Silk Road Mathematical Competition (SRMC). He was the Iranian team leader for the Romanian Masters of Mathematics (RMM) competition. As an instructor, he has been invited to many training camps around the world such as Azerbaijan, Bulgaria, Croatia, Singapore. He also published many articles concerning methods and techniques for solving mathematical competitions problems in Mathematical Reflections (MR), Cibiti Matematiki, i. e., USM (in Ukrainian), Matematika (in Bulgarian). He also proposed some problems for the American Mathematical Monthly (AMM) journal. Navid is collaborating with XYZ-Press publishing house and his first book about polynomials was published in February 2019.

Abstract. In this article we explore polynomial problems from recent Iranian Mathematical Olympiads and other elements from the Iranian experience in teaching polynomials for mathematical olympiad curricula.

1. Introduction

Starting in 2015, the Algebra exams of the third round and TST of the Iranian Mathematical Olympiad have contained some interesting problems about polynomials. Most of these problems are original as well as challenging. This article outlines the conceptual framework concerning ideas about polynomials that touch on some strong points in tandem with some points concerning my teaching experiences. Having said this, the kernel of ideas for this article is to introduce the readers to the Iranian approach to mathematical competitions with exclusive regard to algebra and polynomials.

2. Finding polynomials and examining coefficients

The most generic approach to teaching polynomials is to start with coefficients and identities. Hence, a good entry point into our topic is to start with a polynomial equation. However, although the central idea of this problem seems too easy, only four students solved the problem completely. It was partly because this problem was the fifth problem of an exam with six problems that took six hours! The author of this problem was Mojtaba Zare who received a gold medal at IMO 2015 and immediately started to propose problems and teach algebra for the Mathematical Olympiad curricula. Students can find very many interesting problems concerning finding polynomials and examining the coefficients in Andreescu, et al (2019).

Problem 1. (3rd round Iranian Mathematical Olympiad, 2015, Algebra exam, Problem 5) Find all polynomials $P(x)$ with real coefficients satisfying $P(5x)^2 - 3 = P(5x^2 + 1)$, whenever:

- i. $P(0) \neq 0$,
- ii. $P(0) = 0$.

Solution. Suppose that $P(x)$ is not constant. Let $\deg P(x) = d$, $P(x) = a_0 + a_1x + \dots + a_dx^d$. Comparing the coefficients of both sides we find that $a_d = 5^{-d}$. Then, we can prove by induction that all the coefficients of $P(x)$ are rational. Now, considering the equation $5x^2 + 1 = 5x$, we have that $r = \frac{5+\sqrt{5}}{10}$ is one of the roots. Since $P(x)$ has rational coefficients, it is easy to deduce $P(5r) = P\left(\frac{5+\sqrt{5}}{2}\right) = c + d\sqrt{5}$, for some rational numbers c, d . Further, putting $x = r$ in the original equation, we can find that $P(5r)^2 - 3 = P(5r^2 + 1)$. That is $P(5r)^2 - P(5r) - 3 = 0$. Hence, $P(5r) = \frac{1+\sqrt{13}}{2}$. Impossible!

Remark. As you have seen, this solution doesn't need the condition on $P(0)$. During the meeting of algebra team, the proposer outlined the following proof.

It is easy to deduce $P(5x)^2 = P(-5x)^2$. Thus, $P(x)$ is either odd or even. Assume the latter, then $P(x) = Q(x^2)$, for some polynomial $Q(x)$. Hence, rewrite the original equation as

$$P(x)^2 - 3 = P\left(\frac{x^2}{5} + 1\right).$$

Since $P(x)$ is a polynomial in x^2 , we can assume that $P(x) = R\left(\frac{x^2}{5} + 1\right)$, for some polynomial $R(x)$. Hence,

$$R\left(\frac{x^2}{5} + 1\right)^2 = R\left(\frac{\left(\frac{x^2}{5} + 1\right)^2}{5} + 1\right).$$

Putting $t = \frac{x^2}{5} + 1$, then $R(t)^2 - 3 = R\left(\frac{t^2}{5} + 1\right)$ and $\deg R(x) = \frac{1}{2} \deg P(x)$. Hence, continuing this way, we shall face an infinite descent unless $P(0) = 0$. Therefore, the first case would be reduced to the second case.

Assuming¹ now the second case, define the following sequence $a_0 = 0, a_{n+1} = 1 + \frac{a_n^2}{5}$. We can prove by induction that $a_k \in [1, 2)$, for each positive integer $k \geq 1$. Now, define the sequence $b_n = P(a_n)$. Putting $x = a_n$ in the original equation, we can find that $b_{n+1} = b_n^2 - 3$. It is clear that for $n \geq 1$, the sequence assumes positive integer values and $b_{n+1} > b_n$ for each $n \geq 1$. Thus $\lim_{n \rightarrow +\infty} b_n = +\infty$. On the other hand, since $P(x)$ is a polynomial, $P([1, 2))$ is bounded. That is, b_n should be bounded, which yields a contradiction.

The next problem is selected from our 2017 TST. I was the author of this problem. I thought that it was a very easy problem. But, from our 17 gold medalists, only 6 completely solved it! Most of the students had some computations concerning the coefficients but had not taken this idea further.

¹ This part of proof is the refined version of a proof we find in an exam paper. Unfortunately, this student just solved the second part, assuming $P(0) = 0$. Thanks to Mojtaba Zare for sending the ideas from the exam paper.

Problem 2. (2017 Iranian TST, Test 3, Problem 5) Let $\{c_i\}_{i=0}^{\infty}$ be a sequence of non-negative rational numbers such that $c_{2017} > 0$. Define the sequence of polynomials such that:

$$P_{-1}(x) = 0, P_1(x) = 1, P_{n+1}(x) = xP_n(x) + c_n P_{n-1}(x).$$

Prove that for all $n > 2017$ there does not exist an integer n such that $P_{2n}(x) = P_n(x^2 + c)$ for some rational number c .

Solution. It could immediately be deduced that:

$$P_d(x) = x^d + (c_1 + c_2 + \dots + c_{d-1})x^{d-1} \\ + (c_3c_1 + c_4c_1 + c_4c_2 + \dots + c_{d-1}c_{d-2})x^{d-2} + \dots.$$

The coefficient of x^{d-2} could be written as $\sum_{k=3}^{d-1} c_k \sum_{l=1}^{k-2} c_l$. This is also equal to

$$\frac{1}{2}((c_1 + c_2 + \dots + c_{d-1})^2 - \sum_{k=1}^{d-1} c_k^2) - \sum_{k=1}^{d-2} c_k c_{k+1}.$$

Now, assume by contradiction that there is such an n . By comparing the coefficients of x^{2n-1}, x^{2n-2} we find that:

$$c = \frac{1}{n} \sum_{k=1}^{2n-1} c_k,$$

$$\sum_{k=3}^{2n-1} c_k \sum_{l=1}^{k-2} c_l = \frac{n(n-1)}{2} c^2 + \sum_{k=1}^{n-1} c_k.$$

Substituting the first equality into the second one, we find that

$$\frac{1}{n} (\sum_{k=1}^{2n-1} c_k)^2 = \sum_{k=1}^{2n-1} c_k^2 + 2 \sum_{k=1}^{2n-2} c_k c_{k+1} + 2 \sum_{k=1}^{n-1} c_k (*).$$

Now we prove that the above equality is wrong!

Note that, by the Cauchy-Schwartz inequality, we have:

$$\frac{1}{n} \left(\sum_{k=1}^{2n-1} c_k \right)^2 \leq c_1^2 + \sum_{k=1}^{n-1} (c_{2k+1} + c_{2k})^2.$$

And

$$\frac{1}{n} \left(\sum_{k=1}^{2n-1} c_k \right)^2 \leq c_{2n-1}^2 + \sum_{k=1}^{n-1} (c_{2k-1} + c_{2k})^2.$$

This yields:

$$\frac{2}{n} \left(\sum_{k=1}^{2n-1} c_k \right)^2 \leq 2 \sum_{k=1}^{2n-1} c_k^2 + 2 \sum_{k=1}^{2n-2} c_k c_{k+1}.$$

Applying the resulting inequality to (*) we find that $\sum_{k=1}^{2n-2} c_k c_{k+1} + 2 \sum_{k=1}^{n-1} c_k \leq 0$. Since $c_k \geq 0$ and $c_{2017} > 0$ this is impossible! We are done!

3. On roots of polynomials

The second important topic in teaching polynomials concerns roots. Though most of the students solved many problems on Vieta's formula and the Intermediate Value Theorem (IVT), they found these two problems very hard. It seems that there were some weaknesses in their arguments or lack of innovative ideas.

The first problem was proposed by me for the final exam of Seemurg Training Camp of Nations (STCN) that was held in January 2019

between 6 countries² around the world. Only 8 out of 124 students solved this problem. The reason was they were not brave enough to deal with the complexity which emerges after writing Vieta's formula for the roots.

Problem 3. (2019 STCN, Final Exam, Problem 4)³ Assume that all the roots of $P(x) = x^d - a_1x^{d-1} + \dots + (-1)^d a_d$ lie in $[0,1]$. Prove that for all $k = 1, 2, \dots, d$ we have

$$a_k - a_{k+1} + \dots + (-1)^{d-k} a_d \geq 0.$$

Solution. Let us consider $P(x) = (x - x_1) \dots (x - x_d)$ where $x_i \in [0,1]$. Note that, by Vieta's formula we have:

$$a_i = a_i(x_1, x_2, \dots, x_d) = \sum_{1 \leq s_1, \dots, s_i \leq d} x_{s_1} \dots x_{s_i}.$$

Now we prove the statement of problem by induction on d . The case $d = 1$ is obvious. Note that:

$$P(1) = 1 - a_1 + a_2 - \dots + (-1)^d a_d \geq 0.$$

Thus:

$$(-1)^k a_k + (-1)^{k+1} a_{k+1} + \dots + (-1)^d a_d = P(1) - 1 + a_1 - a_2 + \dots + (-1)^k a_{k-1}.$$

Therefore, the desired inequality leads to:

$$(-1)^k (P(1) - 1 + a_1 - a_2 + \dots + (-1)^k a_{k-1}) \geq 0.$$

² The participating countries were Azerbaijan, Bangladesh, Iran, Mexico, Mongolia, and Tajikistan.

³ Two months later this problem appeared in the problems section of Kvant(2019/1) journal as problem M2544.

Assume the statement of the problem holds true for all positive integers less than or equal to d . Now we must prove for the polynomial

$$\begin{aligned} P(x) &= (x - x_1) \cdots (x - x_d)(x - x_{d+1}) \\ &= x^{d+1} - b_1 x^d + \cdots + (-1)^{d+1} b_{d+1}, \end{aligned}$$

that: $b_k - b_{k+1} + \cdots + (-1)^{d+1-k} b_{d+1} \geq 0$ for all $k = 1, \dots, d + 1$.

Note that:

$$b_i = b_i(x_1, \dots, x_{d+1}) = a_i(x_1, x_2, \dots, x_d) + x_{d+1} a_{i-1}(x_1, x_2, \dots, x_d).$$

According to the above fact, we must prove:

$$\begin{aligned} &(-1)^k (Q(1) - 1 + b_1 - b_2 + \cdots + (-1)^k b_{k-1}) \\ &= (-1)^k (Q(1) - 1 + a_1 + x_{d+1} - a_2 - x_{d+1} a_1) \\ &+ \cdots + (-1)^k (a_{k-1} + x_{d+1} a_{k-2}) \geq 0. \end{aligned}$$

Since $Q(1) = (1 - x_{d+1})P(1)$ one can rewrite the above inequality as:

$$(-1)^k (1 - x_{d+1})(P(1) - 1 + a_1 - a_2 + \cdots + (-1)^k a_{k-1}) \geq 0,$$

which is true, due to the induction hypothesis.

Although the next problem has a simple statement, it needs insightful knowledge about the IVT and the notion of multiple roots. Most of the contestants did not consider the fact that in the neighborhood of a root r , we face a change in the sign of the polynomial unless the root is double or has an even number of occurrences. That is, $P(x) = (x - r)^{2a} Q(x)$, for some natural number a and some polynomial $Q(x)$ such that $Q(r) \neq 0$.

Problem 4. (3rd round Iranian Mathematical Olympiad, 2019, Algebra exam, Midterm, Problem 3) For each positive integer d , find all open intervals $I \subseteq \mathbb{R}$, of largest length, such that for any choice of $a_0, \dots, a_{2d-1} \in I$ the polynomial $P(x) = x^{2d} + a_{2d-1}x^{2d-1} + \dots + a_0$, has no real root.

Solution. The answer is $I = \left(1, 1 + \frac{1}{d}\right)$. Assume that the desired interval is of the form of (b, c) . For some q, r in (b, c) , put $a_i = q$ for odd i and $a_i = r$ for even i , where $0 \leq i \leq 2d - 1$. Then

$$P(-1) = 1 - dq + dr.$$

Since $P(x)$ has no real root, we must have $P(-1) > 0$. Thus, $q - r < \frac{1}{d}$. We can assume that $c - b \leq \frac{1}{d}$. Therefore, consider the interval as $\left(b, b + \frac{1}{d}\right)$. It is easy to find that $b > 0$, since by choosing $a_0 = b + \varepsilon$, for some sufficiently small $\varepsilon > 0$, we find that $P(0) = a_0 = b + \varepsilon$ should be positive.

Now, assign the following numbers to the coefficients of the polynomial.

$$a_{2d-1} = a_{2d-3} = \dots = a_1 = b + \frac{1}{d} + \varepsilon,$$

$$a_{2d} = a_{2d-2} = \dots = a_0 = b + \varepsilon$$

for some sufficiently small $\varepsilon > 0$.

It is clear that for all positive real x , $P(x) > 0$ Now for all negative real x , putting $x = -t$, where $t > 0$, then

$$P(-t) = t^{2d} - \left(b + \frac{1}{d}\right)t^{2d-1} + bt^{2d-2} - \left(b + \frac{1}{d}\right)t^{2d-3} + \dots - \left(b + \frac{1}{d}\right)t + b + \varepsilon Q(t),$$

for some polynomial $Q(t)$, $\deg Q(t) = 2d - 1$. As ε tends to zero, it remains to find all $b > 0$ such that

$$R(t) = t^{2d} - \left(b + \frac{1}{d}\right)t^{2d-1} + bt^{2d-2} - \left(b + \frac{1}{d}\right)t^{2d-3} + \dots - \left(b + \frac{1}{d}\right)t + b \geq 0.$$

Note that $R(1) = 0$. Therefore, $R'(1)$ should be zero. That is,

$$2d - (2d - 1)\left(b + \frac{1}{d}\right) + (2d - 2)b - \dots - \left(b + \frac{1}{d}\right) = 0.$$

Hence, $d(1 - b) = 0$. That is, $d = 1$.

Now, we claim the interval $I = \left(1, 1 + \frac{1}{d}\right)$ works! It is obvious that $P(x)$ has no positive real roots. Now, we prove that $P(x) > 0$ for all negative real x . Put $x = -t, t > 0$. Then

$$P(-t) > t^{2d} - \left(1 + \frac{1}{d}\right)t^{2d-1} + t^{2d-2} - \left(1 + \frac{1}{d}\right)t^{2d-3} + \dots - \left(1 + \frac{1}{d}\right)t + 1.$$

Thus, it remains to prove that

$$\frac{t^{2d} + t^{2d-2} + \dots + t^2 + 1}{d + 1} \geq \frac{t^{2d-1} + t^{2d-3} + \dots + t^3 + t}{d}.$$

Now, because $t^{2d} + 1 \geq t^{2d-2k+1} + t^{2k-1}, t^{2k} + t^{2k-2} \geq 2t^{2k-1}$, we are done.

No students got complete points for this problem. We had six students who got 6/15 for this problem. They proved that the length of the interval is at most $\frac{1}{d}$ and proved the interval $I = \left(1, 1 + \frac{1}{d}\right)$ satisfies the problem conditions. But, they could not prove that it is the only solution. As the author of this problem, I expected more complete solutions from 80 contestants.

In the following remark, I provide an alternative approach to finding the optimal case. It needs some knowledge about limits along with knowledge about the roots. In effect, this approach seems more complicated for high school students. I provide this approach here to show that despite their complexity, sometimes advanced techniques can nevertheless be reconciled with elementary techniques.

Remark. There is an alternative proof for the segment where we proved $b = 1$. One can find that

$$t^{2d} - b(t^{2d-1} - t^{2d-2} + \dots + t - 1) - \frac{1}{d}(t^{2d-1} + t^{2d-3} + \dots + t) \geq 0.$$

Hence for all $t > 1$, $b \leq \frac{1}{d} \cdot \frac{dt^{2d} - (t^{2d-1} + t^{2d-3} + \dots + t)}{t^{2d-1} - t^{2d-2} + \dots + t - 1}$.

And, for all $t < 1$, $b \geq \frac{1}{d} \cdot \frac{dt^{2d} - (t^{2d-1} + t^{2d-3} + \dots + t)}{t^{2d-1} - t^{2d-2} + \dots + t - 1}$.

Thus,

$$b \leq \frac{1}{d} \cdot \lim_{t \rightarrow 1^+} \frac{dt^{2d} - (t^{2d-1} + t^{2d-3} + \dots + t)}{t^{2d-1} - t^{2d-2} + \dots + t - 1},$$

And

$$b \geq \frac{1}{d} \lim_{t \rightarrow 1^-} \frac{dt^{2d} - (t^{2d-1} + t^{2d-3} + \dots + t)}{t^{2d-1} - t^{2d-2} + \dots + t - 1},$$

since the function $\frac{dt^{2d} - (t^{2d-1} + t^{2d-3} + \dots + t)}{t^{2d-1} - t^{2d-2} + \dots + t - 1}$ has a limit as t approaches

Thus, we find that

$$\begin{aligned} \lim_{t \rightarrow 1^-} \frac{dt^{2d} - (t^{2d-1} + t^{2d-3} + \dots + t)}{t^{2d-1} - t^{2d-2} + \dots + t - 1} \\ = \lim_{t \rightarrow 1^+} \frac{dt^{2d} - (t^{2d-1} + t^{2d-3} + \dots + t)}{t^{2d-1} - t^{2d-2} + \dots + t - 1}. \end{aligned}$$

Hence, $b = \frac{1}{d} \cdot \lim_{t \rightarrow 1} \frac{dt^{2d} - (t^{2d-1} + t^{2d-3} + \dots + t)}{t^{2d-1} - t^{2d-2} + \dots + t - 1}$. Finally, note that

$$\begin{aligned} & \frac{dt^{2d} - (t^{2d-1} + t^{2d-3} + \dots + t)}{t^{2d-1} - t^{2d-2} + \dots + t - 1} \\ &= \frac{(t^{2d} - t^{2d-1}) + (t^{2d} - t^{2d-3}) + \dots + (t^{2d} - t)}{(t-1)(t^{2d-2} + t^{2d-4} + \dots + 1)} \\ &= \frac{(t-1)(t^{2d-1} + t^{2d-3}(t^2 + t + 1) + \dots + t(t^{2d-2} + \dots + 1))}{(t-1)(t^{2d-2} + t^{2d-4} + \dots + 1)}. \end{aligned}$$

Thus

$$\begin{aligned} & \lim_{t \rightarrow 1} \frac{dt^{2d} - (t^{2d-1} + t^{2d-3} + \dots + t)}{t^{2d-1} - t^{2d-2} + \dots + t - 1} \\ &= \lim_{t \rightarrow 1} \frac{t^{2d-1} + t^{2d-3}(t^2 + t + 1) + \dots + t(t^{2d-2} + \dots + 1)}{t^{2d-2} + t^{2d-4} + \dots + 1} \\ &= \frac{d^2}{d} = 1. \end{aligned}$$

That is, $b = \frac{1}{d} \cdot d = 1$.

4. Absolute Value, Triangle Inequality, and Complex Numbers

The third topic that I use when I have a lecture on polynomials, is the triangle inequality. Most of the students know it very well. However, they cannot adapt it in their arguments and proof procedures. Furthermore, proofs that proceed based on the triangle inequality need some special attention to the case(s) of equality as well.

This problem was proposed by the author. Five students from the thirteen gold medalists solved it. The interesting issue was that all of these five students became members of our national team for the IMO 2019. It would seem that solving this problem brings fruition!

Problem 5. (Iranian TST, 2019, Exam 3, Problem 1) Let $1 < t < 2$ be a real number. Prove that for all sufficiently large positive integers d , there is a monic polynomial $P(x)$ of degree d , such that all of its coefficients are either 1 or -1 and:

$$|P(t) - 2019| \leq 1.$$

Solution. First we shall prove the following lemma.

Lemma 1. Let b_n , be a sequence of positive real numbers satisfying $b_n \leq 2b_0 + b_1 + \dots + b_{n-1}$. Then for each real number z , $|z| \leq 2b_0 + b_1 + \dots + b_n$, there exist $a_0, \dots, a_n \in \{1, -1\}$ such that:

$$\left| z - \sum_{i=0}^n a_i b_i \right| \leq b_0.$$

Proof. Write the inequality $|z| \leq 2b_0 + b_1 + \dots + b_{n-1}$ in the form $|z - \text{Sgn}(z)b_n| \leq 2b_0 + b_1 + \dots + b_{n-1}$. Then proceed to the proof

by induction on n . For sake of convenience, we also define $\text{Sgn}(0) = 1$. This completes our proof.

Back to our problem. Let us define $b_i = t^i$. Then it is easy to deduce that

$$\begin{aligned} b_n - b_0 &= t^n - 1 \leq 1 + t + \dots + t^{n-1} \\ &= \frac{t^n - 1}{t - 1} = b_0 + b_1 + \dots + b_{n-1}. \end{aligned}$$

Moreover, choose d such that $t^d \geq 2019$. Then

$$2019 \leq t^d \leq 2 + t + \dots + t^d.$$

Hence, by our lemma, there exist $a_0, \dots, a_d \in \{1, -1\}$ such that

$$\left| \sum_{i=0}^d a_i t^i - 2019 \right| \leq 1.$$

We are done.

In the next problem, we need a tricky identity. During July 2017, the problems selection committee told me that they needed a complex number problem. I proposed this problem. Unfortunately, students were not good enough at polynomials with complex coefficients. We had only three complete scores. I designed the first part of the problem in a way that solving it works as a hint for the second part. That is, the student could realize some facts from the relation between the roots of a polynomial and its reciprocal polynomial (i. e., polynomials $P(x)$, $x^d P\left(\frac{1}{x}\right)$, and $d = \deg P(x)$). Inquisitive readers can find some interesting lines of thought about roots of unity and reciprocal polynomials, etc. in Safaei (2019).

Problem 6. (3rd round Iranian Mathematical Olympiad, 2017, Final Algebra exam, Problem 2) Let $P(z) = a_0 + a_1z + \dots + a_dz^d$ be a polynomial with complex coefficients, we define its “reverse” as:

$$P^*(z) = \overline{a_0}z^d + \overline{a_1}z^{d-1} + \dots + \overline{a_d}.$$

- i. Prove that: $P^*(z) = z^d \overline{P\left(\frac{1}{z}\right)}$.
- ii. Let all roots of the polynomial $q_{d-l}(z)$ of degree $d - l$ lie inside or on the unit circle ($l > 0, l \in \mathbb{Z}$).

Prove that all the roots of the following polynomial lie on the unit circle:

$$Q(z) = z^l q_{d-l}(z) + q_{d-l}^*(z).$$

Solution-i. Assume $q_{d-l}(z) = (z - z_1) \dots (z - z_{d-l})$ and $|z_i| \leq 1$ for all $i = 1, \dots, d - l$. Then we can find that $P^*(z) = z^d \overline{P\left(\frac{1}{z}\right)}$.

Solution-ii. If s is a root of $P(z)$ then, $\frac{1}{s}$ must be a root of $P^*(z)$, which leads to:

$$q_{d-l}^*(z) = (1 - z\overline{z_1}) \dots (1 - z\overline{z_{d-l}}).$$

Assume $Q(r) = 0$ for some complex number r . Then

$$r^l q_{d-l}(r) + q_{d-l}^*(r) = 0.$$

Thus, $r^l q_{d-l}(r) = -q_{d-l}^*(r)$ and then

$$|r^l q_{d-l}(r)| = |q_{d-l}^*(r)|.$$

Hence $|r^l| \cdot |q_{d-l}(r)| = |q_{d-l}^*(r)|$ or

$$|r^l| \cdot |(r - z_1) \dots (r - z_{d-l})| = |(1 - r\overline{z_1}) \dots (1 - r\overline{z_{d-l}})|.$$

If $|z_i| = 1$ for some i then $|r - z_i| = |\bar{z}_i|$. $|r - z_i| = |r\bar{z}_i - 1| = |1 - r\bar{z}_i|$. Thereby without loss of generality, we can assume $|z_i| < 1$ for all i . Now we prove the following lemma.

Lemma 2. The following identity holds for all complex numbers r, z_i ,
 $|r - z_i|^2 - |1 - r\bar{z}_i|^2 = (|r|^2 - 1)(1 - |z_i|^2)$.

Proof.

$$\begin{aligned} |r - z_i|^2 - |1 - r\bar{z}_i|^2 &= (r - z_i)(\bar{r} - \bar{z}_i) - (1 - r\bar{z}_i)(1 - \bar{r}z_i) = \\ &= |r|^2 + |z_i|^2 - 1 - |r|^2 \cdot |z_i|^2 = (|r|^2 - 1)(1 - |z_i|^2). \end{aligned}$$

This completes our proof.

We conclude that whenever $|z_i| < 1$ the following corollary holds.

Corollary. If $|r| > 1$ then $|r - z_i| > |1 - r\bar{z}_i|$, and if $|r| < 1$ then $|r - z_i| < |1 - r\bar{z}_i|$.

Now, if $|r| > 1$ then

$$\begin{aligned} |r^l| \cdot |(r - z_1) \cdots (r - z_{d-l})| &> |r^l| \cdot |(1 - r\bar{z}_1) \cdots (1 - r\bar{z}_{d-l})| \\ &> |(1 - r\bar{z}_1) \cdots (1 - r\bar{z}_{d-l})|, \end{aligned}$$

which leads to a contradiction.

Moreover, if $|r| < 1$ then

$$\begin{aligned} |r^l| \cdot |(r - z_1) \cdots (r - z_{d-l})| &< |r^l| \cdot |(1 - r\bar{z}_1) \cdots (1 - r\bar{z}_{d-l})| \\ &< |(1 - r\bar{z}_1) \cdots (1 - r\bar{z}_{d-l})|, \end{aligned}$$

which again leads to a contradiction. Thus $|r| = 1$, and we are done!

Remark. Sometimes using an identity, taking the norm on both sides, and comparing the order of magnitudes of both sides can help fruitfully to finish problems concerning complex numbers.

5. Lagrange's Interpolation Formula (LIF)

The fourth topic that I prefer to teach is Lagrange's interpolation Formula (LIF). By adopting this formula, it becomes possible to determine or characterize the polynomial $P(x)$ by $1 + \deg P(x)$ distinct points. Most students know this formula, they even write this formula in their papers, and they effortlessly finish their idea. They are partly right! This is because most of the problems concerning the LIF need another complementary innovative idea. Readers can find very interesting ideas about the LIF in books like Andreescu and Dospinescu (2010, 2012).

The first problem has a solution that only needs insight from rational and irrational numbers and examining some coefficients. The problems selection committee had not found it. Their solution was based on the LIF. The first solution is from one of the exam papers and the second solution is based on discussions during the month of July 2016. Fourteen out of 74 students solved this problem. Thus, it seems that this problem was hard and was not a good candidate for being the first one on the exam.

Problem 7. (3rd round Iranian Mathematical Olympiad, 2017, Final Algebra exam, Problem 1) Let $P(x)$ be a polynomial with integer coefficients of degree 2016 and with no rational roots. Prove that there exists a polynomial $Q(x)$ with integer coefficients of degree 1395 such that for all distinct roots r, s of $P(x)$, $Q(r) - Q(s)$ is an irrational number.

Solution. First, we will prove the following lemma.

Lemma 3. Assume r, s are irrational numbers. Then, at least one of $r - s, r^2 - s^2$ is irrational.

Proof. Assume the contrary. We find that $r + s = \frac{r^2 - s^2}{r - s}$ is rational. Therefore $2r = r + s + r - s$ is rational. Contradiction. Our proof is complete.

Back to our problem, let $Q(x) = x^{1395} + x^{1394} + \dots + ax^2 + bx$. We will specify a, b in such a way that for all distinct roots r, s of $P(x)$, $Q(r) - Q(s)$ is an irrational number. First of all, we fix a and increase the value of b . Now, we prove the following lemma.

Lemma 4. If for a fixed a and some (r, s) the value of $r - s$ is irrational, then there is at most one b such that $Q(r) - Q(s)$ is rational.

Proof. If for b, c the values $Q_b(r) - Q_b(s), Q_c(r) - Q_c(s)$ are rational, then we subtract them to find $(b - c)(r - s)$ is rational. Absurd. This completes our proof.

Hence, for all large enough b and for all (r, s) such that $r - s \notin \mathbb{Q}$, $Q_b(r) - Q_b(s)$ is irrational. Analogously, if $r^2 - s^2$ is irrational, for all large enough a and for all (r, s) such that $r^2 - s^2 \notin \mathbb{Q}$, $Q_a(r) - Q_a(s)$ is irrational. Now, choose a, b large enough and we are done.

Second solution. In this solution, we need Lemma 1 above and another lemma, provided as follows.

Lemma 5. If a polynomial $P(x)$ of degree d assumes rational values in at least $d + 1$ rational points, the $P(x)$ has rational coefficients.

Proof. Assume that $P(r_0), \dots, P(r_d)$ are rational for the subset $\{r_0, \dots, r_d\}$ of rational numbers. Then, by Lagrange's Interpolation Formula (LIF), we find that

$$P(x) = \sum_{i=0}^d P(r_i) \frac{(x - r_0) \dots (x - r_{i-1})(x - r_{i+1}) \dots (x - r_d)}{(r_i - r_0) \dots (r_i - r_{i-1})(r_i - r_{i+1}) \dots (r_i - r_d)}.$$

Considering the above formula, it is clear that $P(x)$ has rational coefficients. This completes our proof.

Back to our problem. Consider the polynomial $Q_a(x) = (x + a)^{1395}$, for some a that will be determined later. Assume that $Q_a(x)$ does not work. Then for each a there is a pair (r, s) from the roots of $P(x)$ such that $Q_a(r) - Q_a(s) = (r + a)^{1395} - (s + a)^{1395}$ is an integer. Since we have only finitely many pairs of (r, s) , then there is a pair (r, s) such that $S(a) = (r + a)^{1395} - (s + a)^{1395}$ is rational for all but finitely many a . By Lemma 4, $S(a)$ should have rational coefficients. On the other hand, the coefficients of a^{1394}, a^{1393} are $r - s, r^2 - s^2$, whilst by Lemma 3 both of them cannot be rational. We are done.

The next problem was proposed by me. I wanted to emphasize the fact that the solutions of the inequality $|P(x)| < C$ for some polynomial $P(x)$ and some real number C are a subset of an interval of the form $(-a, a)$. At the very first glance, no one thought about the LIF. However, later, one important property of the LIF seemed helpful. That is, examining the leading coefficients on both sides of the following identity

$$P(x) = \sum_{i=0}^d P(r_i) \frac{(x - r_0) \dots (x - r_{i-1})(x - r_{i+1}) \dots (x - r_d)}{(r_i - r_0) \dots (r_i - r_{i-1})(r_i - r_{i+1}) \dots (r_i - r_d)}$$

shows that the leading coefficient of $P(x)$ is equal to $\sum_{i=0}^d \frac{P(r_i)}{(r_i-r_0)\cdots(r_i-r_{i-1})(r_i-r_{i+1})\cdots(r_i-r_d)}$. So, one can think about

establishing a bound for the denominator. This problem was solved by six students out of 72 contestants and all the six students won a gold medal.

Problem 8. (3rd round Iranian Mathematical Olympiad, 2018, Final Algebra exam, Problem 4) Let $P(x)$ be a non-constant polynomial with real coefficients. For all positive real numbers M , prove that there is a positive integer m such that for any monic polynomial $Q(x)$ of degree greater than or equal to m , the total number of integer solutions of the inequality

$$|P(Q(x))| \leq M$$

does not exceed $\deg Q(x)$.

Solution. It is clear that the solutions of the inequality, $|P(x)| \leq M$ are a subset of an interval of the form $(-a, a)$ for some positive real number a . Now, assume $\deg Q(x) = d \geq m$. Consider integers $x_0 < \cdots < x_d$. Then by Lagrange's interpolation formula, one can find that

$$Q(x) = \sum_{i=0}^d Q(x_i) \prod_{i \neq j} \frac{x-x_j}{x_i-x_j}.$$

Since $Q(x)$ is monic, we find that

$$1 = \sum_{i=0}^d Q(x_i) \prod_{i \neq j} \frac{1}{x_i-x_j}.$$

The right-hand side is less than or equal to

$$\max_i |Q(x_i)| \sum_i \frac{1}{i!(d-i)!} < \frac{2^d}{d!} \cdot \max_i |Q(x_i)|.$$

Hence,

$$\max_i |Q(x_i)| > \frac{d!}{2^d} \geq \frac{m!}{2^m}.$$

Now, choose m such that $\left(-\frac{m!}{2^m}, \frac{m!}{2^m}\right) \subseteq (-a, a)$. We deduce that, from any $d + 1$ integers, at least one of them satisfies the inequality $|Q(x)| > \frac{m!}{2^m}$. But, all the integer solutions of the inequality $|P(Q(x))| \leq M$ must satisfy the inequality $|Q(x)| \leq \frac{m!}{2^m}$. We are done.

6. Multi-Variable Polynomials (MVPs)

The last topic I have selected to discuss is Multi-Variable Polynomials (MVPs). Whenever I teach this topic, I start with the similarities between MVPs and Single-Variable Polynomials (SVPs). That is, I have found that this strategy is more consistent in light of the current knowledge of the trainees and so I explicitly define MVPs and extend upon the analogies. Then, after one or two sessions I start to discuss disanalogies between the MVPs and SVPs. Proceeding this way, students develop a better attitude toward and a better understanding of the MVPs.

Based on the above strategy, I concentrate more on the notion of homogeneous polynomials and representing a MVP as the sum of its

homogeneous parts of different degrees. This was my motivation to write an article about homogeneity (Safaei, 2018).

This problem needs a very basic idea of the growth rate of MVPs. That is, in the SVPs, if $P(x) = a_0 + a_1x + \dots + a_dx^d$, then for each $\varepsilon > 0$, $(a_d - \varepsilon)x^d < P(x) < (a_d + \varepsilon)x^d$ for all but finitely many real x . In this problem, I outline the same idea for the MVPs. Sixteen out of 76 students completely solved this problem.

Problem 9. (3rd round Iranian Mathematical Olympiad, 2017, Algebra exam, Midterm, Problem 3) Do there exist infinitely many points $(x_1, y_1), (x_2, y_2), \dots$ in the Cartesian plane such that for any sequence b_1, b_2, \dots of real numbers there exists a polynomial $P(x, y)$ with real coefficients such that for each i , $P(x_i, y_i) = b_i$?

Solution. Consider $P(x, y) = \sum_{i=0}^d P_d(x, y)$, where $P_k(x, y)$ are homogeneous polynomials of degree k . Then, for all sufficiently large values of $|x|, |y|$, $P(x, y) < C(|x| + |y| + 1)^d$ for some constant C . Now, consider the sequence $b_i = i(|x_i| + |y_i| + 1)^d$. Then, for all large enough i , the equation $P(x_i, y_i) = b_i = i(|x_i| + |y_i| + 1)^d$ has only finitely many solutions.

Remark. One can also consider the sequence $b_i = (|x_i| + |y_i| + 1)^{i!}$.

Remark. At the outset, this problem looks like “Lagrange Interpolation Formula (LIF)” for multi-variable polynomials. That is, assume $\deg P(x, y) = d$. Then, the polynomial $P(x, y)$ has $\frac{d(d+1)}{2}$ unknown coefficients. Assume we have two sets $\{x_0, \dots, x_d\}, \{y_0, \dots, y_d\}$. Then, if we know the value of $P(x_i, y_j)$ for all $0 \leq i, j, i + j \leq d$, then, the polynomial $P(x, y)$ could uniquely be determined as follows:

$$P(x, y) = \sum_{0 \leq i, j, i+j \leq d} P(x_i, y_j) \frac{(x - x_0) \cdots (x - x_{i-1})}{(x_i - x_0) \cdots (x_i - x_{i-1})} \cdot \frac{(y - y_0) \cdots (y - y_{j-1})}{(y_j - y_0) \cdots (y_j - y_{j-1})}.$$

However, although it would be a great achievement to determine a multivariable polynomial through this, we cannot find a good idea to finish the above-mentioned problem.

7. Concluding Remarks

In this article, I outlined a framework concerning the important teaching elements of polynomials. For this reason, I used some problems from recent Iranian Mathematical Olympiads. As has been seen, these problems are challenging but interesting. Proceeding in this way, readers can find different approaches implemented to solve those problems, some notes and remarks about the number of complete solutions, and some notes to expose the weakness of other potential arguments. In addition, I introduced some resources for further reading.

Teaching polynomials needs *a priori* knowledge from multiple sources. In some degree, it is akin to teaching Combinatorics or advanced Number Theory. Furthermore, and quite generally, it also has some degree of idiosyncrasy since, as has been previously shown, it needs insight from calculation and algebraic expressions. Rather than being a problem, it is in fact, a great advantage for those who want to solve challenging problems in Algebra.

8. Acknowledgements

I would like to thank Alessandro Ventullo and Dr. Vlad Crisan for their invaluable and wise guidance in improving the text and the structure of some proofs. I would also like to thank the reviewers at the *World Federation of National Mathematical Competitions* (WFNMC) journal given that their critical comments have helped improve the paper immeasurably. Finally, thanks are due to Professor Alexander Soifer, who kindly responded to my letters and made very important suggestions.

9. References

- [1] T. Andreescu and G. Dospinescu, *Problems from the book*, 2nd edition, XYZ-Press, 2010.
- [2] T. Andreescu and G. Dospinescu, *Straight from the book*, XYZ-Press, 2012.
- [3] T. Andreescu, N. Safaei, and A. Ventullo, *117 polynomial problems from the AwesomeMath Summer Program*, XYZ-Press, 2019.
- [4] N. Safaei, *Searching for Homogeneity Across Multi-Variable Polynomials*, Mathematical Reflections, 1, 2018.
- [5] N. Safaei, *Discrete Approach to a Result Concerning a Contour Integral*, Mathematical Reflections, 2, 2019.
- [6] N. Safaei, *Problem M2544 problem*, Kvant, 1, 2019.

pqr Inequality

Robert Bosch (bobbydrg@gmail.com)



Robert Bosch was Coach and Coordinator of Mathematics Competitions during the period (2014-2016) at Archimedean Schools, Miami, FL, USA, culminating with the 2016 Edyth May Sliffe Award for Distinguished Teaching from the Mathematical Association of America (MAA). Involved in problem solving since 2000, he won a Bronze Medal in VIII Iberoamerican Mathematical Olympiad for University Students. The author of 20 articles and 5 books, he received his B.Sc. in Mathematics from University of Havana, Cuba. Robert has given lectures in different math circles, universities, and summer programs, such as the Metroplex Math Circle, Awesome Math Summer Program, IDEA Math Summer Program, University of Texas at Dallas, Florida Atlantic University, and University of Chicago (USA).

Abstract

In this article we present an elegant proof for bounds on the product of three positive real numbers in terms of their sum and the sum of pairwise products. This result, the *pqr*-Inequality, may become a classic method on mathematical inequalities after acceptance by the mathematical community. Also, we show the solutions to ten problems from Mathematical Olympiads from around the world and from journals. All of them are original and suitable for applications of the *pqr* Inequality, with the idea of *unifying* many inequalities through this powerful and novel method.

Dedicated to Jorge Erick López Velázquez

1 Introduction

There are several versions of the pqr Inequality in the literature, this one deals with symmetric polynomial inequalities in three variables, providing optimal bounds for the product abc . In the standard form, non-negative numbers are considered, resulting in the possibility that two of a, b, c are equal or one of them is 0. This approach was studied by Vasile Cîrtoaje in [3], and by Steven Chow, Howard Halim and Victor Rong in [2], as the result of a research project at the Tournament of Towns Summer Conference 2016. This method was previously communicated in the *Art of Problem Solving* (AoPS) as has been noticed in the references of the above article. In this paper we consider positive numbers and sharp bounds for the product abc by means of the zeroes of the first derivative of a cubic polynomial and Rolle's theorem. Tran Phuong wrote about both methods in the book *Diamonds in Mathematical Inequalities* citing many algebraic identities and not always perfectly clear ideas because his manuscript is a draft copy. Jorge Erick López Velázquez rediscovered the pqr Inequality, working on inequalities for the journal *Mathematical Reflections*. I received his ideas in a private communication, missing the proof of sharpness for abc . The notation introduced by him allowed me to prove the minimal and maximal bounds were the best ones as a consequence of the s -term. His initial idea was that this theorem is very powerful in solving any symmetric polynomial inequality in three variables. I explained to him about the complexity of algebraic identities of high degree and gave some examples where after expansion there are non symmetric terms. Usually, dealing with algebraic expressions of degree higher than 6, involves long and complex algebraic transformations; this task could be fixed by means of symbolic computer programs. Frequently, at the end, when using the pqr Method, polynomial factorizations are required.

After the presentation of the main inequality, we show 10 well-selected examples from Mathematical Olympiads from around the world and from the journal *Mathematical Reflections*. Each one involves new and different techniques in applying the *pqr* Inequality.

Many of the inequalities in this article are homogeneous algebraic expressions, so we may assume conditions on the variables. In our experience this theorem has proven to be useful when $a + b + c = k$, where k is a real number, in practice $k = 1$ or $k = 3$. The condition $ab + bc + ca$ equal to a real constant should be analyzed with more detail.

Other conditions, aside from the typical ones (before mentioned), may arise or be assumed, these are transformed into polynomial conditions on several variables, and curiously the inequality to be proved becomes most simple. There are many examples from the Iran Mathematical Olympiad including the following one:

Let a, b, c be non-negative real numbers, such that

$$\frac{1}{a^2 + 1} + \frac{1}{b^2 + 1} + \frac{1}{c^2 + 1} = 1.$$

Show that

$$ab + bc + ca \leq \frac{3}{2}.$$

2 pqr Inequality

Let a, b, c be non-negative real numbers, and

$$\begin{aligned} p &= \frac{a+b+c}{3}, \\ q &= \frac{ab+bc+ca}{3}, \\ r &= abc, \\ s &= \frac{1}{3} \sqrt{\frac{(a-b)^2 + (b-c)^2 + (c-a)^2}{2}} = \sqrt{p^2 - q}. \end{aligned}$$

The following inequality holds

$$\max \{0, (p+s)^2(p-2s)\} \leq r \leq (p-s)^2(p+2s).$$

Proof.

The proof considers the cubic polynomial

$$P(t) = (t-a)(t-b)(t-c) = t^3 - 3pt^2 + 3(p^2 - s^2)t - r,$$

with three real roots, meaning that $P(t_1) \geq 0$ and $P(t_2) \leq 0$ if $t_1 \leq t_2$ are the roots of $P'(t)$. (Notice we used Rolle's theorem.)

But

$$P'(t) = 3(t-p+s)(t-p-s),$$

therefore

$$\begin{aligned} (p-s)^2(p+2s) - r &\geq 0, \\ (p+s)^2(p-2s) - r &\leq 0. \end{aligned}$$

3 Useful identities

$$a^2 + b^2 + c^2 = 9p^2 - 6q, \quad (1)$$

$$a^3 + b^3 + c^3 = 27p^3 - 27pq + 3r, \quad (2)$$

$$a^4 + b^4 + c^4 = 81p^4 - 108p^2q + 18q^2 + 12pr, \quad (3)$$

$$a^5 + b^5 + c^5 = 243p^5 - 405p^3q + 135p^2r + 45p^2r - 15qr \quad (4)$$

$$a^2b^2 + b^2c^2 + c^2a^2 = 9q^2 - 6pr, \quad (5)$$

$$(a + b - c)(b + c - a)(c + a - b) = -27p^3 + 36pq - 8r. \quad (6)$$

4 Examples

4.1 Generalization of an IMO Problem

Generalization to Problem 1 from the Twenty-Fifth IMO, Prague, Czechoslovakia, June 29 - July 10, 1984. Proposed by M. Stoll, B. Haible, Germany.

Let a, b, c be positive real numbers such that $a + b + c = 1$. Show that

$$ab + bc + ca - \lambda abc \leq \frac{9 - \lambda}{27}, \quad \text{for } 0 \leq \lambda \leq \frac{9}{4}. \quad (7)$$

Solution:

We have $p = \frac{1}{3}$.

$$p - 2s < 0 \Leftrightarrow 0 < ab + bc + ca < \frac{1}{4}.$$

In this case by the pqr -Inequality, $abc > 0$. So

$$ab + bc + ca - \lambda abc < \frac{1}{4} \leq \frac{9 - \lambda}{27}.$$

Now $p - 2s \geq 0$ if and only if

$$\frac{1}{4} \leq ab + bc + ca \leq \frac{1}{3}.$$

So, by the pqr -Inequality we need to prove that

$$3q \leq \frac{9 - \lambda}{27} + \lambda(p + s)^2(p - 2s),$$

equivalent to

$$3q \leq \frac{9 - \lambda}{27} + \lambda \left(\frac{1}{3} + \sqrt{\frac{1}{9} - q} \right)^2 \cdot \left(\frac{1}{3} - 2\sqrt{\frac{1}{9} - q} \right).$$

After squaring and multiply by 27 we get,

$$81q \leq 9 - \lambda + \lambda \left(-2 + 27q + (18q - 2)\sqrt{1 - 9q} \right),$$

which is equivalent to

$$\lambda \left(3(1 - 9q) + 2(1 - 9q)\sqrt{1 - 9q} \right) \leq 9(1 - 9q).$$

Setting $x = 1 - 9q$, we obtain $0 \leq x \leq \frac{1}{4}$, it only remains to prove that $\lambda x(3 + 2\sqrt{x}) \leq 9x$; this clearly holds since $0 \leq \lambda \leq \frac{9}{4}$. This completes the proof.



Example 1. [1]

Problem 11 proposed by Mihai Piticari and Dan Popescu.

Let a, b, c be positive real numbers such that $a + b + c = 1$. Show that

$$6(a^3 + b^3 + c^3) + 1 \geq 5(a^2 + b^2 + c^2).$$

Solution:

$$\begin{aligned}a^2 + b^2 + c^2 &= 1 - 6q, \\ a^3 + b^3 + c^3 &= 1 - 9q + 3r.\end{aligned}$$

So, inequality to be proved becomes

$$3q - 9/4 \cdot r \leq \frac{1}{4},$$

clearly true taking $\lambda = \frac{9}{4}$ in inequality (7).



Example 2.

*The Sixth IMO. Moscow, Soviet Union, June 30 - July 10, 1964.
Problem 2, Hungary.*

Denote by a, b, c lengths of the sides of a triangle. Prove that

$$a^2(b + c - a) + b^2(c + a - b) + c^2(a + b - c) \leq 3abc.$$

Solution:

The inequality is homogeneous, so assume $a + b + c = 1$.

$$\begin{aligned}a^2(1 - 2a) + b^2(1 - 2b) + c^2(1 - 2c) &\leq 3abc, \\ a^2 + b^2 + c^2 - 2(a^3 + b^3 + c^3) &\leq 3abc.\end{aligned}$$

We know that

$$\begin{aligned}a^2 + b^2 + c^2 &= 1 - 6q, \\ a^3 + b^3 + c^3 &= 1 - 9q + 3r.\end{aligned}$$

Thus the original inequality becomes

$$12q - 9r \leq 1.$$

This one was previously considered, as result of the constant $\lambda = \frac{9}{4}$, in the inequality (7).



Example 3.

British Mathematical Olympiad 1999.

Let a, b, c be positive real numbers such that $a + b + c = 1$. Show that

$$7(ab + bc + ca) \leq 2 + 9abc.$$

Solution:

After division by 7, the inequality is

$$ab + bc + ca - 9/7 \cdot abc \leq 2/7.$$

Clearly true by the constant $\lambda = \frac{9}{7}$ in the inequality (7).

4.2 Problems from the journal *Mathematical Reflections*

Example 4.

Problem O11. Iurie Boreico and Ivan Borsenco.

Let a, b, c be positive real numbers not all equal. Prove that

$$\frac{a^2b + a^2c + b^2a + b^2c + c^2a + c^2b - 6abc}{a^2 + b^2 + c^2 - ab - bc - ca} \geq \frac{16abc}{(a + b + c)^2}.$$

Solution:

The inequality is homogeneous. So, we can assume $a + b + c = 1$. With the notation from the pqr -Inequality, we have $p = \frac{1}{3}$, and

$$\frac{3q}{25 - 144q} \geq r.$$

By the upper bound for r , provided by the main theorem, it will be enough to prove that

$$\frac{3q}{25 - 144q} \geq (p - s)^2(p + 2s).$$

Setting $x = 9q$, with $0 < x \leq 1$, this inequality is

$$24x^2 - 49x + 25 \geq (25 - 16x)(1 - x)\sqrt{1 - x}$$

Squaring we obtain

$$256x^5 - 992x^4 + 1441x^3 - 930x^2 + 225x \geq 0,$$

and this polynomial factors as

$$x(16x - 15)^2(x - 1)^2 \geq 0.$$



Example 5.

Problem O388. Nguyen Viet Hung, Hanoi University of Science, Vietnam.

Prove that in any triangle ABC with area S ,

$$\frac{m_a m_b m_c (m_a + m_b + m_c)}{\sqrt{m_a^2 m_b^2 + m_b^2 m_c^2 + m_c^2 m_a^2}} \geq 3S.$$

where m_a, m_b, m_c are the medians.

Solution:

The initial inequality was proposed with the lower bound $2S$

instead of the stronger 3S. Squaring, denoting the medians by x, y, z respectively and using the well-known formula

$$9S^2 = (m_a + m_b + m_c)(m_b + m_c - m_a)(m_c + m_a - m_b)(m_a + m_b - m_c),$$

we need to show that

$$x^2y^2z^2(x+y+z) \geq (x^2y^2 + y^2z^2 + z^2x^2)(y+z-x)(z+x-y)(x+y-z),$$

for x, y, z positive real numbers. With the notation from the pqr -Inequality

$$\begin{aligned} x^2y^2 + y^2z^2 + z^2x^2 &= 9(p^2 - s^2)^2 - 6pr, \\ (y + z - x)(z + x - y)(x + y - z) &= 9p(p^2 - 4s^2) - 8r. \end{aligned}$$

The inequality to be proved becomes

$$\begin{aligned} F = f(r) &= pr^2 + [3(p^2 - s^2)^2 - 2pr] [9p(4s^2 - p^2) + 8r] \geq 0, \\ &= -15pr^2 + [24(p^2 - s^2)^2 - 18p^2(4s^2 - p^2)] r + \\ &+ 27p(p^2 - s^2)^2(4s^2 - p^2) \geq 0. \end{aligned}$$

The function $f(r)$ is clearly concave, so to find the minimal value it's enough to look at the endpoints for r given by the theorem. If $r = (p - s)^2(p + 2s)$ then $F = 6s^2(p - s)^2(p + 2s)^3 \geq 0$. If $p \geq 2s$ and $r = (p + s)^2(p - 2s)$ then $F = 6s^2(p + s)^2(p - 2s)^3 \geq 0$. Finally, if $p < 2s$ then $r > 0$. So, $F = 27p(p^2 - s^2)^2(4s^2 - p^2) \geq 0$.



Example 6.

Problem O399. Titu Andreescu, University of Texas at Dallas, USA.

Let a, b, c be positive real numbers. Prove that

$$\frac{a^5 + b^5 + c^5}{a^2 + b^2 + c^2} \geq \frac{1}{2}(a^3 + b^3 + c^3 - abc).$$

Solution:

We proceed by writing the sum of powers as functions of the symmetric elementary ones. Denote

$$\begin{aligned}x &= a + b + c, \\y &= ab + bc + ca, \\z &= abc.\end{aligned}$$

Then

$$\begin{aligned}a^5 + b^5 + c^5 &= x^5 - 5x^3y + 5xy^2 + 5x^2z - 5yz, \\a^3 + b^3 + c^3 &= x^3 - 3xy + 3z, \\a^2 + b^2 + c^2 &= x^2 - 2y.\end{aligned}$$

Now the original inequality is

$$x^5 - 5x^3y + 4xy^2 + 8x^2z - 6yz \geq 0.$$

Since the original inequality is homogeneous we can suppose without loss of generality that $a + b + c = 1$, that is to say $x = 1$. So, we need to prove that

$$4y^2 - 5y + 1 + (8 - 6y)z \geq 0$$

with $0 < y \leq \frac{1}{3}$ and $z > 0$ due to the well-known inequality $(a+b+c)^2 \geq 3(ab+bc+ca)$. Clearly $8-6y > 0$ and supposing $0 < y < \frac{1}{4}$ the inequality is done because $4y^2 - 5y + 1 = (y-1)(4y-1)$. It only remains to consider the case $\frac{1}{4} \leq y \leq \frac{1}{3}$. This is the hard one, we proceed by the application of the *pqr*-Inequality. Say,

$$z \geq \max \left\{ 0, \left(\frac{1}{3} + \sqrt{\frac{1}{9} - \frac{y}{3}} \right)^2 \cdot \left(\frac{1}{3} - 2\sqrt{\frac{1}{9} - \frac{y}{3}} \right) \right\}.$$

But

$$\frac{1}{3} \geq 2\sqrt{\frac{1}{9} - \frac{y}{3}} \Leftrightarrow y \geq \frac{1}{4},$$

so

$$z \geq \left(\frac{1}{3} + \sqrt{\frac{1}{9} - \frac{y}{3}}\right)^2 \cdot \left(\frac{1}{3} - 2\sqrt{\frac{1}{9} - \frac{y}{3}}\right).$$

After several algebraic transformations the inequality to be proved becomes

$$27(4y^2 - 5y + 1) + (8 - 6y)(9y - 2) + (8 - 6y)(6y - 2)\sqrt{1 - 3y} \geq 0,$$

equivalent to

$$54y^2 - 51y + 11 \geq (36y^2 - 60y + 16)\sqrt{1 - 3y} \geq 0,$$

squaring we obtain

$$3888y^5 - 11340y^4 + 13068y^3 - 6723y^2 + 1566y - 135 \geq 0,$$

or

$$27(4y - 1)(4y^2 - 8y + 5)(3y - 1)^2 \geq 0,$$

completing the proof.



Example 7.

*Problem 35. Viorel Vajaitu and Alexandru Zaharescu.
Gazeta Matematică. [1]*

Let a, b, c be positive real numbers. Show that

$$\frac{ab}{a + b + 2c} + \frac{bc}{b + c + 2a} + \frac{ca}{c + a + 2b} \leq \frac{1}{4}(a + b + c).$$

Solution:

Since the inequality is homogeneous, we can suppose without loss of generality $a + b + c = 1$. So, the original inequality can be rewritten as

$$\frac{ab}{c+1} + \frac{bc}{a+1} + \frac{ca}{b+1} \leq \frac{1}{4}.$$

After clearing denominators, we obtain

$$(a+1)(b+1)(c+1) \geq 4ab(a+1)(b+1) + 4bc(b+1)(c+1) + 4ca(a+1)(c+1).$$

The left side is

$$\begin{aligned} & abc + ab + bc + ca + a + b + c + 1, \\ &= abc + ab + bc + ca + 2, \\ &= r + 3q + 2. \end{aligned}$$

The right side is

$$\begin{aligned} & 4(a^2b^2 + b^2c^2 + c^2a^2) + 8(ab + bc + ca) - 12abc, \\ &= 36q^2 - 24pr + 24q - 12r, \\ &= 36q^2 + 24q - 20r. \end{aligned}$$

So, all that we need to prove is

$$21r \geq 36q^2 + 21q - 2.$$

Let us apply the main inequality.

$$p - 2s < 0 \Leftrightarrow 0 < q < \frac{1}{12},$$

in this case we have to prove that

$$36q^2 + 21q - 2 \leq 0 \Leftrightarrow (3q + 2)(12q - 1) \leq 0.$$

The other case is when

$$p - 2s \geq 0 \Leftrightarrow \frac{1}{12} \leq q \leq \frac{1}{9}.$$

Namely,

$$21 \cdot \left(\frac{2}{9} - q + \frac{2}{3} \sqrt{\frac{1}{9} - q} \right) \cdot \left(\frac{1}{3} - 2\sqrt{\frac{1}{9} - q} \right) \geq 36q^2 + 21q - 2.$$

Setting $x = 9q$, the above inequality becomes

$$2(1 - x^2) \geq 7(1 - x)\sqrt{1 - x}, \quad \text{for } \frac{3}{4} \leq x \leq 1.$$

This is equivalent to

$$4x^2 + 57x - 45 > 0 \Leftrightarrow (x + 15)(4x - 3) > 0.$$



Example 8.

Austrian-Polish Mathematical Olympiad 2000.

Let a, b, c be non-negative real numbers such that $a + b + c = 1$.
Prove that

$$2 \leq (1 - a^2)^2 + (1 - b^2)^2 + (1 - c^2)^2 \leq (1 + a)(1 + b)(1 + c).$$

Solution:

Let us prove the left side.

$$\begin{aligned} & (1 - a^2)^2 + (1 - b^2)^2 + (1 - c^2)^2 \geq 2, \\ \Leftrightarrow & a^4 + b^4 + c^4 - 2(a^2 + b^2 + c^2) + 3 \geq 2, \\ \Leftrightarrow & 18q^2 + 4r \geq 0. \end{aligned}$$

The right side is equivalent to

$$ab + bc + ca + abc + 2 \geq a^4 + b^4 + c^4 - 2(a^2 + b^2 + c^2) + 3.$$

This one can be rewritten as

$$r \leq q(1 - 6q).$$

By the theorem, all that we need to show is

$$\left(\frac{1}{3} - \sqrt{\frac{1}{9} - q}\right)^2 \cdot \left(\frac{1}{3} + 2\sqrt{\frac{1}{9} - q}\right) \leq q(1 - 6q).$$

After several algebraic transformations we obtain

$$6561q^4 + 729q^3 - 81q^2 + 27q \geq 0.$$

This expression factors as

$$27q(243q^3 + 27q^2 - 3q + 1).$$

Setting $x = 3q$, the cubic is

$$9x^3 + 3x^2 - x + 1,$$

which is clearly positive since the quadratic $3x^2 - x + 1$ is positive, completing the proof.



Example 9.

Polish Mathematical Olympiad 1996.

Let a, b, c be positive real numbers, such that $a + b + c = 1$. Show that

$$\frac{a}{a^2 + 1} + \frac{b}{b^2 + 1} + \frac{c}{c^2 + 1} \leq \frac{9}{10}.$$

Solution:

After clearing denominators this inequality is

$$9r^2 + (12 - 30q)r + (81q^2 - 84q + 18) \geq 0.$$

It suffices to prove the discriminant Δ of this quadratic is negative.

$$\Delta = -2016q^2 + 2304q - 504 < 0 \Leftrightarrow 28q^2 - 32q + 7 > 0.$$

Since we know $1 - 9q \geq 0$, it is appropriate to write the quadratic in q as a new quadratic in $(1 - 9q)$. Thus we get,

$$\frac{28}{81}(1 - 9q)^2 + \frac{232}{81}(1 - 9q) + \frac{307}{81} \geq 0.$$



Example 10.

Polish Mathematical Olympiad 1999.

Let a, b, c be positive real numbers with sum 1. Show that

$$a^2 + b^2 + c^2 + 2\sqrt{3abc} \leq 1.$$

Solution:

The original inequality is successively,

$$\begin{aligned} ab + bc + ca &\geq \sqrt{3abc}, \\ a^2b^2 + b^2c^2 + c^2a^2 &\geq abc. \end{aligned}$$

By identity (5), and from $p = \frac{1}{3}$, we get,

$$81s^4 - 18s^2 + 1 \geq 27r.$$

Now, by the pqr -Inequality, we need to show that

$$81s^4 - 18s^2 + 1 \geq (1 - 3s)^2(1 + 6s),$$

which is equivalent to

$$81s^4 - 54s^3 + 9s^2 \geq 0.$$

Finally, this expression factors as

$$9s^2(3s - 1)^2 \geq 0.$$

This completes the proof.



5 Problems for Independent Study

In the following problems the numbers a, b, c are positive real.

1. Given $a + b + c = 1$. Show that

$$\frac{ab}{1 - c^2} + \frac{bc}{1 - a^2} + \frac{ca}{1 - b^2} \leq \frac{3}{8}.$$

2. Given $a + b + c = 2$. Prove that

$$(a) \quad \sqrt{a^2b + b^2c + c^2a} + \sqrt{ab^2 + bc^2 + ca^2} \leq 2.$$

$$(b) \quad \sqrt{a^3b + b^3c + c^3a} + \sqrt{ab^3 + bc^3 + ca^3} \leq 2.$$

3. Let x, y, z be positive real numbers. Prove that

$$\frac{2x^2y^2z^2}{x^3y^3 + y^3z^3 + z^3x^3} + \frac{1}{3} \geq \frac{3xyz}{x^3 + y^3 + z^3}.$$

4. (Russian Mathematical Olympiad 2005).

Given $a^2 + b^2 + c^2 = 1$. Show that

$$\frac{a}{a^3 + bc} + \frac{b}{b^3 + ca} + \frac{c}{c^3 + ab} \geq 3.$$

5. Let a, b, c be non-negative real numbers, such that $a^2 + b^2 + c^2 = 1$. Show that

$$1 \leq a + b + c - abc \leq \frac{8\sqrt{3}}{9}.$$

6. (Vasile Cîrtoaje).

Given $a^2 + b^2 + c^2 = 3$. Prove that

$$(2 - ab)(2 - bc)(2 - ca) \geq 1.$$

7. (Vasile Cîrtoaje).

Given $abc = 1$. Prove that

$$a^2 + b^2 + c^2 + 6 \geq \frac{3}{2}(a + b + c + ab + bc + ca).$$

8. (Le Trung Kien, Vo Quoc Ba Can).

Given

$$ab + bc + ca + 6abc = 9.$$

Show that

$$a + b + c + 3abc \geq 6.$$

References

- [1] Titu Andreescu, Gabriel Dospinescu, Vasile Cîrtoaje, Mircea Lascu. *Old and New Inequalities*. GIL Publishing House. (2004).

- [2] Steven Chow, Howard Halim, Victor Rong. *The pqr-Method*. Crux Mathematicorum. Volume 43(5) and Volume 43(6), (2017).

- [3] Vasile Cîrtoaje. *Mathematical Inequalities, Volume 1, Symmetric Polynomial Inequalities*. University of Ploiesti, Romania, (2015).

Remembering John Horton Conway

Peter James Taylor
University of Canberra
pjt013@gmail.com

Born: 26 December 1937, Liverpool, England

Died: 11 April 2020, New Jersey, USA (age 82)

The mathematics community was shocked to learn of John Conway's death following the main announcement made by Gee [2]. Conway had had health issues, but contracted COVID-19 and died of it.

John Horton Conway FRS studied at Gonville and Caius College, Cambridge, where he obtained Bachelor, Masters and Doctoral degrees, and was a professor there until 1987, when he moved to Princeton University as the John von Neumann Professor in Applied and Computation Mathematics, Emeritus from 2013.

John Conway achieved so many famous results and worked in so many fields that they are well documented elsewhere, and I will not attempt to undertake to relist them. Rather, I will briefly discuss how it came about that he was special guest of the Australian Mathematics Trust when it hosted the World Federation of National Mathematics Competitions (WFNMC) conference in Melbourne in 2002.

Probably his most famous result was the development of the Game of Life, which was introduced to the public by Martin Gardner in *Scientific American* in 1970. But despite the large output of beautiful work which he achieved, there were two features of Conway which stood out, features which are not normally expected of a high-level researcher.

One of these was the way in which he could convey interesting and

very high level mathematics to an average audience, in a book or engagingly in person, exciting and enthusing the audience. People would travel a long way to hear a Conway lecture.

The second feature was Conway's enthusiasm for challenge, not just meeting challenge, but in particular issuing challenge. He not only enjoyed solving problems, but importantly he was a master creator. Both of these features made him highly eligible to be involved with our problem creators.

He also wrote many highly readable books. His book which first attracted my attention was *Winning Ways for Mathematical Plays* [1], which he co-authored with Richard K Guy and Elwyn Berlekamp.

So I was already well informed about Conway, but in 1990 I visited Moscow and discovered the very high esteem in which he was held also in the Soviet Union and presumably other Eastern Bloc countries after my discussion with Kolya Vasiliev [3]. Kolya chaired the problems committee at the time to created the elegant problems which have always appeared in the Tournament of Towns.

Bulgaria hosted the second WFNMC Conference in Pravets in 1994 and to the delight of all who attended, the Bulgarians arranged to have Paul Erdős as their special guest. Of course Erdős gave the principal keynote lecture, but the main value of his attendance was that, in this relatively small and convivial event in which the attendees virtually live together for several days, over the course of the conference everyone had their chance to meet Erdős and discuss mathematics with him.

In 1998 Australia was chosen to host the 4th WFNMC Conference in 2002, to be held in Melbourne. Conway was on my list to play a similar role to that of Erdős in 1994. He was to come to Canberra in 2000, where he gave one of his trademark lectures to a packed audience and after questions he went on to one of his well-known sessions where he could name the day of the week for any date offered from the audience,

which was very popular. While in Canberra I seized the opportunity to discuss the WFNMC conference with him and invite him to be our guest. He agreed immediately and fulfilled his promise two years later.

At the 2002 conference in Melbourne we opened his keynote lecture to the public, and it was given in a large packed theatre at The University of Melbourne. He also attended all other sessions and mixed fully with the 60 or so mathematicians who attended the conference. He clearly enjoyed his interaction with all of us.

It was a great privilege for me and the other participants to have known Conway, and I am sure we all agree he was one of the very great mathematicians of his era. It is a very sad loss that he become a victim of this insidious virus.

References

- [1] Conway, John H, Guy, Richard K and Berlekamp, Elwyn, *Winning Ways for Mathematical Plays*, Academic Press, 1982.
- [2] Gee, Sue, *John Conway dies from Coronavirus*, <https://www.i-programmer.info/news/82-heritage/13614-john-conway-dies-from-coronavirus.html> , 2020.
- [3] NB Vasiliev: Obituary, <http://www.wfnmc.org/obitvassiliev.html> , 1998.

International Mathematics Tournament of Towns

Andy Liu



Andy Liu is a Canadian mathematician. He is a professor emeritus in the Department of Mathematical and Statistical Sciences at the University of Alberta. Liu attended New Method College in Hong Kong. He then did his undergraduate studies in mathematics at McGill University, and earned his Ph.D. in 1976 from the University of Alberta, under the supervision of Harvey Abbott, with a dissertation about hypergraphs. He was the leader of the Canadian team at the International Mathematical Olympiad in 2000 (South Korea) and 2003 (Japan) and acts as vice-president of the Tournament of Towns.

Selected Problems from the Spring 2019 Papers

1. Do there exist seven distinct positive integers with sum 100 such that they are determined uniquely by the fourth largest among them?
2. The sum of all terms of a sequence of positive integers is 20. No term is equal to 3, and the sum of any number of consecutive terms is not equal to 3. Can such a sequence have more than 10 terms?
3. Prove that any triangle can be cut into 2019 quadrilaterals with both incircles and circumcircles.
4. Prove that for any two adjacent digits of a positive multiple of 7, there exists a digit such that no matter how many times it is inserted between these two digits, the resulting number is still a multiple of 7.
5. In triangle ABC , $AB = BC$. K is a point inside such that $KC = BC$ and $\angle KAC = 30^\circ$. Determine $\angle AKB$.

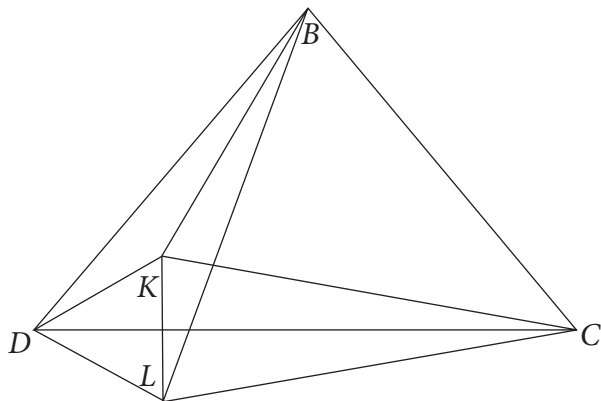
6. As the assistant watches, the audience puts a coin in each of two of 13 boxes in a row. The assistant opens one box that does not contain a coin and exits. The magician enters and opens four boxes simultaneously. Devise a method that will guarantee that both coins are in the four boxes opened by the magician.
7. There are $\binom{10}{5}$ cards each containing a different subset of size 5 of the variables x_1, x_2, \dots, x_{10} . Anna takes a card, Boris takes a card, and then turns alternate until all the cards have been taken. Boris then chooses the values for the variables, provided that $0 \leq x_1 \leq \dots \leq x_{10}$. Can he ensure that the sum of the products of the numbers on his cards is greater than the sum of the products of the numbers on Anna's cards?
8. Starting at $(0,0)$, each segment of a polygonal line either goes up or to the right, and can change directions only at lattice points. Associated with each polygonal line is a chessboard consisting of all unit squares that share at least one point with the polygon line. Prove that for any integer $n > 2$, the number of polygonal lines whose associated chessboards can be dissected into dominoes in exactly n different ways is equal to $\varphi(n)$, the number of positive integers that are less than n and relatively prime to n .

Solutions

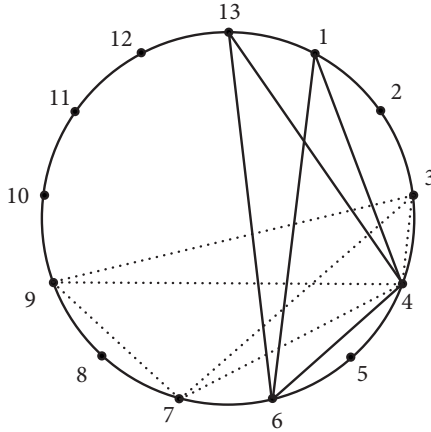
1. If the fourth largest number is 22, then the sum of the largest four numbers is at least $22+23+24+25 = 94$. Hence the sum of the smallest three numbers is at most $100 - 94 = 6$. They must be 1, 2 and 3, and the other four numbers must be 22, 23, 24 and 25.
2. Such a sequence with 11 terms is 1, 1, 4, 1, 1, 4, 1, 1, 4, 1, 1.
3. Divide each side of a triangle into 26 equal parts and join the points of division by lines parallel to the sides of the triangle. This divides the triangle into $26^2 = 676$ triangles. If we combine the four at the top, we have 673 triangles. Now divide each into

three kites by dropping from its incentre perpendiculars to the sides. A kite always has an incircle, and a kite with two right angles opposite each other has a circumcircle. The number of kites is $673 \times 3 = 2019$.

4. Let two adjacent digits of a multiple of 7 be chosen. We separate it into two numbers x and y , with x consisting of all the digits from the left up to and including the first of the two chosen digits, and y consisting of the remaining digits. Let n be the number of digits in y . Then the original multiple is $10^n x + y$, and the number obtained by inserting a digit d between the chosen digits is $10^n(10x + d) + y$. The difference between these two numbers is $10^n(9x + d)$. Since every seventh number is a multiple of 7, there exists at least one value for d such that $9x + d$ is a multiple of 7. Then the new number will also be a multiple of 7. We claim that the same digit d can be added k times between the chosen digits for any positive integer k , and we will still have a multiple of 7. We use mathematical induction on k . The basis $k = 1$ has already been established. Suppose the claim holds up to some $k \geq 1$. The difference between the number after k copies of d has been added and the number after $k + 1$ copies of d has been added is $10^{n+k}(9x + d)$, which is a multiple of 7. This completes the inductive argument.
5. Let L be the point such that BCL is an equilateral triangle, as shown in the diagram below. Perform a counterclockwise 60° rotation about L , mapping C into B and K into D . We claim that D coincides with A . Note that $\angle KLC = 60^\circ + \angle KLB = \angle DLB$. Since $LC = LB$ and $LK = LD$, triangles KLC and DLB are congruent. Hence $DB = KC = BC$. Moreover, since K and L are symmetric about DC , $\angle KDC = 30^\circ$. This justifies the claim. It follows that $\angle AKB = \angle LKB = \frac{1}{2}(360^\circ - 60^\circ) = 150^\circ$.

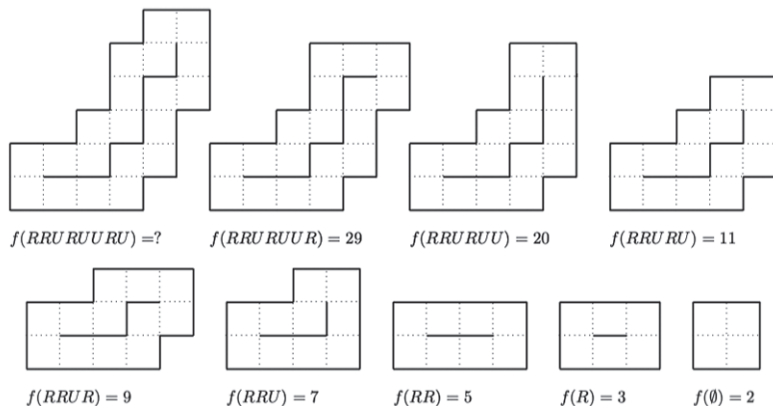


6. The assistant mentally arranges the boxes in clockwise order, dividing the circle into thirteen unit arcs. The length of a chord is measured by the number of unit arcs on the minor arc it cuts off. Consider the quadrilateral in the diagram below. The lengths of its four sides and two diagonals are 1, 2, 3, 4, 5 and 6 in some order, covering all possible chord lengths. When the audience chooses two of the boxes, the assistant determines the length of the chord joining them. Then he rotates the quadrilateral about the centre of the circle until this chord coincides with a side or a diagonal of the quadrilateral. There is always a unique position for the quadrilateral. The assistant will open the box immediately preceding the two adjacent boxes on the quadrilateral. For example, if the boxes chosen by the audience are numbered 7 and 9, the assistant will rotate the quadrilateral to the position shown in dotted lines in the diagram below, and will open the box numbered 2. When the magician comes in, she looks at the number n of the open box. Then she opens the boxes numbered $n + 1$, $n + 2$, $n + 5$ and $n + 7$, reduced modulo 13. Continuing the example, she will open the boxes numbered $2+1=3$, $2+2=4$, $2+5=7$ and $2+7=9$.



7. Boris always chooses $x_1 = x_2 = x_3 = 0$ and $x_8 = x_9 = x_{10} = 100$. He will choose $1 \leq x_4 \leq x_5 \leq x_6 \leq x_7 \leq 12$ according to Anna's action. Then the only cards which matter are those containing all of x_8, x_9 and x_{10} as well as two of x_4, x_5, x_6 and x_7 . Thus the game simplifies to one with six cards containing the pairs $(x_4, x_5), (x_4, x_6), (x_4, x_7), (x_5, x_6), (x_5, x_7)$ and (x_6, x_7) . In the first round, Anna will take (x_6, x_7) . Boris takes (x_5, x_7) . Since both (x_4, x_7) and (x_5, x_6) are better than (x_4, x_6) , each will get one of them in the second round. In the final round, Anna takes (x_4, x_6) over (x_4, x_5) . If Anna takes (x_4, x_7) in the second round, Boris chooses $x_4 = 1, x_5 = 3, x_6 = 4$ and $x_7 = 5$. Anna's sum is $20 + 5 + 4 = 29$ while Boris's sum is $15 + 12 + 3 = 30$. If Anna takes (x_5, x_6) in the second round, Boris chooses $x_4 = 3, x_5 = 4, x_6 = 5$ and $x_7 = 12$. Anna's sum is $60 + 20 + 15 = 95$ while Boris's sum is $48 + 36 + 12 = 96$. Hence Boris always wins.
8. A polygonal line may be represented by a word in which every letter is either U for up or R for right. We use the notation $f(w)$ to denote the number of ways into which the associated chessboard of the word w may be dissected into dominoes. Thus the word $RRURUURU$ represents the polygonal line in the first diagram below. The subsequent diagrams show the polygonal lines repre-

sented by words obtained from $RRURUURU$ by contracting one letter at a time from the end, down to the empty word. In each case, the associated chessboard is also shown, along with the value of f .



The above values of f are calculated recursively, based on the last two. We have

$$\begin{aligned}
 f(RR) &= f(R) + f(\emptyset) = 5; \\
 f(RRU) &= f(\emptyset) + f(RR) = 7; \\
 f(RRUR) &= f(RRU) + f(\emptyset) = 9; \\
 f(RRURU) &= f(\emptyset) + f(RRUR) = 11; \\
 f(RRURUU) &= f(RRUR) + f(RRURU) = 20; \\
 f(RRURUUR) &= f(RRURUU) + f(RRUR) = 29; \\
 f(RRURUURU) &= f(RRURUUR) + f(RRURU) = 38.
 \end{aligned}$$

In each case, $f(w)$ is the sum of two terms. The first term is obtained when the top right square of the chessboard associated with w is covered by a vertical domino. The second term is obtained when the top right square of the chessboard associated with w is covered by a horizontal domino. The placement of this domino may force the placement of other dominoes.

In the first and the fifth equations, where the last two letters of w are the same, $f(w)$ is the sum of the preceding two terms. In the other five equations, where the last two letters of w are different, $f(w)$ is the sum of the preceding term and the last term for which the next two letters are the same, if such a term exists. Otherwise, $f(w)$ is just one more than the preceding term.

For the second, the third and the fourth equations, such a term exists, namely $f(\emptyset) = f(RR) - f(R)$. The second equation may be rewritten as $f(RRU) = (f(RR) - f(R)) + f(RR) = 2f(RR) - f(R)$. For the third and the fourth equations, we have $f(RRURUUR) = 2f(RRU) - f(RR)$ and $f(RRURU) = 2f(RRUR) - f(RRU)$.

For the last two equations, such a term is $f(RRUR) = f(RRURUU) - f(RRURU)$. For the sixth equation, we have $f(RRURUUR) = 2f(RRURUU) - f(RRURU)$. Similarly, $f(RRURUURU) = 2f(RRURUUR) - f(RRURUU)$ for the last equation. In other words, $f(w)$ is the difference between twice the preceding term and the term before that.

In every sequence such as $\{2,3,5,7,9,11,20,29,38\}$, the first two terms are always 2 and 3. If a and b are two consecutive terms, then the next term is either $a+b$ or $2b-a$. It follows that a and b are relatively prime, and $a < b < 2a$. Let the last two terms be m and n . Then m and n are relatively prime, and $m < n < 2m$. We can reconstruct the entire sequence backwards. If $3m > 2n$, as in the case $3 \times 29 > 2 \times 38$, the preceding term must be $2m - n$ or 20 in our example. If $3m < 2n$, as in $3 \times 11 < 2 \times 20$, the preceding term must be $n - m$, or 9 in our example. Continuing this way, we can trace the sequence back to 3 and 2.

Such a numerical sequence matches exactly two words, one starting with U and the other starting with R . There are exactly $\frac{1}{2}\phi(n)$ values of m that satisfy $m < n < 2m$ and are relatively prime to n . Thus there are exactly $\phi(n)$ words whose associated chessboards can be dissected into dominoes in exactly n ways.

The 60th International Mathematical Olympiad

Angelo Di Pasquale
IMO Team Leader, Australia



Angelo was twice a contestant at the International Mathematical Olympiad. He completed a PhD in mathematics at the University of Melbourne studying algebraic curves. He is currently Director of Training for the Australian Mathematical Olympiad Committee (AMOC), and Australian Team Leader at the International Mathematical Olympiad.

He enjoys composing Olympiad problems for mathematics contests.

The 60th International Mathematical Olympiad (IMO) was held 11-22 July 2019 in the city of Bath, United Kingdom. This year was the third time that the UK has hosted the IMO. A total of 621 high school students from 112 countries participated¹. Of these, 65 were girls.

Each participating country may send a team of up to six students, a Team Leader and a Deputy Team Leader. At the IMO the Team Leaders, as an international collective, form what is called the *Jury*. This Jury was ably chaired by Adam McBride.²

The first major task facing the Jury is to set the two competition papers. During this period the Leaders and their observers are trusted to keep all information about the contest problems completely confidential.

The local Problem Selection Committee had already shortlisted 32 problems from the 204 problem proposals submitted by 58 of the participating countries from around the world. During the Jury

¹ This is the largest number of individual students and the largest number of countries in the history of the IMO.

² Adam McBride also chaired the Jury the last time the IMO was held in the UK back in 2002.

meetings four of the shortlisted problems had to be discarded from consideration due to being too similar to material already in the public domain.

Eventually, the Jury finalised the exam problems and then made translations into the 58 languages required by the contestants.

The six problems that ultimately appeared on the IMO contest papers may be described as follows.

1. An easy functional equation proposed by South Africa.
2. A medium geometry problem proposed by Ukraine.
3. A difficult combinatorics problem in algorithmic graph theory couched in the language of social networking. It was proposed by Croatia.
4. An easy number theory problem proposed by El Salvador.
5. A medium to easy problem in combinatorics proposed by the USA.
6. A difficult triangle geometry problem proposed by India.

These six problems were posed in two exam papers held on Tuesday 16 July and Wednesday 17 July. Each paper had three problems. The contestants worked individually. They were allowed four and a half hours per paper to write their attempted proofs. Each problem was scored out of a maximum of seven points.

After the exams, the Leaders and their Deputies spent about two days assessing the work of the students from their own countries, guided by marking schemes, which had been agreed to earlier. A local team of markers called *Coordinators* also assessed the papers. They too were guided by the marking schemes but are allowed some flexibility if, for example, a Leader brought something to their attention in a contestant's exam script that was not covered by the marking scheme. The Team Leader and Coordinators have to agree on scores for each student of

the Leader's country in order to finalise scores. Any disagreements that cannot be resolved in this way are ultimately referred to the Jury.

The contestants found Problem 1 to be the easiest with an average score of 5.18. Problem 6 was the hardest, averaging just 0.4.

The score distributions by problem number were as follows.

Mark	P1	P2	P3	P4	P5	P6
0	73	251	520	211	156	558
1	65	135	46	63	20	25
2	6	30	3	4	168	7
3	24	6	6	7	12	0
4	14	6	5	13	5	1
5	5	3	9	19	7	0
6	52	92	4	47	3	3
7	382	98	28	257	250	27
Mean	5.18	2.40	0.57	3.74	3.57	0.40

The medal cuts were set at 31 points for Gold, 24 for Silver and 17 for Bronze. The medal distributions³ were as follows.

	Gold	Silver	Bronze	Total
Number	52	94	156	302
Proportion	8.4%	15.1%	25.1%	48.6%

These awards were presented at the closing ceremony.

Of those who did not get a medal, a further 144 contestants received an Honourable Mention for scoring full marks on at least one problem.

The following six contestants achieved the most excellent feat of a perfect score of 42.

³ The total number of medals must be approved by the Jury and should not normally exceed half the total number of contestants. The numbers of Gold, Silver and Bronze medals should be approximately in the ratio 1:2:3.

- Baiting Xie, People's Republic of China
- Zhizhen Yuan, People's Republic of China
- Jan Fornal, Poland
- Youngjun Cho, Republic of Korea
- Colin Shanmo Tang, USA
- Daniel Zhu, USA

The 2019 IMO was organised by the United Kingdom Mathematics Trust.

Hosts for future IMOs have been secured up to 2025 as follows.

8-18 July, 2020*	Russian Federation
7-16 July, 2021	USA
2022	Norway
2023	Japan
2024	---
2025	Australia

Much of the statistical information found in this report can also be found on the official website of the IMO.

www.imo-official.org

* Due to the pandemic, IMO 2020 will be held virtually in the month of September.

Tuesday, July 16, 2019

Problem 1. Let \mathbb{Z} be the set of integers. Determine all functions $f: \mathbb{Z} \rightarrow \mathbb{Z}$ such that, for all integers a and b ,

$$f(2a) + 2f(b) = f(f(a + b)).$$

Problem 2. In triangle ABC , point A_1 lies on side BC and point B_1 lies on side AC . Let P and Q be points on segments AA_1 and BB_1 , respectively, such that PQ is parallel to AB . Let P_1 be a point on line PB_1 , such that B_1 lies strictly between P and P_1 , and $\angle PP_1C = \angle BAC$. Similarly, let Q_1 be a point on line QA_1 , such that A_1 lies strictly between Q and Q_1 , and $\angle CQ_1Q = \angle CBA$.

Prove that points P , Q , P_1 , and Q_1 are concyclic.

Problem 3. A social network has 2019 users, some pairs of whom are friends. Whenever user A is friends with user B , user B is also friends with user A . Events of the following kind may happen repeatedly, one at a time:

Three users A , B , and C such that A is friends with both B and C , but B and C are not friends, change their friendship statuses such that B and C are now friends, but A is no longer friends with B , and no longer friends with C . All other friendship statuses are unchanged.

Initially, 1010 users have 1009 friends each, and 1009 users have 1010 friends each. Prove that there exists a sequence of such events after which each user is friends with at most one other user.

Language: English

Time: 4 hours and 30 minutes
Each problem is worth 7 points

Wednesday, July 17, 2019

Problem 4. Find all pairs (k, n) of positive integers such that

$$k! = (2^n - 1)(2^n - 2)(2^n - 4) \cdots (2^n - 2^{n-1}).$$

Problem 5. The Bank of Bath issues coins with an H on one side and a T on the other. Harry has n of these coins arranged in a line from left to right. He repeatedly performs the following operation: if there are exactly $k > 0$ coins showing H , then he turns over the k^{th} coin from the left; otherwise, all coins show T and he stops. For example, if $n = 3$ the process starting with the configuration THT would be $THT \rightarrow HHT \rightarrow HTT \rightarrow TTT$, which stops after three operations.

- (a) Show that, for each initial configuration, Harry stops after a finite number of operations.
- (b) For each initial configuration C , let $L(C)$ be the number of operations before Harry stops. For example, $L(THT) = 3$ and $L(TTT) = 0$. Determine the average value of $L(C)$ over all 2^n possible initial configurations C .

Problem 6. Let I be the incentre of acute triangle ABC with $AB \neq AC$. The incircle ω of ABC is tangent to sides BC , CA , and AB at D , E , and F , respectively. The line through D perpendicular to EF meets ω again at R . Line AR meets ω again at P . The circumcircles of triangles PCE and PBF meet again at Q .

Prove that lines DI and PQ meet on the line through A perpendicular to AI .

Language: English

Time: 4 hours and 30 minutes
Each problem is worth 7 points

Some Country Totals

Rank	Country	Total
1	People's Republic of China	227
1	United States of America	227
3	Republic of Korea	226
4	Democratic People's Republic of Korea	187
5	Thailand	185
6	Russian Federation	179
7	Vietnam	177
8	Singapore	174
9	Serbia	171
10	Poland	168
11	Hungary	165
11	Ukraine	165
13	Japan	162
14	Indonesia	160
15	India	156
15	Israel	156
17	Romania	155
18	Australia	154
19	Bulgaria	152
20	United Kingdom	149
21	Taiwan	148
22	Kazakhstan	146
23	Islamic Republic of Iran	145
24	Canada	144
25	France	142
26	Mongolia	141
27	Italy	140
28	Peru	137
29	Brazil	135
29	Turkey	135
31	Philippines	129
32	Germany	126
33	Saudi Arabia	124
34	Norway	122
35	Belarus	119
36	Estonia	118
37	Hong Kong	117
37	Netherlands	117
39	Slovakia	114
40	Greece	112

Distribution of Awards at the 2019 IMO

Country	Total	Gold	Silver	Bronze	HM
Albania	37	0	0	0	2
Algeria	46	0	0	1	3
Angola	0	0	0	0	0
Argentina	95	0	0	3	1
Armenia	104	0	2	1	2
Australia	154	2	1	3	0
Austria	84	0	0	4	1
Azerbaijan	98	0	0	3	2
Bangladesh	76	0	0	1	4
Belarus	119	0	2	2	2
Belgium	75	0	1	1	3
Bolivia	9	0	0	0	0
Bosnia and Herzegovina	84	0	0	0	5
Botswana	2	0	0	0	0
Brazil	135	0	2	4	0
Bulgaria	152	0	5	1	0
Cambodia	10	0	0	0	1
Canada	144	1	1	4	0
Chile	20	0	0	0	2
Colombia	77	0	0	2	2
Costa Rica	34	0	0	0	2
Croatia	110	0	0	3	3
Cuba	23	0	0	0	2
Cyprus	47	0	0	0	3
Czech Republic	106	0	0	4	2
Democratic People's Republic of Korea	187	3	3	0	0
Denmark	105	0	1	2	3
Dominican Republic	5	0	0	0	0

Country	Total	Gold	Silver	Bronze	HM
Ecuador	32	0	0	0	3
Egypt	12	0	0	0	0
El Salvador	45	0	0	2	0
Estonia	118	0	1	4	0
Finland	78	0	1	1	2
France	142	0	2	4	0
Georgia	108	0	1	4	1
Germany	126	1	0	3	2
Ghana	11	0	0	0	1
Greece	112	0	1	2	3
Guatemala	4	0	0	0	0
Honduras	3	0	0	0	0
Hong Kong	117	0	1	3	1
Hungary	165	1	3	2	0
Iceland	37	0	0	0	2
India	156	1	4	0	1
Indonesia	160	1	4	1	0
Iraq	17	0	0	0	1
Ireland	61	0	1	0	2
Islamic Republic of Iran	145	1	2	3	0
Israel	156	1	3	2	0
Italy	140	0	2	4	0
Japan	162	2	2	2	0
Kazakhstan	146	0	2	4	0
Kenya	0	0	0	0	0
Kosovo	43	0	0	0	3
Kyrgyzstan	19	0	0	0	0
Latvia	56	0	0	0	4
Lithuania	96	0	0	3	3
Luxembourg	9	0	0	0	0
Macau	92	0	0	3	3

Country	Total	Gold	Silver	Bronze	HM
Malaysia	71	0	0	2	2
Mexico	111	0	1	3	2
Mongolia	141	1	1	3	1
Montenegro	33	0	0	0	1
Morocco	80	0	0	1	4
Myanmar	11	0	0	0	0
Nepal	17	0	0	0	1
Netherlands	117	0	1	4	1
New Zealand	89	0	0	2	2
Nicaragua	17	0	0	0	2
North Macedonia	47	0	0	0	2
Norway	122	0	1	3	2
Pakistan	34	0	0	1	1
Panama	37	0	0	1	1
Paraguay	18	0	0	0	0
People's Republic of China	227	6	0	0	0
Peru	137	0	3	1	1
Philippines	129	0	1	5	0
Poland	168	1	3	2	0
Portugal	93	0	1	1	4
Puerto Rico	3	0	0	0	0
Republic of Korea	226	6	0	0	0
Republic of Moldova	100	0	1	1	3
Russian Federation	179	2	4	0	0
Saudi Arabia	124	0	1	4	0
Serbia	171	3	1	2	0
Singapore	174	2	4	0	0
Slovakia	114	0	1	3	2
Slovenia	109	0	2	1	3
South Africa	106	0	0	4	2
Spain	110	0	0	5	1

Country	Total	Gold	Silver	Bronze	HM
Sri Lanka	73	0	0	1	5
Sweden	92	1	0	1	3
Switzerland	89	0	0	3	1
Syria	92	0	1	1	3
Taiwan	148	1	2	3	0
Tajikistan	82	0	1	1	2
Tanzania	3	0	0	0	0
Thailand	185	3	3	0	0
Trinidad and Tobago	34	0	0	0	2
Tunisia	48	0	0	0	4
Turkey	135	1	1	3	1
Turkmenistan	53	0	0	0	3
Uganda	5	0	0	0	0
Ukraine	165	1	4	1	0
United Arab Emirates	0	0	0	0	0
United Kingdom	149	1	2	3	0
United States of America	227	6	0	0	0
Uruguay	29	0	0	0	2
Uzbekistan	81	0	0	1	3
Venezuela	3	0	0	0	0
Vietnam	177	2	4	0	0
Total (112 teams, 621 contestants)		52	94	156	144

N.B. Not all countries sent a full team of six students.



Australian Maths Trust
170 Haydon Drive, Bruce ACT 2617
Australia.
Tel: +61 2 62015136