YES THEY CAN!

Figure 1: The 2012 REU class.

Moshe Rosenfeld[1]

[1]Support from the Vietnam Institute for Advanced Study in Mathematics (VIASM) during the final preparation of this work is gratefully acknowledged.

VIETNAM NATIONAL UNIVERSITY

HANOI UNIVERSITY OF SCIENCE

FACULTY OF MATHEMATICS, MECHANICS AND INFORMATICS

ADVANCED MATHEMATICS PROGRAM

RESEARCH EXPERIENCE FOR UNDERGRADUATES

Figure 2: Nguyen Tho Tung, Do Van Hoan, Le Tien Nam, Tran Van Do, Nguyen Thi Xuan, Hoang Duc Trung, Tran Nhat Tan

Hanoi - 2012

Contents

0.1 Acknowledgments

First and foremost I would like to acknowledge the work of the students who took part in this project. Their willingness to take the extra challenge, their energy, their determination to produce this book during a period of heavy load of classes and final exams were inspiring.

We also want to acknowledge the support and help of Professors Lê Minh Hà and Vũ Hoàng Linh who believed in the students, and helped organize this class.

This class could not happen without the support of the Vietnam Education Foundation (VEF) which facilitated two of my semesters. [2]

And finally, to my wife Sharon Morris who hosted the students, helped them improve their language skills and helped edit this book.

Moshe Rosenfeld

1 Introduction

It was with a lot of trepidation that the advanced mathematics program at Hanoi University of Science (HUS) decided to launch this experimental effort in the Fall semester of 2012, to engage undergraduate students from the program in active research. We knew that they are skillful problem solvers. But could they do research? Can they read research papers, understand them, derive ideas, adopt tools and produce new results? The students had a heavy course load, limited resources and the burden of the pressure to do well in each class they took. We wondered how they would respond to the challenge of "*d*oing research". Despite all this they came, they read papers, they tackled and solved problems, and managed to produce high quality results. This collection of articles is the result of their efforts. They cooperated with each other, they generated jointly ideas, and they wanted to produce this book to showcase their efforts.
They answered our question loudly and clearly: **Yes They Can!**[3].

In the Fall semester of 2012, 15 students initially enrolled in the Research Experience for Undergraduates (REU) class. Most were from K-54, the current junior class. A few were from K-55 and two from K-53 the current graduating class. A few dropped out primarily because of their heavy, required course load. As one of the students put it: "*o*ur course load is so heavy that we cannot find time to think."

Seven students completed the REU class:

Nguyen Tho Tung, Le Tien Nam, Tran Nhat Tan, Tran Van Do, Do Van Hoan, Hoang Duc Trung, Nguyen Thi Xuan.

How does one do research in mathematics? L. Danzer, B. Grünbaum and G.C. Shepard addressed this question in their paper *E*quitransitive Tilings or How to Discover new

[2]This research was funded in part by a grant from the Vietnam Education Foundation (VEF). The opinions, findings, and conclusions stated herein are those of the authors and do not necessarily reflect those of VEF.

[3]One of the articles was submitted and published in the Journal of Graph Theory. We expect to submit soon three more papers based on these articles.

Mathematics[4]. They noted that the crux of the matter is the **problem**. It is easy to come up with difficult problems, they abound in mathematics, some date back more than 2000 years, left to us by the Greeks. The challenge was to find tractable problems, problems that can be easily understood, yet challenging and have a good chance of making progress.

To meet these challenges and address the diversified interests of this group, I chose "elementary" problems. We explored problems in Number Theory, in Geometry and Combinatorics; problems that an intelligent high school student could at least understand even if the solution might be complex or unknown. Intentionally, I started with some problems I knew how to solve or for which solutions had been published or known. This way I could always give students hints and help them make progress. We also tackled some open problems.

Many of the problems we dealt with trace their origin to Paul Erdős, probably the most prolific mathematician in the 20^{th} century. 2013 was his 100^{th} birthday and we would like to dedicate this collection of articles to him[5].

Figure 3: Paul Erdős.

1.1 Number Theory

The first problem we tackled was finding infinitely many quintuples of consecutive integers (runs of length 5) of the form $n^2 + 2m^2$. Nam proved that indeed there are infinitely

[4]L. Danzer, B. Grünbaum and G.C. Shepard, Equitransitive Tilings or How to Discover New Mathematics, Mathematics Magazine, Vol. 60, No. 2, April 1987, pp. 67-89.

[5]We hoped to finish the book in 2013, but we learned that the impossible takes a bit longer.

many such runs, and Tùng found an efficient algorithm that finds m and n for prime numbers p that can be represented in this form. While these are known results (the quintuples of consecutive integers result has not been published yet) both Nam and Tùng found the proofs on their own.

Nam, Tùng and Tân proved that the Diophantine equation $a^2 + b^2 + ab = 7^{2n}$ has a solution which is relatively prime to 7. They generalized it and used it to find new constructions of con-cyclic points with integral distances.

Độ and Tùng proved that for a prime $p > 10$, one can match $\{a_k\}$, the quadratic residues mod p, with $\{b_k\}$, the non-quadratic-residues so that all differences $(a_k - b_k)^2$ mod p will be distinct. This property can be used to construct some combinatorial designs, and prove some properties of certain Hadamard matrices.

1.2 Geometry

The starting point of our geometric problems was distances among points in the plane. Questions about distances among points in the plane, in particular integral distances, are as old as mathematics. We started with N. Anning and Paul Erdős proof that if you have a set of infinite points in the plane such that the distance between any two points of the set is integral then the set must be colinear [6].
Tùng first proved that if infinitely many points in the set are colinear then all must be on one line. Tân proved that given three non colinear points, the number of points whose distances from these points are integral is finite. This proves the Anning-Erdős theorem (this is one of the many known and published proofs of this theorem).
Tùng was able to use Eisenstein integers (numbers of the form $a + b\sqrt{-3}$) that constructed for every integer n, a set of points on a circle with integral distances. This construction was previously found by Harborth, Kemnitz and Möller who used it to give a bound to the diameter of sets of n points with mutual integral distances. Nam was able to find a new, elementary proof. We hope that our approach will help improve these bounds and also guide us to construct sets of points in general position (no three on a line, no four on a circle) with integral distances (the current record is seven points).

In 1935 Paul Erdős proposed the following "elementary" problem: given a point P inside a triangle ΔABC, then the sum of distances of P from the vertices is at least twice the sum of distances of P from the edges. At least six different proofs of this theorem have been published. In 1956 A. Florian managed to generalize Paul Erdős' triangle inequality to convex quadrilaterals. Using a different method Tân managed to find a different proof. He proceeded to generalize the inequality to convex n-gons, answering a question

[6] Anning, Norman H.; Erdős, Paul (1945), "Integral distances", Bulletin of the American Mathematical Society 51 (8): 598 - 600

conjectured in 1956 by A. Florian [7]. Later we discovered papers by Shay Gueron and Itai Shafrir in which the Erdős-Mordell inequality was generalized to star-shaped polygons. The question of characterizing for which polygons equality holds, was left open. Tân solved it.

A classical problem in combinatorial geometry is Nelson's unit distance graph problem:

> *H*ow many colors are needed to color the points in the plane
> so that two points at distance 1 apart receive different colors?

In 1950 Ed Nelson proved that at least four colors are needed and John Isbell showed how to do it using seven colors. Sixty two years later, no progress has been made; we still do not know whether 4 colors are enough or more might be needed.
If you take four points in the plane, then among the six distances determined by them, at least one cannot be an odd integer. This led to the following generalization of the unit distance graph:

> *C*an you color the points in the plane in a finite number of colors, so that two points, an odd distance apart will have different colors?

We can regard the points of the plane as vertices of a graph, connecting two points by an edge if their distance is an odd integer. We call this graph the Odd-Distance graph. A classical result of Erdős and De Bruijn asserts that an infinite graph is k-colorable if and only if every finite subgraph is k-colorable. So to find bounds for the chromatic number of this graph, we need to find finite subgraphs with a large chromatic number. We can then ask: which graphs are subgraphs of this graph? In the book ''Problems in Discrete and Computational Geometry'' the authors claimed that the only obstacle preventing a graph G from being a subgraph of the Odd-Distance graph is containing K_4 as a subgraph. Nam refuted this claim by proving that the 5-wheel is not a subgraph of the odd-distance graph, thus opening the door to many further investigations trying to uncover other graphs that are not subgraphs of the Odd-Distance graph[8]. In the article faithful embedding of 3-colorable graphs in the odd distance graph Nam proved that every 3-colorable graphs can be faithfully embedded in $\mathbb{R}^2$ such that two points are at odd distance apart if and only if they are connected by an edge in the graph. As a byproduct, it produced a new proof that every 3-colorable graph is a subgraph of the odd distance graph and also proved that the maximum number of odd distances among n points in $\mathbb{R}^2$ is the Turán number.

[7] A. Florian, Zu einem Satz von P. Erdös, Eelemente der Mathematik, 1955, pp. 55-59.
[8] This paper was published in the Journal of Graph Theory in 2013

1.3 Combinatorics

A classical puzzle asks the following:

> 101 ants are distributed on a 100 cm long stick. Initially, they all start moving in a randomly chosen preassigned direction (left or right) at a speed of 1 cm/min. When two ants collide, they reverse direction. When an ant reaches the end of the stick, it drops off and disappears. Will all ants eventually disappear? How long will it take?

Salmon are known to leave their hatching place, make a long journey in the ocean, return to their hatching place, spawn the next generation of fish and die. Inspired by this phenomenon and by the ants puzzle, we introduced the salmon Puzzle: given n randomly distributed points on a circle. At the start, each point starts moving along the circle either clockwise or counter clockwise at the same constant speed. When two points collide, they reverse direction. When a point reaches its origin, it "dies."

1. Will they all eventually die?
2. Are there possible initial conditions that will allow some to survive?
3. Starting with n points, how many can survive?

Nam proved many results related to this puzzle.

We included a proof of Sperner's lemma, discovered by Độ. It is one of the known proofs of this famous lemma that Độ rediscovered on his own.

In summary, here is what the students had to say about this mathematical journey:

The experimental Research Experience for Undergraduates (REU) was introduced and organized by Professor Moshe Rosenfeld in the Fall semster of 2012. It was probably the first REU program offered for the advanced mathematics program at Hanoi University of Science. We, the students, are very lucky to be a part of this excellent program.

We officially met Professor Moshe Rosenfeld once a week to either discuss approaches to the questions proposed in the previous weeks or to eagerly listen to Professor Moshe Rosenfeld introducing new problems. Additionally, we were encouraged to discuss with Professor Rosenfeld anytime we wanted. For us, these outside class discussions were the most interesting part of this REU. Most of the time, we did not come up with solutions but we occasionally discovered new ideas and solved some proposed problems. With Prof. Moshe's guidance, some students were able to produce new and original results. For example, Tan and Nam got some new interesting results in Geometry and Graph Theory, one such result was published in the Journal of Graph Theory while other could lead to future publications.

Through this REU program, we learned new skills which, we believe, will be essential skills for our future career. Just to mention some examples: we learned how to read papers to get new ideas, how to cooperate with our colleagues to tackle problems, and how to write a mathematical article in a professional way. In short, we learned 'how to do research in Mathematics'-which was the program's ultimate purpose.

This program could not be run without support from the Department of Mathematics-Mechanics-Informatics at Hanoi University of Science. We would like to express our sincere thanks for our beloved Department. We also want to say thanks to Sharron Morris, who helped us greatly in improving our English and helped us revise this book.

Finally, we would like to express our sincere thanks to Professor Moshe Rosenfeld who brought many interesting problems for us to think, who patiently listened to our approaches, and who consistently pushed us forward in producing this book. Without his guide and encouragement, we would never have had a chance to enjoy such an excellent experience in our life.

2 Number theory

2.1 Matching quadratic and non-quadratic residues modulo p

Nguyen Tho Tung and Tran Van Do

Abstract

We use Weil's theorem to prove that for all primes $p > 5$, $QR_p = \{\alpha_1, \ldots, \alpha_{\frac{p-1}{2}}\}$, the quadratic residues in $\mathbb{F}_p^*$, can be matched with the non-quadratic residues $NR_p = \{\beta_1, \ldots, \beta_{\frac{p-1}{2}}\}$ such that:

$$\{\pm(\alpha_1 - \beta_1), \ldots, \pm(\alpha_i - \beta_i), \ldots, \pm(\alpha_{\frac{p-1}{2}} - \beta_{\frac{p-1}{2}}\} = \mathbb{F}_p^*.$$

2.1.1 Introduction

A classical problem in combinatorial design theory is covering the edges of mK_n (the complete graph of order n where any two vertices are connected by m parallel edges) by copies of a given graph G. If G happens to be a graph of order n we call it a spanning graph design.
In [3], we observed that the smallest integer m for which $G(2n, n-1)$ (a graph of order $2n$, regular of degree $n-1$) can cover the edges of mK_{2n} is $m = n-1$. If indeed this cover exists, we denote it by:

$$(n-1)K_{2n} = (2n-1)G(2n, n-1)$$

For example if $G(2n, n-1) = 2K_n$ (two disjoint copies of the complete graph K_n) then $(n-1)K_{2n} = (2n-1)(2K_n)$ exists if and only if there is a Hadamard matrix of order $2n$.

The crown graph $Cr(2n)$ is the bipartite graph $K_{n,n} \backslash nK_2$ (that is the complete bipartite graph $K_{n,n}$ from which a perfect matching has been deleted). For example, the cycle C_6 and the 3-cube are examples of crown graphs of order 6 and 8 respectively. We asked: is

$$(n-1)K_{2n} = (2n-1)Cr(2n) \tag{2.1.1}$$

If this spanning graph design exists, it creates a $2n \times (2n-1)$ matrix $A_{2n,2n-1}$ as follows: Let $G_1, \ldots G_{2n-1}$ be the labeled $2n-1$ copies of $Cr(2n)$.

1. $A_{1,i} = 1,\ i = 1, 2, \ldots, 2n-1$.
2. $A_{k,i} = 1$ if k belongs to the same partition as the vertex 1 in the labeled graph G_i; -1 otherwise.

We call such matrices *c*rown matrices. If in addition, a crown matrix $A_{2n,2n-1}$ has the following properties:

1. All entries in the matrix are ± 1.
2. Each column has n $+1's$ and n $-1's$.
3. The Hamming distance between any two rows is $\geqslant n-1$.
4. In each column we can identify a perfect matching between the entries $+1$ and -1 such that if we ignore these pairs in calculating the Hamming distance, the remaining Hamming distance between any two rows will be exactly $n-1$

And vice versa, if such a matrix exists, then the spanning graph design (2.1.1) exists. This problem is a puzzle-like problem. To demonstrate it consider the crown graph $Cr(8)$: We wish to label 7 copies of this graph by the integers $1, 2, \ldots, 8$ such that every pair

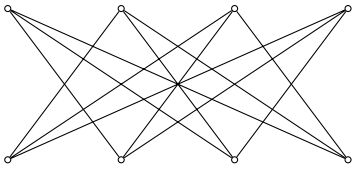


Figure 4: The graph $Cr(8)$

$\{i, j\}$, $1 \leqslant i < j \leqslant 8$ appears in exactly three edges.

A large potential source of structures that can yield crown matrices are the Hadamard matrices. These are orthogonal matrices H, of order $4n$ in which $H_{i,j} = \pm 1$. For such matrices, we can always multiply rows and columns by -1 to obtain a Hadamard matrix of order $4n$ such that $H_{1,i} = H_{i,1} = +1$, $i = 1, 2, \ldots, 4n$. Hence if we remove the first column, we obtain a $2n \times (2n-1)$ matrix in which the Hamming distance between any two rows is n. Now if we can remove a perfect $(+1, -1)$-matching in each column so that for every two rows exactly one pair $(+1, -1)$ is removed we obtain the graph design (2.1.1).

Construction of Hadamard matrices is a well researched topic in combinatorics with many open problems. One construction, the so-called Paley matrices, is based on quadratic residues in finite fields. For such matrices, the existence of the matching described in the abstract, yields the desired $2n \times (2n-1)$ matrix thus constructing the spanning graph design (2.1.1).

The following example can help clarify this construction. We start with a Hadamard matrix of order 8 in standard form (meaning that all entries in the first row and first

column are $+1$). We delete the first column and obtain the following 8×7 matrix:

$$A = \begin{pmatrix} +1 & +1 & +1 & +1 & +1 & +1 & +1 \\ +1 & +1 & +1 & -1 & -1 & -1 & -1 \\ +1 & -1 & -1 & +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & -1 & -1 & +1 & +1 \\ -1 & +1 & -1 & +1 & -1 & +1 & -1 \\ -1 & +1 & -1 & -1 & +1 & -1 & +1 \\ -1 & -1 & +1 & +1 & -1 & -1 & +1 \\ -1 & -1 & +1 & -1 & +1 & +1 & -1 \end{pmatrix}$$

It is easy to verify that the Hamming distance between any two rows is 4. We now construct 7 copies of $K_{4,4}$ as follows:

1. The vertices of each copy will be labeled by $\{1, 2, \ldots, 8\}$
2. In copy number i the vertex n will be in the same partition of vertex 1 if $A_{n,i} = +1$ and the vertices $\{n, m\}$ will be connected by an edge if $A_{n,i}A_{m,i} = -1$.

We wish to remove from each copy a perfect matching so that the remaining graph will be $Cr(8)$ and every pair (n, m) will be an edge in exactly 3 of the seven copies. We leave it to the reader to find a matching in each column such that every pair (m, n) will be selected exactly once. This will yield the graph design:

$$3K_8 = 7Cr(8). \tag{2.1.2}$$

Figure 5 shows two of the seven copies of $Cr(8)$ obtained as follows: in column 1 we

Figure 5: Two copies of the graph $Cr(8)$

match $[i, i+4]$, $i = 1, 2, 3, 4$. This produces the left copy of $Cr(8)$. In column 2 we match $[1, 3], [2, 4], [5, 7], [6, 8]$ which produces the right copy.

Weil's theorem is considered to be one of the most beautiful theorems of the 20^{th} century mathematics. We use this theorem to establish the existence of the matching described in the abstract for Paley Hadamard matrices. This matching proves the existence of the graph designs :

$$(n-1)K_{2n} = (2n-1)Cr(2n)$$

2.1.2 Some notation and background

We introduce some notation, definitions and some background which will be used in this article. We start with a definition and some fundamental properties of finite fields. The proofs of these properties can be found in many elementary books on number theory such as [4].

Definition 2.1 *Let A and B be a partition of $\{1, 2, \ldots, 2n\}$ into two subsets each with n numbers. We say that the partition (A, B) is **matchable** if it is possible to pair the members of A with the members of B so that $\{\pm(a_i - b_i)\} \bmod (2n+1) = \{1, 2, \ldots, 2n\}$.* ■

Let p be a prime number. We denote by $\mathbb{F}_p$ the finite field with p elements. Traditionally, we view this field's elements as $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ where all additions and multiplications are done mod p.

Definition 2.2 *Let $a \neq 0 \in \mathbb{F}_p$. We say that a is a quadratic residue mod p if the equation $x^2 = a \bmod p$ has a solution, else, we say that a is a non-quadratic residue mod p.* ■

We shall denote the set of quadratic residues in $\mathbb{F}_p$ by QR_p and the non-quadratic residues by NR_p.

Example 2.3
Suppose $p = 13$ then $QR_{13} = \{1, 4, 9, 3, 12, 10\}$ and $NR_{13} = \{2, 5, 6, 7, 8, 11\}$. ■

Lemma 2.4 *$\mathbb{F}_p^*$, the group of all non-zero elements in $\mathbb{F}_p$ is cylic.* ■

PROOF See [4], chapter 4, page 40. ■

Lemma 2.4 implies that there exists an element $\alpha \in F_p$ such that each element in $\mathbb{F}_p^*$ can be represented uniquely as α^j for $j \in \{1, \ldots, p-1\}$. Such an element is called a primitive element.
The following simple consequences will be used throughout this note: (we assume that α is a primitive element in $\mathbb{F}_p$).

1. m is a quadratic residue mod p if and only if $m = \alpha^{2i} \bmod p$.
2. $-1 = \alpha^{\frac{p-1}{2}} \bmod p$
3. If $p = 3 \bmod 4$ then $-1 \in NR_p$.
4. If $p = 5 \bmod 8$ then $i = \sqrt{-1} \in NR_p$.

We also use the standard Legendre symbol.

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p \mid a \\ 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is a non-quadratic residue mod } p \end{cases}$$

We have the following properties of Legendre's symbol which will be used through out part 2. The proof of this proposition can be found in 4.

Proposition 2.5 *For any $a, b \in \mathbb{Z}$ we have*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p,$$

and consequently

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

■

We also define what we mean by a character of a finite field.

Definition 2.6 *A character of a finite field is a function $\chi : \mathbb{F} \to \mathbb{C}$ such that*

1. $\chi(0) = 0$
2. $\chi(1) = 1$
3. $\chi(ab) = \chi(a)\chi(b)$

In other words χ is a group homomorphism from $\mathbb{F}^*$ to $\mathbb{C}^*$ and $\chi(0) = 0$.
Also, since $\forall x \in \mathbb{F}_p^*$, $x^k = 1$ for some positive integer k if χ is a character on $\mathbb{F}_p^*$ then $\chi^k(x) = 1$.
This means that for every character χ there is a smallest positive integer s such that $\chi^s(x) = 1$ $\forall x \in \mathbb{F}_p^*$; s is the order of the character χ. ■

Note that the Legendre symbol is a character of order 2 on the field $\mathbb{F}_p$.

We also need the following lemma which will be used to compute sums later. Interested readers can consult a hint in [4], exercises 6, 7, 8 page 63.

Lemma 2.7 *Let a, b, c be integers and p a prime number such that $p \nmid a$ and $p \nmid (a^2 - 4bc)$ then*

$$\sum_{x \in \mathbb{F}_p} \left(\frac{ax^2 + bx + c}{p}\right) = -(\frac{a}{p}).$$

■

Weil's theorem is useful in many proofs. It provides a powerful tool for establishing the existence of elements in final fields with prescribed properties.

Theorem 2.8 (Weil) *Let χ be a character of the finite field $\mathbb{F}_p$ of order s. Let $f(x)$ be a polynomial in $\mathbb{F}_p$ of degree d that cannot be written in the form $c \times h(x)^s$. Then:*

$$\left| \sum_{a \in \mathbb{F}_p} \chi(h(a)) \right| \leqslant (d-1)\sqrt{p}.$$

■

As an example of applying Weil's theorem we prove that $\mathbb{F}_p,\ p = 5 \bmod 8; p > 5$ contains an element $a \in NQ_p$ such that $2a^2 + 1 \in NQ_p$.

Let us denote by E_p the number of nonzero elements a in $\mathbb{F}_p$ such that a and $2a^2 + 1$ are both non quadratic residues mod p. We have the following theorem. [9]

Theorem 2.9

$$E_p = \frac{1}{4} \sum_{a \in \mathbb{F}_p} \left[1 - \left(\frac{a}{p}\right)\right] \cdot \left[1 - \left(\frac{2a^2+1}{p}\right)\right] > 0$$

For primes $p > 5,\ p = 5 \bmod 8$. ■

PROOF For a fixed element a, let us consider the product

$$\left[1 - \left(\frac{a}{p}\right)\right] \times \left[1 - \left(\frac{2a^2+1}{p}\right)\right].$$

If $a = 0$ then the product is 0. In addition, it cannot happen that $2a^2 + 1 = 0 \bmod p$ as -2 is not a quadratic residue mod p. Thus $\left(\frac{2a^2+1}{p}\right)$ only takes values in $\{1, -1\}$. If a or $2a^2 + 1$ is a quadratic residue mod p then the product is 0. Otherwise, when both a and $2a^2 + 1$ are non quadratic residues mod p the product is 4. Thus, the sum

$$\sum_{a \in \mathbb{F}_p} \left[1 - \left(\frac{a}{p}\right)\right] \cdot \left[1 - \left(\frac{2a^2+1}{p}\right)\right]$$

equals 4 times the number of $a \in \mathbb{F}_p$ such that both a and $2a^2 + 1$ are non quadratic residues mod p.

Next we show that $E_p > 0$ for all $p > 5$. First, we can simplify E_p:

$$4E_p = \sum_{a \in \mathbb{F}_p} \left[1 - \left(\frac{a}{p}\right) - \left(\frac{2a^2+1}{p}\right) + \left(\frac{2a^3+a}{p}\right)\right].$$

Or we can rewrite this as

$$4E_p = p - \sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right) - \sum_{a \in \mathbb{F}_p} \left(\frac{2a^2+1}{p}\right) + \sum_{a \in \mathbb{F}_p} \left(\frac{2a^3+a}{p}\right).$$

[9] A second proof of Theorem 2.9 will be given in the appendix.

Let:

$$A = \sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right), \quad B = \sum_{a \in \mathbb{F}_p} \left(\frac{2a^2+1}{p}\right) \text{ and } C = \sum_{a \in \mathbb{F}_p} \left(\frac{2a^3+a}{p}\right)$$

As half the elements in $\mathbb{F}_p^*$ are quadratic residues and half of them are not, we conclude that $A = 0$.
By lemma 2.7 we obtain

$$B = -\left(\frac{2}{p}\right) = 1.$$

For C by Weil's theorem on characters (see theorem 2.8) we have

$$|C| \leqslant 2\sqrt{p}.$$

Hence

$$4E_p \geqslant p - 1 - 2\sqrt{p}.$$

So when $p > 5$ $E_p > 0$. ∎

2.1.3 Main Results

We are now ready to tackle the main result:

Problem 2.10 *Let $\mathbb{F}_p$ be a finite field with $p > 5$ elements where p is a prime number. Is the partition (QR_p, NR_p) of $\mathbb{F}_p^*$ matchable?* ∎

We will illustrate this by some examples.

Example 2.11
For $p = 5$ the set of quadratic residues mod p *is $\{1,4\}$ while the set of non-quadratic residues* mod p *is $\{2,3\}$. There are only two ways to match the sets QR_5 and NR_5, namely $\{[1,3],[2,4]\}$ or $\{[1,2],[3,4]\}$. However, we can easily see that both partitions are not matchable.*
Let's take $p = 7$. $\{[1,6],[2,5],[3,4]\}$ is a matchable partition ∎

More general, for any prime $p \equiv 3 \bmod 4$; -1 is a non quadratic residue mod p so we have the following matchable partition:

Theorem 2.12 *Let p be a prime of the form $4k+3$ then the partition*

$$\{[a,-a] | a \text{ is a quadratic residue } \bmod p\}$$

is matchable. ∎

PROOF Since -1 is not a quadratic residue mod p, for any $a \in QR_p$, $-a \in NQ_p$. Consider the matches $\{(a_i, -a_i)\}$ $a_i \in QR_p$.
$a_i - (-a_i) = 2a_i$, so if $(a_i - (-a_i)) = 2a_i = (a_j - (-a_j)) = 2a_j$ then $a_i = a_j$ and if $(a_i - (-a_i)) = 2a_i = -(a_j - (-a_j)) = -2a_j$ then $a_i = -a_j$ but this is not possible since $a_i \in QR_p$ and $-a_j \in NR_p$.

2.1.3.1 $p = 4k + 3$

When $p = 3 \bmod 4$ we could easily match $x \in QR_p$ with $\alpha \cdot x \in NR_p$ to obtain the matchable partition. For instance $\alpha = -1 \in NR_p$ is a simple choice. We cannot find a single multiplier α when $p = 4k + 1$ as $\pm(\alpha - 1)x,\ x \in QR_p$ will all be either in NR_p or QR_p. Our strategy is to partition QR_p into two equal parts and find different multipliers for each part.

The following example will demonstrate our approach:

QR_{29}	1	16	24	7	25	23	20	28	13	5	22	4	6	9
NQ_{29}	2	3	19	14	21	17	11	18	27	26	10	15	8	12
Diffs	1	13	5	7	25	23	9	19	15	21	17	11	27	3

Note that if $x \bmod 29$ is even then $-x \bmod 29$ is odd. Thus since the differences shown are odd and distinct this means that the set of all differences is $1, 2, \ldots, 28$ or this is a matchable partition. Note that the first 7 differences are quadratic residues and the last 7 are non-quadratic residues. How did we find this matchable partition? Follow the proof below.

2.1.3.2 $p = 8k + 5$

We shall need the following lemmas. Proofs of these lemmas can be found in almost every elementary number theory book. For instance, interested readers can find proofs in [4].

Lemma 2.13 *If $p \equiv 5 \bmod 8$ is a prime then 2 is a non-quadratic residue $\bmod\ p$.* ∎

PROOF As noted in 2.1.2; -1 is a quadratic residue $\bmod\ p$ but $i = \sqrt{-1}$ is not. Besides, we have

$$(1 + i)^2 = 2i.$$

Thus $2 \in NR_p$. ∎

As we saw in lemma 1, all quadratic residues $\bmod\ p$ are of the form α^{2j} for $j \in \{1, \ldots, \frac{p-1}{2}\}$ where α is a primitive element. We partition QR_p into two sets:

$$I_1 = \{x_j = \alpha^{4j} \mid j \in \{1, \ldots, \frac{p-1}{4}\}\}$$

$$I_2 = \{y_j = \alpha^{4j-2} \mid j \in \{1, \ldots, \frac{p-1}{4}\}\}$$

We have the following observations:

1. Since $p = 8k + 5$, $\alpha^{\frac{p-1}{2}} = \alpha^{4k+2} = -1$.

2. $\alpha^{4k+2} I_2 = -I_2 = I_1$.

3. $\alpha^{4j} + \alpha^{4i} \neq 0$.

4. $\alpha^{4j-2} + \alpha^{4i-2} \neq 0$.

To produce the desired matchable partition we will try to multiply I_1 and I_2 by two suitable numbers $\{\gamma, \beta\}$. We list some sufficient conditions for (γ, β):

1. γ, β are both non quadratic residues mod p.

2. The two sets γI_1 and βI_2 partition the set NR_p; in other words, for any $i, j \in \{1, \ldots, \frac{p-1}{4}\}$ we have
$$\gamma x_i \neq \beta y_j \bmod p.$$
We also notice that the squares of the differences between two numbers in a pair $(x_i, \gamma x_i)$ are $(1-\gamma)^2 x_i^2$. As $x_i + x_j \neq 0$ for any i, j all numbers $(1-\gamma)^2 x_i^2$ are different and thus all numbers $\pm(x_i - \gamma x_i)$ are different. Similarly, all differences between two numbers in a pair $(y_i, -\beta y_i)$ are different. Thus, we only need to require one more condition:

3. $\{\pm(x_i - \gamma x_i)\} \cap \{\pm(y_i - \beta y_i)\} = \varnothing$.

A sufficient condition for 3 is $1-\gamma$ is a quadratic residue mod p and $1-\beta$ is not. In summary, we need (γ, β) having the following properties.

1. γ, β are non quadratic residues mod p.

2. $\gamma - 1$ is a quadratic residue mod p.

3. $\beta - 1$ is not a quadratic residue mod p.

4. $\gamma x_i \neq \beta y_j$ for all $i, j \in \{1, \ldots, \frac{p-1}{4}\}$.

By lemma 2.13, for $p = 8k+5$ we can choose $\gamma = 2$, which satisfies the conditions on γ. Therefore, our remaining task is to prove that there exists β satisfying the above conditions.

1. Choose $a \in NR_p$ such that $2a^2 + 1 \in NR_p$. Such a number exists by lemma 2.13.

2. Let $\beta = -2a^2$.

3. $p = 8k+5 \Rightarrow -1 = \alpha^{4k+2}$; $\quad a \in NR_p \Rightarrow a = \alpha^{2m+1} \Rightarrow \beta y_j = -2a^2 \cdot \alpha^{4j+2} = 2 \cdot \alpha^{4m+2} \alpha^{4k+2} \alpha^{4j+2} = 2 \cdot \alpha^{4s+2}$.

4. Thus $2x_i = 2\alpha^{4i} \neq \beta \cdot y_j$.

This establishes the existence of the matchable partition (QR_p, NR_p) when $p \equiv 5 \bmod 8$.

Example 2.14
Example 2.1.3.1 is derived by finding the element a such that:

1. *a is a non quadratic residue* mod p.
2. $2a^2 + 1$ *is a non quadratic residue* mod p.

We know that such an element exists. We find a using the following simple code in SAGE,

```
for i in range (29):
    if (kronecker(i,29)==-1):
        if (kronecker(2*i*i+1,29)==-1):
            print i
```

We can take $a = 3$. *Thus we choose* $\gamma = 2, \beta = -2 \times 3^2 = 11 \bmod 29$. *To produce the partition of* QR_{29} *we need to find a primitive root. Using SAGE, if we type*

```
primitive_root(29)
```

we get 2. *From the the proof above the partition*

$$I_1 = \{1, 16, 24, 7, 25, 23, 20\}, \quad I_2 = \{28, 13, 5, 22, 4, 6, 9\},$$

and

$$2I_1 = \{2, 3, 19, 14, 21, 17, 11\}, \quad 11I_2 = \{18, 27, 26, 10, 15, 8, 12\}.$$

produces the matchable partition in 2.1.3.1. ■

2.1.3.3 $p = 8k + 1$ and p is not a Fermat prime

In this case we will follow the same strategy we employed when $p = 8k + 5$; that is partition QR_p into two equal parts (I_1, I_2), find multipliers (γ, β) such that $(I_1, \gamma I_1), (I_2, \gamma\beta I_2)$ will form a matchable partition. Unlike the previous case, we do not have the convenience of a fixed integer for the multiplier γ that works for all primes $p \equiv 1 \bmod 8$.

First we describe the partition of QR_p. In this case we have:

$$p = 8k + 1 = s \cdot 2^n + 1, \; s = 2m + 1 \geqslant 3.$$

Let α be a fixed primitive element in $\mathbb{F}_p$.

$$\text{Let } I_1 = \{\alpha^{2m+j\cdot 2^n}, \; m = 1, \ldots, 2^{n-2}, \; 0 \leqslant j < s\}. \tag{2.1.3}$$

$$\text{Let } I_2 = \{\alpha^{2m+j\cdot 2^n}, \; m = 2^{n-2} + 1, \ldots, 2^{n-1}, \; 0 \leqslant j < s\}. \tag{2.1.4}$$

1. Claim 1: If $x = \alpha^{2m+j\cdot 2^n} \in I_1$ then $-x \in I_2$
2. PROOF $\quad -1 = \alpha^{s\cdot 2^{n-1}} \Rightarrow \alpha^{2m+j\cdot 2^n} \cdot \alpha^{s\cdot 2^{n-1}} = \alpha^{2m+j\cdot 2^n} \cdot \alpha^{\frac{s-1}{2}\cdot 2^n + 2^{n-1}}$
$= \alpha^{2m+2^{n-1}+s'2^n} \in I_2$.
$(2^{n-1} < 2m + 2^{n-1} \leqslant 2^n; s' = j + \frac{s-1}{2}$ if $j \leqslant \frac{s-1}{2}$; $j - \frac{s-1}{2}$ otherwise.) ∎
3. Claim 2: $\quad \forall x \in I_1 : \; x \cdot \alpha^{2^{n-1}} \in I_2$.
4. PROOF $\alpha^{2m+j\cdot 2^n} \cdot \alpha^{2^{n-1}} = \alpha^{2m+2^{n-1}+j\cdot 2^n} \in I_2$ since $2(m + 2^{n-2}) \geqslant 2(2^{n-2} + 1)$. ∎
5. So: $I_1 = -I_2$. and $-\alpha^{2^{n-1}} I_1 = I_1$.

So all we need now is to find a pair (γ, β) such that:

a. $\gamma \in NR_p$.

b. $\beta \in QR_p$.

c. $\gamma I_1 \cap \gamma\beta I_2 = \varnothing$.

b. $(\gamma - 1)(\gamma\beta - 1) \in NR_p$.

If we take $\beta = -\alpha^{2^{n-1}}$ then condition $[b]$ and $[c]$ are automatically satisfied. We will find a $\gamma \in NR_p$ such that $\gamma - 1 \in QR_p$ while $\gamma \cdot \beta - 1 \in NR_p$.

Actually we can prove something stronger: for any $\beta \neq 0 \in QR_p$ there exists $\gamma \in \mathbb{F}_p$ such that $\gamma \in NR_p; \gamma - 1 \in QR_p$ while $\gamma \cdot \beta - 1 \in NR_p$.

We use the same method as in the case $8k + 5$.
Let $D_p = \mid \{n \in \mathbb{F}_p \mid n \in NR_p,\ n - 1 \in QR_p$ and $\beta \cdot n - 1 \in NR_p\} \mid$.

Lemma 2.15

$$D_p = \frac{1}{8} \sum_{n \in \mathbb{F}_p} \left[1 - \left(\frac{n}{p}\right)\right] \left[1 + \left(\frac{n-1}{p}\right)\right] \left[(1 - \left(\frac{\beta \cdot n - 1}{p}\right)\right].$$

∎

PROOF The argument is identical to the argument used in theorem **??**. ∎

Theorem 2.16

$$8D_p = p + 1 + \sum_{n \in \mathbb{F}_p} \left(\frac{n(n-1)(\beta \cdot n - 1)}{p}\right) > 0$$

∎

PROOF First, we have

$$\sum_{n\in\mathbb{F}_p}\left(\frac{n}{p}\right)=\sum_{n\in\mathbb{F}_p}\left(\frac{n-1}{p}\right)=\sum_{n\in\mathbb{F}_p}\left(\frac{\beta n-1}{p}\right)=0.$$

In addition, by lemma 2.7, we also have

$$\sum_{n\in F_p}\left(\frac{n(n-1)}{p}\right)=-\left(\frac{1}{p}\right),$$

$$\sum_{n\in F_p}\left(\frac{n(\beta n-1)}{p}\right)=-\left(\frac{\beta}{p}\right)=-1,$$

$$\sum_{n\in F_p}\left(\frac{(n-1)(\beta n-1)}{p}\right)=-\left(\frac{\beta}{p}\right)=-1.$$

So, by combining these equalities, we get

$$8D_p=p+1+\sum_{n\in\mathbb{F}_p}\left(\frac{n(n-1)(\beta n-1)}{p}\right).$$

For any $n\in\mathbb{F}_p$ we have

$$\left(\frac{n(n-1)(\beta n-1)}{p}\right)\in\{0,1,-1\}.$$

Hence:

$$\sum_{n\in\mathbb{F}_p}\left(\frac{n(n-1)(\beta n-1)}{p}\right)\geqslant-(p-2).$$

Consequently

$$8D_p=p+1+\sum_{n\in\mathbb{F}_p}\left(\frac{n(n-1)(\beta n-1)}{p}\right)>0.$$

Thus, we can conclude that $D_p>0$ and the partition $(I_1.\gamma I_1),(I_2,\gamma\cdot(-\alpha^{2^{n-1}})\cdot I_2)$ is a matchable partition. ■

Remark 2.17 *1. The assumption $p\neq 2^q+1$ was crucial for the proof. We needed $p=s\cdot 2^k+1$ with $s=2m+1\geqslant 3$.*

2. The Fermat primes $p=2^{2^m}+1$ will be dealt with in the next section.

3. To help the reader appreciate the proof we conclude with an example: $p=97=3\cdot 32+1$. ■

2.1.3.4 $p = 97 = 3 \cdot 2^5 + 1$

1. 5 is primitive mod 97. (use SAGE).
2. $QR_{97} = \{1, 25, 5^4, \ldots, 5^{2m}, \ldots, 5^{94}\}$
3. $I_1 = \{5^2, 5^{2+2^5}, 5^{2+2\cdot 2^5}, 5^4, 5^{4+2^5}, 5^{4+2\cdot 2^5}, \ldots, 5^{16}, 5^{16+2^5}, 5^{16+2\cdot 2^5}\} =$
$\{25, 2, 70, 43, 50, 4, 8, 86, 3, 6, 16, 75, 53, 12, 32, 64, 9, 24, 48, 31, 18, 36, 96, 62\}$
4. $I_2 = \{5^{18}, 5^{18+2^5}, 5^{18+2\cdot 2^5}, 5^{20}, 5^{20+2^5}, 5^{20+2\cdot 2^5} + \ldots 5^{32}, 5^{32+2^5}, 5^{32+2\cdot 2^5}\} =$
$\{27, 72, 95, 93, 54, 47, 94, 89, 11, 22, 91, 81, 65, 44, 85, 73, 33, 88, 79, 49, 66,$
$35, 61, 1\}$
5. $5 \in NR_{97}$, $(5-1) = 4 \in QR_{97}$, $5 \cdot (5^{64}) = 5^{65} \bmod 97 = 14 \in NR_{97}$, $5^{65} - 1 \bmod 97 = 13 \in NR_{97}$.

We are ready now to produce the matchable partition. In order to have a nice display we split the quadratic residues in I_1 and I_2 into two halves. The top line are the quadratic residues, the line below are the matched non-residues and the third line contains the odd differences mod 97. Note that the fur sets of differences contain the odd integers $1, 3, \ldots, 2 \cdot k + 1, \ldots, 95$ proving that this is a matchable partition.

I_1 :

25	2	70	43	50	4	8	86	3	6	16	75
28	10	59	21	56	20	40	42	15	30	80	84
3	89	11	75	91	81	65	53	85	73	33	9

53	12	32	64	9	24	48	31	18	36	96	62
71	60	63	29	45	23	46	58	90	83	92	19
79	49	31	35	61	1	95	27	25	47	93	43

I_2 :

27	72	95	93	54	47	94	89	11	22	91	81
87	38	69	41	77	76	55	82	57	17	13	67
37	63	71	45	23	29	39	7	51	5	19	83

65	44	85	73	33	88	79	49	66	35	61	1
37	34	26	52	74	68	39	7	51	5	78	14
69	87	59	21	41	77	57	55	15	67	17	13

2.1.3.5 p is a Fermat prime

In this section, we will give a proof for the case that p is a Fermat prime. Recall that Fermat primes are primes of the form $p = 2^{2^m} + 1$. The only known Fermat primes are $3, 5, 17, 257, 2^{2^{16}} + 1$. Whether there are more or infinitely many Fermat primes is an open problem. Let $p = 2^{2^m} + 1 = \ m \geqslant 4$. For simplicity, we write $p = 2^{8k} + 1$.

Definition 2.18 *We define the character χ from the multiplicative group $\mathbb{F}_p^*$ to the set of 4^{th} roots of unity as follows:*

$$\chi(x) = \phi(x^{2k})$$

■

Note that for $x \in \mathbb{F}_p^* \Rightarrow x^{2k} \in \{\pm\sqrt{-1} \bmod p, \pm 1\}$. $\phi(1, -1, \sqrt{-1}, -\sqrt{-1}) = (1, -1, i, -i)$ is a homomorphism from $F_p^* \to \mathbb{C}$.
$\chi(x \cdot y) = \chi(x) \cdot \chi(y)$ hence χ is a character of order 4 of the multiplicative group $\mathbb{F}_p^*$. Also χ^2 is the Legendre symbol.

Definition 2.19 *An element $x \in \mathbb{F}_p^*$ such that $x = y^4$ is a **quartic** element.* ■

The following beautiful property of Fermat Primes will also be used in our discussion:

Lemma 2.20 *Every non quadratic residue in $\mathbb{F}_p$, $p = 2^j + 1$ is a primitive element.* ■

PROOF Every non quadratic residue in $\mathbb{F}_p$ is of the form α^{2k+1}. As $\gcd(p-1, 2k+1) = 1$: $\alpha^{m\cdot(2k+1)} \neq 1$ if $m < 2^{2^j}$ hence α^{2k+1} is a primitive element in $\mathbb{F}_p$. ■

We start with an example: let $p = 17$.

1. 14 is a primitive element in $\mathbb{F}_{17}$.
2. $QR_{17} = [14^2, 14^4, \ldots, 14^{2i}, \ldots, 14^{16}] \bmod 17 = [9, 13, 15, 16, 8, 4, 2, 1]$.

This is a matchable partition of (QR_{17}, NR_{17}):

QR_{17}	9	13	15	16		8	2	4	1
NR_{17}	7	12	6	3		5	14	10	11
Diff	15	1	9	13		5	3	11	7

The structure of this matchable partition is as follows:

1. The first row contains the eight quadratic residues mod 17 grouped in three groups:
2. - The first group is $[14^2, 14^4, 14^6, 14^8]$.
   - The second group is $[14^{10}, 14^{14}]$.
   - The third group is $[14^{12}, 14^{16}]$.

3. The second row contains the eight non-residues obtained by multiplying the first group by $14 \in NR_{17}$, the second group by $14^3 \bmod 17 = 7$ and the third group by $14^{-1} \bmod 17 = 11$.

4. The third row are the differences. We show the odd differences so it is easy to see that they are all distinct.

Note that $14 \in NR_{17},\ (14-1) \in QR_{17},\ (7-1), (11-1) \in NR_{17}$.

We are ready now to show the matchable partition in general. As in the example above, we start by a partition of the quadratic residues into three groups (α is a primitive element):

$$S_1 = \{\alpha^{2i} \mid 1 \leqslant i \leqslant 2k\} \quad S_2 = \{\alpha^{4j-2} \mid k \leqslant j \leqslant 2k-1\}$$

$$S_3 = \{\alpha^{4j+4} \mid k \leqslant j \leqslant 2k-1\}.$$

We will prove that there is an element $\alpha \in NR_p$ such that:

$$[S_1, \alpha S_1],\ [S_2, \alpha^3 S_2],\ [S_3, \alpha^{-1} S_3]$$

will form a matchable partition of QR_p and NR_p. (note that $\alpha \in NR_p \Rightarrow \alpha$ is a primitive element).
We first note that if $\alpha \in NR_p$ then α^{-1} and $\alpha^3 \bmod p \in NR_p$. Also, if $x \in S_2$ then $x = \alpha^{4(k+j)+2}$ and $-x = \alpha^{4k} \cdot \alpha^{4(k+j)+2} = \alpha^{4j-+2} \in S_1$. This implies that $\{\pm(x - \alpha^{-1}x)\} \mid x \in S_2$ are all distinct. The same argument applies to S_1 and S_3.

If α satisfies the following:

1. $\alpha S_1 \cup \alpha^3 S_2 \cup \alpha^{-1} S_3 = NR_p$.
2. $\alpha - 1 \in QR_p$ this will insure that $\pm(S_1 - \alpha S_1) = QR_p$.
3. $\alpha^{-1} - 1$ and $\alpha^3 - 1 \in NR_p$ This will insure that $\pm\{S_2 - \alpha^{-1} S_2\} \cup \pm\{S_3 - \alpha^3 S_3\} \subset NR_p$.
4. $\pm\{S_2 - \alpha^{-1} S_2\} \cup \pm\{S_3 - \alpha^3 S_3\} = NR_p$.

Then this partition together with the indicated multipliers will form a matchable partition (QR_p, NR_p).

Claim 2.21 *If there is an $\alpha \in NR_p$ such that $\alpha - 1 \in QR_p,\ \alpha^{-1} - 1, \alpha^3 - 1 \in NR_p$ and $\chi(\alpha^3 - 1) = \chi(\alpha^{-1} - 1)$ then the following holds:*

$$a1. \quad \alpha S_1 \cup \alpha^3 S_2 \cup \alpha^{-1} S_3 = NR_p. \tag{2.1.5}$$

$$a2. \quad \pm (S_1 - \alpha S_1) = QR_p. \tag{2.1.6}$$

$$a3. \quad \pm \{S_2 - \alpha^{-1} S_2\} \cup \pm\{S_3 - \alpha^3 S_3\} = NR_p. \tag{2.1.7}$$

■

PROOF

$$\alpha S_1 = \{\alpha^3, \alpha^5, \ldots, \alpha^{4k+1}\}.$$

$$\alpha^3 S_2 = \{\alpha^{4k+5}, \alpha^{4k+9}, \ldots, \alpha^{8k+1}(= \alpha)\}$$

$$\alpha^{-1} S_3 = \{\alpha^{4k+3}, \alpha^{4k+7}, \ldots, \alpha^{8k-1}\}.$$

This proves a1.

$$(x \in S_1 \Rightarrow -x \notin S_1 \text{ and } \alpha - 1 \in QR_p) \text{ implies a2.}$$ ∎

To prove a3 it is enough to show that $\pm\{S_2 - \alpha^{-1}S_2\} \cap \pm\{S_3 - \alpha^3 S_3\} = \varnothing$. Since $\chi(x) = i$ for $x \in S_2$ and $\chi(y) = -i$ for $y \in S_3$ a3 is satisfied because $\chi(\alpha^3 - 1)\chi(\alpha^{-1} - 1) = -1$. In fact, we can see that $\chi(\alpha^3 - 1)$ and $\chi(\alpha^{-1} - 1)$ are either i or $-i$

In summary, we need to prove that in $\mathbb{F}_p$ we can find a primitive element α that satisfies:

b1. α is not a quadratic residue mod p.

b2. $\alpha - 1$ is a quadratic residue mod p.

b3. $(\alpha^3 - 1),\ (\alpha^{-1} - 1) \in NR_p$.

b4. $\chi(\alpha^3 - 1) \cdot \chi(1 - \alpha^{-1}) = -1$.

These requirements are equivalent to the following:

c1. α is not a quadratic residue mod p.

c2. $\alpha - 1$ is a quadratic residue mod p.

c3. $\chi(\alpha(\alpha^2 + \alpha + 1)) = -1$.

PROOF :

1. $\alpha \cdot (1 - \alpha^{-1}) = \alpha - 1 \in QR_p \Rightarrow (1 - \alpha^{-1}) \in NR_p$.
2. $\chi(\alpha(\alpha^2 + \alpha + 1)) = -1 \Rightarrow (\alpha^2 + \alpha + 1) \in NR_p$. Furthermore, $\chi(\alpha^2 + \alpha + 1) = \chi(\alpha)$.
3. Since $(\alpha - 1) \in QR_p$; $(\alpha - 1)(\alpha^2 + \alpha + 1) = (\alpha^3 - 1) \in NR_p$.
4. Finally, $\chi(\alpha \cdot (\alpha^3 - 1)(1 - \alpha^{-1})) = \chi((\alpha - 1)^2 \cdot (\alpha^2 + \alpha + 1) = \chi(\alpha^2 + \alpha + 1)) = -\chi(\alpha) \Rightarrow \chi((\alpha^3 - 1)(1 - \alpha^{-1})) = -1$.
   (We used the fact that $\alpha - 1 \in QR_p$ implies that $\chi((\alpha - 1)^2) = 1$). ∎

We note that $\chi((\alpha^3-1)\cdot(\alpha^{-1}-1)) = -1 \Rightarrow \chi(\alpha^3-1) = \chi(\alpha^{-1}-1) = i$ or $-i$. Thus $\alpha^3 - 1 = \alpha^{4m+r}$ and $\alpha^{-1} - 1 = \alpha^{4s+r}$, $r \in \{1,3\}$. hence $\pm\{S_2 - \alpha^{-1}S_2\} \cap \pm\{S_3 - \alpha^3 S_3\} = \varnothing$.

We will prove the existence of α by following the same approach as in the previous cases. We first observe that:

$$p(x) = \left(1-\chi(x^2)\right)\left(1+\chi((x-1)^2)\right)\left(1-\chi(x(x^2+x+1)\right)\left(1+\chi(x(x^2+x+1))^2\right) \neq 0$$
$$\text{iff } x \in NR_p, (x-1) \in QR_p \text{ and } \chi(x(x^2+x+1)) = -1.$$

If we denote by G_p the number of $\alpha \in \mathbb{F}_p$ satisfying conditions b1-b4 then we have the following theorem

Theorem 2.22

$$G_p = \frac{1}{16}p(x) > 0.$$

■

PROOF As noted above, $p(x) \neq 0$ only when x satisfies conditions b1 - b4, furthermore, for such x, $p(x) = 16$. Next, we will show that $G_p > 0$.

To estimate G_p we will use Weil's theorem (see 2.8). Indeed, expanding the four terms of $p(x)$ and using theorem 2.8 combined with the same arguments as were used previously in the proof of Theorem 2 we have

$$16G_p \geqslant p - 2 - 41\sqrt{p}.$$

When $p \geqslant 2^{2^4}+1$, for $\mathbb{F}_{17}$ we showed a matchable partition and for $p = 257$ we can take $\alpha = 24$. In this case 23 is a quadratic residue modulo 257 and more over $23(23^2+23+1) \equiv 3^{4\times 60}$. Thus, α satisfies our desired properties. ■

2.1.4 Final Remarks

The above theorem can be extended to any finite field with $q = p^n$ elements with p odd, $q > 5$ and $q \neq 9$. The reason we only chose to work with $\mathbb{F}_p$ is because it is more familiar. The proof for the general case is almost identical to our proof.

Another generalization naturally invites itself. Let $(A = \{a_1, \ldots, a_n\}, B = \{b_1, \ldots, b_n\}$ be an arbitrary partition of $\{1, 2, \ldots, 2n\}$. Is every such partition matchable? The following example shows a partition of $\{1, 2 \ldots, 14\}$ which is not matchable.

$$A = \{1, 4, 7, 10, 13, 3, 12\}$$
$$B = \{2, 5, 8, 11, 14, 6, 9\}$$

This example was found by Roman Shotak. It cane be extended to all integers of the form $10k+4$. This suggests the following question:

Problem 2.23 *For which integers k every even partition of* $\{1, 2, \ldots, 2k\}$ *is matchable?* ■

2.1.5 Acknowledgement

We would like to express our sincere thank to all students who attended our presentations. Their comments helped us improve this article. Finally, we would like to thank Le Tien Nam for his idea in the construction of the matchable partition for $p = 8k + 1$. His idea was the missing piece of the puzzle that we looked for in our search for a solution.

Bibliography

[1] Ding-Zhu and F.K.Hwang, Existence of symmetric skew balanced starters, Proceeding of the American Mathematical Society, Volume 104, Number 2.

[2] Olof Hanner, Construction of Balanced Howell Rotations for $2(p^r + 1)$ partnerships, Journal of Combinatorial Theory, series A 33.

[3] J. Kratochvíl, J. Nešetríl & M. Rosenfeld, Matchability of Hadamard Matrices, Congressus Numerantium 117 (1996) pp. 175-185

[4] Kenneth Ireland, Michael Rosen, A classical introduction to modern number theory, Graduate Texts in Mathematics, volume 84.

[5] Andrew Granville, Binomial coefficient modulo prime powers

2.2 On primes of the form $a^2 + kb^2$

Nguyen Tho Tung

Abstract

Some prime numbers p can be represented in the form $a^2 + kb^2$. For instance, $97 = 9^2 + 4^2$, $59 = 3^2 + 2 \cdot 5^2$. In this article, we will show an efficient algorithm to find such representations for $k = 1, 2, 3, 5$.

Keywords: Prime numbers, Algorithm

2.2.1 Introduction

Anyone fascinated by the beauty of mathematics probably knows the simple but beautiful theorem.

Theorem 2.24 *For any prime $p = 4k + 1$, there exist two positive integers a, b such that*

$$p = a^2 + b^2.$$

■

For example,

$$5 = 1^2 + 2^2, 13 = 2^2 + 3^2, 17 = 1^2 + 4^2, 73 = 3^2 + 8^2.$$

Fermat, a famous French mathematician, was the first to claim to have a proof for the theorem. However, he never publicized it. The first recorded proof was given by Euler using infinite descent [1]. Later on, in 1775, Dirichlet provided a proof using quadratic forms. Dedekind, one of the greatest number theorists in history, provided two proofs using Gaussian integers $\mathbb{Z}[i]$, Gauss gave a proof and many other famous mathematicians did as well. Recently, Don Zagier [2] gave an astonishingly short proof, a one sentence proof, using involutions.

Many of these beautiful proofs were *existence* proofs. They did not provide an efficient fast way to find a and b. They are typical of the 17^{th} to the first half of the 20^{th} century trend in mathematical research that emphasized *conceptual complexity*. In the middle of the 20^{th} century a major shift towards *computational complexity* has been taking place in mathematics research. In this article we concentrate on the computational complexity of Fermat's theorem.

Having said that, given any odd prime number we can figure out immediately whether it can be written as the sum of two positive integers by checking its residue modulo 4. It is, however, not clear how to find such a representation. For instance, 4175433389 is a

prime number, clearly it is of the form $4k+1$, how fast can we find two integers such that $4175433389 = a^2 + b^2$?

In this article, we will demonstrate a way to do it fast, actually with a hand held calculator it can be done in minutes. We also include a code run by SAGE [5] to find such a representation.

A curious reader may ask a more general question

Question 2.25 *Let k be a fixed positive integer. For which primes p, there exists a pair (a, b) such that*

$$a^2 + kb^2 = p.$$

In this case, can we efficiently find such a representation? ■

The first part of the this question is almost completely answered in [4]. This small note will partially answer the second part of this question. To be more precise, we show that for $k = 1, 2, 3, 5$ the algorithm we are going to introduce can also apply to these k.

2.2.2 The case $k = 1$

First, we start by finding an integer $0 < u < p$ such that $u^2 \equiv -1 \bmod p$. This number always exists since $p \equiv 1 \bmod 4$. This can be easily accomplished as follows:

1. Start with $a = 2$.
2. Calculate $m = a^{\frac{p-1}{2}}$.
3. If $m = p - 1$ then $a^{\frac{p-1}{4}} \bmod p = u = \sqrt{-1} \bmod p$ else:
4. a = next-prime(a).

Since half the numbers in $\{1, 2, \ldots p-1\}$ are not quadratic residues mod p you are bound to find $u = \sqrt{-1} \bmod p$ very quickly [10]. When looking for $\sqrt{-1} \bmod p$ this can be done quickly, even by hand for small integers, or by a computer for large ones.

For example, let $p = 61$:

$2^6 \bmod 61 = 3,\ 2^{24} \bmod 61 = 3^4 \bmod 61 = 20,\ 2^{30} = 60 = -1 \bmod 61.$

$$\text{So:} \quad \sqrt{-1} \bmod 61 = 2^{15} \bmod 61 = 11$$

The algorithm for finding a and b is as follows:

[10] A general algorithm for finding a square root modulo p is the Tonelli- Shanks algorithm see 6

1. Find $u = \sqrt{-1} \bmod p$.
2. Let r_k be the sequence of remainders produced by the Euclidean algorithm.
3. Stop when $r_{k+1}^2 < p$.
4. $a = r_{k+1},\ b = \sqrt{p - r_{k+1}^2}$

Clearly, $a^2 + b^2 = p$. The correctness of the algorithm will be established once we prove that $b \in \mathbb{N}$.

We recall the Euclidean algorithm for finding the $GCD(p, u)$:

Algorithm 2.26 (Euclid)

$$r_0 = p \bmod u \qquad p = ub_0 + r_0 \tag{2.2.1}$$
$$r_1 = u \bmod r_0 \qquad u = r_0 \cdot b_1 + r_1 \tag{2.2.2}$$
$$r_2 = r_0 \bmod r_1 \qquad r_0 = r_1 \cdot b_2 + r_2 \tag{2.2.3}$$
$$\vdots \tag{2.2.4}$$
$$r_{k+1} = r_{k-1} \bmod r_k \qquad r_{k-1} = r_k \cdot b_{k+1} + r_{k+1} \tag{2.2.5}$$

■

This algorithm produces a monotonically decreasing sequence of remainders $\{r_0 > r_1 > \ldots > r_n\}$. When x, y are relatively prime the algorithm stops when $r_n = 1$. In particular, $r_{k+1} > 0$.

We define the following sequence:

$$f_0 = b_0, \quad f_1 = 1 + b_0 b_1, \quad f_i = f_{i-2} + b_i f_{i-1}, \forall i \geqslant 2.$$

Lemma 2.27

$$\forall i \in \{0, 1, \cdots, k\} \quad , p = r_i f_{i+1} + r_{i+1} f_i.$$

■

PROOF We proceed by induction on i. For $i = 0$ we have:

$$p = ub_0 + r_0 = (r_0 b_1 + r_1) b_0 + r_0 = r_0(b_0 b_1 + 1) + r_1 b_0 = r_0 f_1 + r_1 f_0,$$

Suppose it is true for all $i < k$. We are going to show that the above equality also happens for $i + 1$. By the induction hypothesis, $p = r_i f_{i+1} + r_{i+1} f_i$. Substituting $r_i = r_{i+1} b_{i+2} + r_{i+2}$ we have:

$$p = (r_{i+1} b_{i+2} + r_{i+2}) f_{i+1} + r_{i+1} f_i = r_{i+1} b_{i+2} f_{i+1} + r_{i+1} f_i + r_{i+2} f_{i+1}.$$

Finally, the equality $f_{i+2} = b_{i+2}f_{i+1} + f_i$ implies that

$$p = r_{i+1}f_{i+2} + r_{i+2}f_{i+1}.$$

Therefore, by the principle of mathematical induction, the above relation holds for all $i \in \{0, 1, \ldots, k\}$. ∎

Corollary 2.28 $f_{k+1} < \sqrt{p}$ ∎

PROOF $p = r_k f_{k+1} + r_{k+1} f_k \geqslant r_k f_{k+1}$. As we assume that $r_k \geqslant \sqrt{p}$, we must have $f_{k+1} < \sqrt{p}$. ∎

2.2.2.1 Proof of the correctness of the Algorithm

Theorem 2.29 *The above algorithm produces* (a, b) *such that* $a^2 + b^2 = p$ *where* $a, b \in \mathbb{N}$. ∎

PROOF Claim: there exist integers g_i such that $\mid g_i \mid \leqslant f_i$ and $g_i^2 + r_i^2 \equiv 0 \bmod p$ for all $i \in \{0, \cdots, k+1\}$.

For $k = 0$: $p = r_0 + ub_0 \equiv 0 \bmod p$. Hence:

$$(r_0 + ub_0)(r_0 - ub_0) = r_0^2 + b_0^2 0 \bmod p \quad (g_0 = b_0).$$

Suppose it is true that for $i < k + 1$. By the Euclidean Algorithm, we have

$$r_{i+1} = -r_i b_{i+1} + r_{i-1}. \tag{2.2.6}$$

Since $u^2 \equiv -1 \bmod p$, we have $r_i^2 + g_i^2 \equiv (r_i + ug_i)(r_i - ug_i) \bmod p$. Because $p \mid (r_i^2 + g_i^2)$, p must either divide $r_i + ug_i$ or $r_i - ug_i$. In other words, there exists $\epsilon \in \{1, -1\}$ such that $-r_i \equiv u\epsilon g_i \bmod p$. Similarly, for r_{i-1} there exists $\eta \in \{-1, 1\}$ such that $r_{i-1} \equiv \eta u g_{i-1} \bmod p$. From 3.3.1, we get:

$$r_{i+1} \equiv u\epsilon b_{i+1} g_i + u\eta g_{i-1} \bmod p.$$

Thus, if we take $g_{i+1} = \epsilon b_{i+1} g_i + \eta g_{i-1}$ we get:

$$r_{i+1}^2 + g_{i+1}^2 \equiv 0 \bmod p.$$

In addition, we also have

$$\mid g_{i+1} \mid = \mid \epsilon b_{i+1} g_i + \eta g_{i-1} \mid \leqslant b_{i+1} \mid g_i \mid + \mid g_{i-1} \mid \leqslant b_{i+1} f_i + f_{i-1} = f_{i+1}.$$

Thus g_{i+1} satisfies our claim and by induction, the claim is proved.

By corollary 2.28, we can see that $g_{k+1} \leqslant f_{k+1} < \sqrt{p}$. Since $p \mid (r_{k+1}^2 + g_{k+1}^2)$, there exists an integer m such that $r_{k+1}^2 + g_{k+1}^2 = mp$ for some m. However, since r_{k+1} and g_{k+1} are both smaller than $\sqrt{p}$ (since $f_{k+1} < \sqrt{p}$), we conclude that $r_{k+1}^2 + g_{k+1}^2 < 2p$. Consequently, $m = 1$ and

$$r_{k+1}^2 + g_{k+1}^2 = p.$$

∎

The following example illustrates the algorithm:

Example 2.30
Let $p = 97 = 4 \cdot 24 + 1$. We know that p can be written as the sum of two squares. Let us find this representation by using our algorithm. First we need to find a number u such that

$$u^2 \equiv -1 \bmod 97.$$

either by paper/pencil calculation or using SAGE, we can easily find $u = 22$. Next, we have

$$97 = 22 \times 4 + 9.$$

Since $9^2 < 97$, our algorithm stops here. We have $a = 9$ and $b = \sqrt{97 - 81} = 4$. ■

Example 2.31
Let us demonstrate how quick this algorithm is for $p = 4175433389$ which we mentioned earlier. First, we can easily find that a square root of -1 modulo p is 457631382. We are ready now to find the sequence of remainders in our algorithm:

$$r_0 = mod(p, u) = 56750951,$$

$$r_1 = mod(u, r_0) = 3623774,$$

$$r_2 = mod(r_0, r_1) = 2394341,$$

$$r_3 = mod(r_1, r_2) = 1229433,$$

$$r_4 = mod(r_2, r_3) = 1164908,$$

$$r_5 = mod(r_3, r_4) = 64525,$$

$$r_6 = mod(r_4, r_5) = 3458.$$

We can observe that $r_5^2 > p$ but $r_6^2 < p$. Thus, we can take $a = r_6$ and $b = \sqrt{p - a^2} = 64525$. In summary, we have

$$4175433389 = 3458^2 + 64525^2.$$

■

It is remarkable that the algorithm executed only six calculations of $a \bmod b$ on a 10 digits long integer.

2.2.2.2 SAGE code

The following SAGE function will decide whether a prime p is the sum of two squares and if this is the case, this algorithm also provides such a presentation.

```
def a(p):
    if mod(p,4)== 3:
        print 'p cannot be written as a^2 + b^2.'
    else:
        a = p
        b = mod(-1,p).sqrt()
        r = a%b
        while r^2 > p:
            r = a%b
            a = b
            b = r
        c = sqrt(p-r^2)
        print (r,c)
```

For example, if we type $a(97)$ we get $(9,4)$.

$$97 = 9^2 + 4^2.$$

2.2.3 $p = a^2 + k \cdot b^2$

Clearly, if $p = a^2 + k \cdot b^2$ then $a^2 = -k \cdot b^2 \bmod p$ hence $-k$ must be a quadratic residue mod p. For which primes p $(-k)$ is a quadratic residue mod p? The answer is given by the beautiful theory of quadratic reciprocity. It started with Fermat around 1650, formulated and conjectured by Euler in 1744, tackled by Legendre in the $1790's$ and finally proved by Gauss in 1979 when he was 19 years old. It states:

A: $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{2}}$ when p and q are odd primes.

B: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

C: $\left(\frac{2}{p}\right)$ [11] $= (-1)^{\frac{p^2-1}{8}}$

2.2.3.1 $k = 2$

Theorem 2.32 *An odd prime p can be represented in the form $a^2 + 2b^2$ if and only if $p \equiv 1, 3 \bmod 8$.* ■

[11] This is the Legendre symbol.

PROOF The necessary part is a direct consequence of item C: above. As an aside, there is an elementary proof that -2 is a quadratic residue mod p when $p = 1 \bmod 8$:

If $p = 1 \bmod 8$ then -1 and $i = \sqrt{-1} \bmod p$ are both quadratic residues mod p. Since $(1-i)^2 = -2 \cdot i$, -2 is a quadratic residue mod p.

Suppose that p is of the form $8k+1$ or $8k+3$, then there exists an integer u such that $u^2 \equiv -2 \bmod p$. We consider the following set:

$$A = \{x + uy \mid 0 \leqslant x \leqslant [\sqrt{p}], 0 \leqslant y \leqslant [\sqrt{p}]\}.$$

This set has $([\sqrt{p}]+1)^2 > p$ elements, so there must exist two elements that have the same residue modulo p. Suppose $x_1 + uy_1$ and $x_2 + uy_2$ are these two elements. Then we have

$$\mid x_1 - x_2 \mid^2 \equiv a^2 \mid y_1 - y_2 \mid^2 \equiv -2 \mid y_1 - y_2 \mid^2 \bmod p.$$

If we put $a = \mid x_1 - x_2 \mid, b = \mid y_1 - y_2 \mid$, then they are not both 0 and $p \mid a^2 + 2b^2$. Moreover, by the definition of the set A, we also have $a < \sqrt{p}$ and $b < \sqrt{p}$. Thus $a^2 + 2b^2$ must be either p or $2p$. If $a^2 + 2b^2 = p$, then we are done. Otherwise, we must have $2p = a^2 + 2b^2$. This equality implies that a is even, so $a = 2a_1$. We then have $p = 2a_1^2 + b^2$ ∎

2.2.4 The algorithm for finding (a, b) such that $a^2 + 2b^2 = p$

We start with an integer $0 < u < p$ such that $u^2 \equiv -2 \bmod p$. As in the case $p = a^2 + b^2$ we apply the Euclidean algorithm to (p, u):

$$r_0 = p \bmod u \qquad p = ub_0 + r_0 \tag{2.2.7}$$

$$r_1 = u \bmod r_0 \qquad u = r_0 \cdot b_1 + r_1 \tag{2.2.8}$$

$$r_2 = r_0 \bmod r_1 \qquad r_0 = r_1 \cdot b_2 + r_2 \tag{2.2.9}$$

$$\vdots \tag{2.2.10}$$

$$r_{k+1} = r_{k-1} \bmod r_k \qquad r_{k-1} = r_k \cdot b_{k+1} + r_{k+1} \tag{2.2.11}$$

We stop when $r_{k+1}^2 < p$. By the same argument as in the $a^2 + b^2$ case, we can find g_{k+1} such that $r_{k+1}^2 + 2g_{k+1}^2 \in \{p, 2p\}$ for some $\mid g_{k+1} \mid < \sqrt{p}$. There are two possibilities:

Case 1. r_{k+1} is odd. Then $r_{k+1} + 2g_{k+1}^2$ is odd and consequently, $r_{k+1}^2 + 2 \cdot g_{k+1}^2$ cannot be $2p$. Thus, we must have $r_{k+1}^2 + 2 \cdot g_{k+1}^2 = p$.

Case 2. If $r_{k+1} = 2m$ is even. Then $r_{k+1}^2 + 2g_{k+1}^2$ is even and must be equal $2p$

$$r_{k+1}^2 + 2g_{k+1}^2 = 2p \Longrightarrow 2m^2 + g_{k+1}^2 = p.$$

Finding $u = \sqrt{-2} \bmod p$ can be done very quickly.

If $p = 8k + 3$, then $u = (-2)^{2k+1}$. Since -2 is a quadratic residue modulo p we have

$$1 = (-2)^{\frac{p-1}{2}} = (-2)^{4k+1} \bmod p \Longrightarrow -2 = (-2)^{4k+2} \bmod$$

$$\Longrightarrow (-2)^{2k+1} = \sqrt{-2} \bmod p.$$

For instance, let $p = 59 = 8 \times 7 + 3$. Then, $\sqrt{-2} \bmod 59 = (-2)^{2\times 7+1} \bmod 59 = 36$. Executing our algorithm we get:

$$r_0 = 59 \bmod 36 = 23,$$

$$r_1 = 36 \bmod 23 = 13,$$

$$r_2 = 23 \bmod 13 = 10,$$

$$r_3 = 13 \bmod 10 = 3.$$

We stop here because $r_3^2 < p$. Since r_3 is odd, we get:

$$59 = 3^2 + 2 \times 5^2.$$

The following example highlights the efficiency of the algorithm: it takes only 8 simple mod computations on a 10-digit long integer to find a and b.

Example 2.33
Let us consider $p = 2030390003$ *which is of the form* $8k + 3$. *Therefore,* p *can be written in the form* $a^2 + 2b^2$. *Either using the simple method introduce in example* 3 *or using* $SAGE$, *we can efficiently find that* $u = 323173818$ *is a square root of* -2 *modulo* p. *We are now ready to run our algorithm*

$$r_0 = p \bmod u = 91347095.$$

$$r_1 = u \bmod r_0 = 49132533.$$

$$r_2 = r_0 \bmod r_1 = 42214562.$$

$$r_3 = r_1 \bmod r_2 = 6917971.$$

$$r_4 = r_2 \bmod r_3 = 706736.$$

$$r_5 = r_3 \bmod r_4 = 557347.$$

$$r_6 = r_4 \bmod r_5 = 149389.$$

$$r_7 = r_5 \bmod r_6 = 109180.$$

$$r_8 = r_6 \bmod r_7 = 40209.$$

We can see that $r_8^2 < p$ *but* $r_7^2 > p$, *so we stop at* r_8. *Since* r_8 *is odd, we arrive at case* 1. *Our algorithm tells us that*

$$2030390003 = 40209 + 2 \times 14381^2.$$

■

Remark 2.34 *Will the algorithm stop at an odd remainder? The answer is not necessarily. Take* $p = 83$. *A square root of* -2 *modulo* 83 *is* 9. *Now* $r_0 = mod(83, 9) = 2$. *Our algorithm stops after only one step. We arrive at the second possibility and get*

$$83 = 2 \times 1^2 + 9^2.$$

■

The following example illustrates the process of finding $\sqrt{-2} \bmod p$:

Example 2.35
Let $p = 353 = 11 \cdot 32 + 1$.

1. $(-2)^{176} = 1 \bmod 353 \qquad 3^{176} = -1 \bmod 353$
2. $(-2)^{88} = 1 \bmod 353$
3. $(-2)^{44} = -1 = 3^{126} \bmod 353$
4. $(-2)^{22} \bmod 353 = 311 = 3^{88} \bmod 353$
5. $(-2)^{11} \bmod 353 = 70 \qquad 3^{44} \bmod 353 = 283 = -70 \bmod 353$
6. $(-2)^{11} = 3^{44+176} \bmod 353$
7. $-2 = (-2)^{12} \cdot 3^{352-220} \bmod 353$
8. $\Longrightarrow \sqrt{-2} = (-2)^6 \cdot 3^{66} \bmod 353 = 307$

Applying the Euclidean algorithm we get:

1. $353 \bmod 307 = 46$
2. $307 \bmod 46 = 31$
3. $46 \bmod 31 = 15$
4. $353 = 15^2 + 128 = 15^2 + 2 \cdot 8^2$. ■

2.2.5 The case $k = 3$

With a similar proof to the case $k = 2$, we can show that.

Theorem 2.36 *A prime number* p *can be represented in the form* $x^2 + 3y^2$ *iff* $p \equiv 1 \bmod 3$. ■

Comment 2.37 Note that since the arithmetic progression $3k + 1$ contains infinitely many primes due to Dirichlet's theorem. Therefore, there are infinitely many primes of the form $a^2 + 3b^2$.

We start by finding u such that $u^2 \equiv -3 \bmod p$. Then we apply the Euclidean algorithm to (p, u). As in the previous cases, we can find r_{k+1} and g_{k+1} such that $r_{k+1}^2 + 3g_{k+1}^2 \in \{p, 2p, 3p\}$. Moreover $r_{k+1}^2 + 3g_{k+1}^2 \neq 2p$ as this would imply that either 2 divides p or $p \equiv 4 \bmod 8$. Thus, we have $r_{k+1}^2 + 3g_{k+1}^2 \in \{p, 3p\}$. We divide the algorithm into two cases.

Case 1. r_{k+1} and 3 are relatively prime. This happens only when

$$r_{k+1}^2 + 3g_{k+1}^2 = p.$$

In this case, the pair (r_{k+1}, g_{k+1}) yields $p = r_{k+1}^2 + 3 \cdot g_{k+1}$.

Case 2. $3 \mid r_{k+1}$. Then we have

$$g_{k+1}^2 + 3 \times \left(\frac{r_{k+1}}{3}\right)^2 = p.$$

Thus, $(g_{k+1}, \frac{r_{k+1}}{3})$ gives us again a representation of p in the form $a^2 + 3b^2$. We will illustrate this algorithm with some examples.

Example 2.38
Consider $p = 100003$. A square root of $-3 \bmod p$ is $u = 14241$. Executing the algorithm we have:

$$100003 \bmod 14241 = 316.$$

Since $316^2 < p$ we have

$$100003 = 316^2 + 3 \times 7^2.$$

■

Example 2.39
We now illustrate the process of finding $\sqrt{-3}$. Let $p = 457 \equiv 1 \bmod 3$.

It is easy to find that $\sqrt{-3} \bmod 457$ is 190. Applying the Euclidean algorithm we get:

$$457 \bmod 190 = 77$$
$$190 \bmod 77 = 36$$
$$77 \bmod 36 = 5$$
$$5^2 + (457 - 25) = 5^2 + 3 \cdot 144 = 5^2 + 3 \cdot 12^2 = 457.$$

■

2.2.6 The case $k = 5$

We begin with the following theorem whose proof can be found in [4].

Theorem 2.40 *A prime p can be represented in the form $a^2 + 5b^2$ iff $p = 5$ or*

$$p \equiv 1, 9 \bmod 20.$$

■

Again, we can also show that there exist a pair (r_k, g_k) where r_k is the first remainder such that $r_k^2 < p$ such that

- $r_k^2 + 5g_k^2$ is divisible by p
- $r_k, g_k < \sqrt{p}$.

These tell us that $r_k^2 + 5g_k^2 = mp$ for some $1 \leqslant m \leqslant 5$. We observe that if $r_k^2 + 5g_k^2 = mp$, then mp is a quadratic residue modulo 5. However, since p is a quadratic residue modulo 5 , we can conclude that m is also a quadratic residue modulo p. Hence, $m \in \{1, 4, 5\}$. We can analyze these cases as follows.

First, we observe that if $a^2 + 5b^2 = 4p$, then both a and b are even. In this case, if we let $a'^2 + 5b'^2 = p$ where $a' = \frac{a}{2}, b' = \frac{b}{2}$.

Next, if $a^2 + 5b^2 = 5p$, then by letting $a = 5a_1$ we have $b^2 + 5a_1^2 = p$.

Final remarks Needles to say the Euclidean algorithm produces some surprising, nice algorithms for calculating a, b such that $p = a^2 + kb^2$ for given primes p. As noted by Stan Wagon in [7], the case $k = 1$ is even more striking as $a = r_{k+1}$ the first remainder whose square is less than p and $b = r_{k+2}$.

It is possible that this approach can lead to an efficient algorithm for finding this representation for any integer k as we can efficiently find $\sqrt{-k} \bmod p$.

Bibliography

[1] Fermat's theorem on sums of two squares, Wikipedia.

[2] Don Zagier, A One-Sentence Proof That Every Prime Is a Sum of Two Squares, The American Mathematical Monthly, Vol. 97, No. 2 (Feb., 1990), pp. 144

[3] Matthew Baker, Algebraic Number Theory free lecture notes.,

[4] David A.Cox Primes of the form $x^2 + ny^2$.

[5] `http://www.sagemath.org/`

[6] `https://en.wikipedia.org/wiki/Tonelli%E2%80%93Shanks_algorithm`

[7] Stan Wagon, The Euclidean Algorithm Strikes Again,T he American Mathematical Monthly, Vol. 97, No. 2 (Feb., 1990), pp. 125-129.

2.3 Consecutive integers of the form $a^2 + 2b^2$

Le Tien Nam

Abstract

There exist infinitely many strings of 5 consecutive integers $n, n+1, ..., n+4$ such that each of them can be written as $a^2 + 2b^2$, $(a, b \in \mathbb{Z}^+)$.

2.3.1 Introduction

[by Moshe Rosenfeld] A "religious" belief among number therorists is:

> If there is no simple reason why a given pattern of primes should not occur, then it should occur infinitely often, with an asymptotically predictable frequency.

Does this belief apply to other sequences of integers? In this section we will investigate the sequences $S(k) = \{a^2 + kb^2 \mid a, k, b \in \mathbb{N}\}$.

Definition 1 *A sequence of consecutive integers is called a* ***run****.*

For example, a run of length 5 in $S(2)$ is:

$$18 \cdot 44^2 = 34848 = (4 \cdot 44)^2 + 2 \cdot 44^2$$
$$18 \cdot 44^2 + 1 = 34849 = 1^2 + 2 \cdot (3 \cdot 44)^2$$
$$18 \cdot 44^2 + 2 = 34850 = 180^2 + 2 \cdot 35^2$$
$$18 \cdot 44^2 + 3 = 34851 = 95^2 + 2 \cdot 36^2$$
$$18 \cdot 44^2 + 4 = 34852 = 2^2 + 2 \cdot (3 \cdot 44)^2.$$

It is a simple exercise to show that there are no four consecutive integers of the form $a^2 + b^2$ (in $S(1)$) and it is not too difficult to show that $S(1)$ contains infinitely many runs of length three.
I first proposed the problem in the title of this section to Erick Wong in 1992 when I was visiting Simon Fraser University in Canada. Erick solved it. His solution was very similar to Nam's: start with the 5-runs $18m^2, 18m^2+1, 18m^2+2, 18m^2+3, 18m^2+4$ and prove that for infinitely many integers m, $18m^2 + 2$ and $18m^2 + 3$ can be represented as $a^2 + 2b^2$. Except for this similar start, the proofs went on different tangents.

Erick proceeded to obtain a Ph.D. (2012) from the University of British Columbia in Vancouver, Canada. His dissertation was in number theory. It includes many results, including this result and a much deeper investigation of runs and other structures in integers of the form $a^2 + rb^2$.

In general, the sequence of integers of the form $a^2 + rb^2$ for a fixed r can contain runs of length $\leqslant 5$. When $r = 2 \bmod 8$ it can have runs of length 5. Can we always find infinitely many runs of length 5?
The answer is most likely yes.

2.3.2 Propositions

Proposition 2.41 *There exist infinitely many strings of 5 consecutive integers* $n, n+1, ..., n+4 \in S(2)$. ∎

1. $n = 18k^2 = (4k)^2 + 2.k^2$
2. $n + 1 = 18k^2 + 1 = 1^2 + 2.(3k)^2$
3. $n^2 + 4 = 18k^2 + 4 = 2^2 + 2.(3k)^2$.

Thus, we can prove the proposition by showing that for infinitely many integers k $n + 2$ and $n + 3$ have the form $a^2 + 2b^2$.

Let us consider two positive integral sequences $\{a_n\}, \{b_n\}$ such that:

$$\begin{cases} a_1 = 40, b_1 = 23 \\ a_{n+1} = 1351a_n + 2340b_n \\ b_{n+1} = 780a_n + 1351b_n \end{cases}$$

We will prove by induction two lemmas:

Lemma 2.42 $a_n^2 - 3b_n^2 = 13, \ \forall n \in \mathbb{Z}^+$. ∎

PROOF The lemma is correct for $n = 1$. Assume that it is correct for n; this means that $a_n^2 - 3b_n^2 = 13$. Then:

$$a_{n+1}^2 - 3b_{n+1}^2 = (1351^2 - 3.780^2)(a_n^2 - 3b_n^2) = 13 \quad \text{(by induction)}.$$

Hence, $a_n^2 - 3b_n^2 = 13, \ \forall n \in \mathbb{Z}^+$. ∎

Lemma 2.43 $a_n = 4 \bmod 18$ *and* $b_n = 5 \bmod 6 \ \forall n \in \mathbb{Z}^+$. ∎

PROOF The lemma is correct for $n = 1$. Assume that it is correct for n; this means that:

$$a_n = 4 \bmod 18, b_n = 5 \bmod 6.$$

Then:

$$\begin{cases} a_{n+1} = 1351a_n + 2340b_n = a_n = 4 \bmod 18 \\ b_{n+1} = 780a_n + 1351b_n = b_n = 5 \bmod 6 \end{cases}$$

Therefore, by induction, $a_n = 4 \bmod 18$ and $b_n = 5 \bmod 6 \ \forall n \in \mathbb{Z}^+$. ∎

Based on the two sequences above, we consider 5 other sequences:$\{x_n\}, \{y_n\}, \{z_n\}$, $\{t_n\}, \{k_n\}$:

$$x_n = \frac{a_n - 4}{9},\ \ y_n = 2x_n + 1,\ \ z_n = \frac{b_n + 4}{3},\ \ t_n = 2z_n - 3,\ \ k_n = \frac{9x_n^2 + 8x_n}{4}.$$

For example,

$$n = 1, \quad (a_1, b_1, x_1, y_1, z_1, t_1, k_1) = (40, 23, 4, 9, 9, 15, 44).$$

By lemma 2, it is easy to check that all sequences are integral sequence. Besides, by lemma 1, we have:

$$\begin{aligned} & 13 = a_n^2 - 3b_n^2 = (9x_n) + 4^2 - 3(z_n - 4)^2 \\ \Rightarrow\ & 9x_n^2 + 8x_n = 3z_n^2 - 8z_n + 5 \\ \Rightarrow\ & k_n = \frac{9x_n^2 + 8x_n}{4} = \frac{3z_n^2 - 8z_n + 5}{4}. \end{aligned}$$

Thus, we have:

$$\begin{aligned} 18k_n^2 + 2 &= 18k_n^2 - 4k_n + (9x_n^2 + 8x_n + 2) \\ &= 18k_n^2 + 4k_n(2x_n - y_n) + x_n^2 + y_n^2 \quad (\text{because } y_n = 2x_n + 1) \\ &= (4k_n + x_n)^2 + 2(k_n - y_n)^2. \qquad (2.3.1) \\ 18k_n^2 + 3 &= 18k_n^2 - 12k_n + (9z_n^2 - 24z_n + 18) \\ &= 18k_n - 4k_n(2z_n - t_n) + z_n^2 + t_n^2 \quad (\text{because } t_n = 2z_n - 3) \\ &= (4k_n - z_n)^2 + 2(k_n + t_n)^2. \qquad (2.3.2) \end{aligned}$$

From $(1), (2)$, we can conclude that $18k_n^2 + 2$ and $18k_n^2 + 3$ have the form $a^2 + 2b^2$. This means that the string $18k_n^2, 18k_n^2 + 1, ..., 18k_n^2 + 4 \in S(2)$.

Because $\{a_n\}$ is an increasing sequence of positive integers, so are $\{x_n\}$ and $\{k_n\}$. This means that there are infinitely many integers k_n for which $18k_n^2, 18k_n^2 + 1, ..., 18k_n^2 + 4 \in S(2)$. This completes the proof.

Proposition 2.44 *There does not exist a strings of 6 consecutive integers $n, n+1, ..., n+5$ such that each of them can be written as $a^2 + 2b^2$, $(a, b \in \mathbb{Z}^+)$.* ■

PROOF Because

$$\begin{cases} a^2 = 0; 1; 3; 4 \bmod 6 \\ 2b^2 = 0; 2 \bmod 6 \end{cases} \quad \Rightarrow a^2 + 2b^2 \neq 5 \bmod 6.$$

However, in a strings of 6 consecutive integers, there does always exist an integer $k \equiv 5 \bmod 6$. ■

2.4 Relatively prime solutions of the equation $a^2 + ab + b^2 = c^2$.

Nguyen Tho Tung, Le Tien Nam

Abstract

In this article we will show 2 different proofs for the fact that there exist positive, relatively prime integers a, b such that:

$$a^2 + ab + b^2 = 7^{2n}. \tag{2.4.1}$$

2.4.1 Introduction

While this is a number theoretical problem it has a geometric motivation. It is a tool for constructing large sets of points in $\mathbb{R}^2$, no three on a line such that the distance between any two points is an integer. Note that if a, b, c are the lengths of the sides of a triangle ΔABC then if $a^2 + ab + b^2 = c^2$ then $\angle ACB = \frac{\pi}{3}$. This allows us to rotate triangles about their center and construct large sets of points on a circle such that all distances among them are integers.We shall see how to use this result in our article: *"Constructing integer distance graphs"*.
The equation

$$a^2 + ab + b^2 = c^2 \tag{2.4.2}$$

is elementary, any high-school student can understand it. As such, it merits an elementary proof. Nam's proof is completely elementary, while Tùng's proof is *almost* elementary. He obtains a recurrence relation and shows how it is derived using the integral domain $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ where $\omega = \frac{1+\sqrt{-3}}{2}$.

2.4.2 The first proof - by Nguyen Tho Tung

We use Algebraic Number Theory to solve this problem.

Proposition 2.45 *For each positive integer n, there exist two positive, relatively prime integers a, b such that*

$$a^2 + ab + b^2 = 7^n. \tag{2.4.3}$$

■

PROOF Consider the Integral Domain $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ where $\omega = \frac{1+\sqrt{-3}}{2}$.

This Integral Domain is a Euclidean Domain with norm given by:

$$N(a+b\omega) = (a+b\omega)\overline{(a+b\omega)} = a^2+ab+b^2.^{12}$$

We first note that $N(2+\omega) = 7$ and hence $N((2+\omega)^n) = 7^n$. Our goal is to show that for all $n \in \mathbb{N}$ we can find positive integers a_n, b_n such that:

$$a_n + b_n\omega = (2+\omega)^n.$$

Note that this imples that:

$$N(a_n+b_n\omega) = a_n^2 + a_nb_n + b_n^2 = N((2+\omega)^n)) = 7^n$$

We have:

$$a_{n+1} + b_{n+1}\omega = (a_n+b_n\omega)(2+\omega) = (2a_n - b_n) + (a_n+3b_n)\omega.$$

here we use the fact that $\omega^2 = \omega - 1$. These equalities imply that:

$$\begin{cases} a_{n+1} = 2a_n - b_n \\ b_{n+1} = a_n + 3b_n. \end{cases}$$

with initial conditions: $a_0 = 1, a_1 = 2, b_0 = 0, b_1 = 1$.

The above relations give us:

$$a_{n+2} = 2a_{n+1} - b_{n+1} = 2a_{n+1} - (a_n+3b_n) = 2a_{n+1} - a_n - 3(2a_n - a_{n+1}) = 5a_{n+1} - 7a_n.$$

Similarly we also have

$$b_{n+2} = 5b_{n+1} - 7b_n.$$

Taking the sequence modulo 7 we have

$$a_{n+1} \equiv 5a_n \bmod 7, \forall n \geqslant 1.$$

As $a_1 = 2$, from the above relation, we can conclude that $7 \nmid a_n$ for all n. In addition, we have

$$a_n^2 + a_nb_n + b_n^2 = 7^n.$$

Therefore, a_n and b_n are relatively prime. Otherwise, 7 would be a divisor of a_n.

It remains to show that we can always find positive integers a_n, b_n. In case both are negative then $|a_n|^2 + |a_n||b_n| + |b_n|^2 = 7^n$. If one is negative and the other is positive, since

[12] $$(a+b\omega)\overline{(a+b\omega)} = (\frac{2a+b+b\sqrt{-3}}{2})(\frac{2a+b-b\sqrt{-3}}{2}) = a^2+ab+b^2$$

they are relatively prime we may assume without loss of generality that $b_n > |a_n|$. It is now easy to check that:

$$(b_n - |a_n|)^2 + |a_n|(b_n - |a_n|) + |a_n|^2 = b_n^2 + a_n b_n + a_n^2 = 7^n$$

so we obtain the positive solution $(b'_n, a'_n) = (b_n - |a_n|, |a_n|)$. ■

We will illustrate some numerical data. Let us denote by a_n, b_n the integer solution of (1) defined above and (A_n, B_n) the positive pair associated with (a_n, b_n).

n	a_n	b_n	A_n	B_n
0	1	0	1	0
1	2	1	2	1
2	3	5	3	5
3	1	18	1	18
4	-16	55	39	16
5	-87	149	62	87
6	-323	360	37	323

Corollary 2.46 *The equation $a^2 + ab + b^2 = 7^{2n}$ has at least n distinct positive solutions (a, b).* ■

PROOF •

- $3^2 + 3 + 5^2 = 7^2$.
- Assume by induction that $a^2 + ab + b^2 = 7^{2n}$ has n disitnct solutions $\{(a_i, b_i), i = 1, \ldots, n\}$.
- Then $\{(7a_i, 7b_i)\}$ plus the relatively prime pair (a, b) that exists by proposition 1, give us $n + 1$ positive solutions to $a^2 + ab + b^2 = 7^{2(n+1)}$. ■

Remark 1 *:*

1. *The proof also holds for all prime p such that $p \equiv 1 \bmod 6$.*
2. *The negative solution can also be useful in constructing sets in the plane with mutual integral distances. Note that if $a^2 - ab + b^2 = c^2$ then a, b, c are te sides of triangle with edge lengths a, b, c and angle $\frac{\pi}{6}$.* ■

2.4.3 Second proof - by Le Tien Nam

This proof is elementary, easily understood by high school students.

We restate the proposition and prove it by induction.

Conclusion 2.47 *The equation $a^2 + b^2 + ab = 7^n$ has at least one positive integer solution (a, b) such that* $\gcd(a, 7) = 1$ ■

PROOF :

It is easy to see that for $n = 1, 2,\ (1, 2)$ *and* $(3, 5)$ solve the equation.

Assume that the claim is true for n, that is there are integers a, b satisfying the claim. We shall prove that the claim also holds for $n + 1$.

Without loss of generality, we can assume that $a < b$. Consider the following three pairs of numbers:

1. $(c_1, d_1) = (2b - a, 3a + b)$

$$\begin{aligned} \Rightarrow c_1^2 + d_1^2 + c_1 d_1 &= (2b - a)^2 + (3a + b)^2 + (2b - a)(3a + b) \\ &= a^2 + 4b^2 - 4ab + 9a^2 + b^2 + 6ab - 3a^2 + 2b^2 + 5ab \\ &= 7(a^2 + b^2 + ab) \\ &= 7^{n+1}. \end{aligned}$$

2. $(c_2, d_2) = (b - 2a, 3a + 2b)$

$$\begin{aligned} \Rightarrow c_2^2 + d_2^2 + c_2 d_2 &= (b - 2a)^2 + (3a + 2b)^2 + (b - 2a)(3a + 2b) \\ &= 7(a^2 + b^2 + ab) \\ &= 7^{n+1}. \end{aligned}$$

3. $(c_3, d_3) = (2a - b, a + 3b)$

$$\begin{aligned} \Rightarrow c_3^2 + d_3^2 + c_3 d_3 &= (2a - b)^2 + (a + 3b)^2 + (2a - b)(a + 3b) \\ &= 7(a^2 + b^2 + ab) \\ &= 7^{n+1}. \end{aligned}$$

By the assumptions we have : $c_1, d_1, d_2, d_3 > 0$. Thus:

1. If $\gcd(c_1, 7) = 1 \Rightarrow (c_1, d_1)$ satisfies the claim for $n + 1$.
2. If $\gcd(c_1, 7) \neq 1 \Rightarrow 7 | c_1 \Rightarrow 7 | 2b - a$
   Note that if $7 | 2a - b$ then $7 | 2b - a + 4a - 2b = 3a$ contradicting the assumption that $gcd(a, 7) = 1$, so $\gcd(2a - b, 7) = 1$

- If $2a - b < 0$, then (c_2, d_2) satisfies the claim for $n + 1$.
- If $2a - b > 0$, then (c_3, d_3) satisfies the claim for $n + 1$.

Hence, the claim is true for $n + 1$ and by the principle of mathematical induction the claim is true for every positive integer n. ∎

By a similar argument we can also prove the following generalization:

Proposition 2.48 *For every r for which there exists, a pair of relatively prime positive integers (a_0, b_0) such that $r = a_0^2 + b_0^2 + a_0 b_0$, the equation:*

$$a^2 + b^2 + ab = r^n \tag{2.4.4}$$

has at least one positive integer solution (a_n, b_n) such that $\gcd(a_n, b_n) = 1$.
It follows that for each positive integer n the equation 2.4.4 has at least n different pairs of positive integers that solve it. ∎

These results will help us construct sets of points in the plane, no three on a line such that the distance between any pair of points is an integer. We call such sets of points **integral sets**.

3 Geometry

3.1 Non collinear integral sets.

Tran Nhat Tan, Le Tien Nam

Abstract

A set of points in the Euclidean plane $\mathbb{R}^2$ is an **integral set** if the distance between any two points in the set is an integer.
In this article we give two constructions of arbitrarily large integral sets, no three on a line. One construction is trigonometry based and the other is based on elementary number theory. We also prove that among all sets of n points in $\mathbb{R}^2$ these constructions produce sets that maximize the number of odd distances among the points.

3.1.1 Introduction

Comment 3.1 M. Rosenfeld proved (see [3]) that it is not possible to find 4 points in $\mathbb{R}^2$ such that all six distances among them are odd integers. In other words, if we construct a graph whose vertices are points in $\mathbb{R}^2$ and connect two vertices by an edge, this graph does not contain K_4 as a subgraph. By Turàn's theorem, the graph $K_{n,n,n}$ maximizes the number of edges among all graphs of order $3n$.

By constructing sets of points in which the odd distances realize the graph $K_{n,n,n}$ they maximize the number of odd distances among any sets of $3n$ points in $\mathbb{R}^2$. By deleting one or two points, we obtain sets that maximize the number of odd distances among any set of points in $\mathbb{R}^2$.

Are there infinite integral sets of points in $\mathbb{R}^2$? The answer is yes! the set $\{(\pm n, 0) \mid n \in \mathbb{N}\}$ is an infinite set of integral points. Surprisingly, this is essentially the only set. Paul Erdős and Norman Anning proved in 1945 that every infinite integral set in $\mathbb{R}^2$ is collinear (see [1]).

In a lecture at Vietnam National University of Science in Hanoi 2011, Professor Moshe Rosenfeld posed the following problem:

Question 3.2 *Construct 6 points in the plane $\mathbb{R}^2$, no three on a line, such that all distances among them are integers.* ■

For $n = 4$ this is easy. The 4 points $M, N, P, Q \in \mathbb{R}^2$ with coordinates $M(4,0), N(-4,0), P(0,3), Q(0,-$ form an integral set. However, Professor Rosenfeld showed us another approach. In a triangle with sides a, b, c such that $a^2 + b^2 + ab = c^2$ the angle between sides a and b is

$\widehat{C} = 120^\circ$. This follows from the law of cosine,

$$\cos C = \frac{a^2 + b^2 - c^2}{2ab} = \frac{-ab}{2ab} = -\frac{1}{2} \quad \text{or equivalently} \quad \widehat{C} = 120^\circ.$$

Next, we draw an equilateral triangle ABC with side 7, and its circumscribed circle centered at O. Let D be a point such that $DA = 3, DB = 5$ (see figure 6).

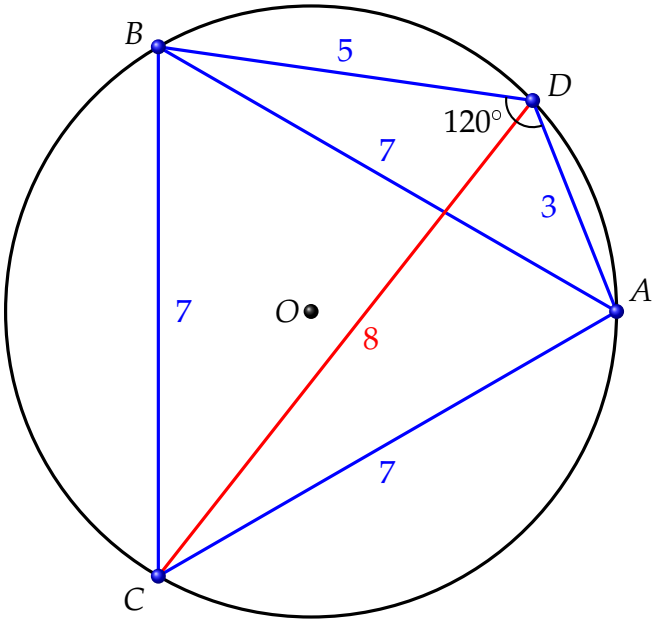


Figure 6: Rosenfeld's approach to solve Question 3.2.

Since $3^2 + 5^2 + 3.5 = 7^2$, $DA^2 + DB^2 + DA.DB = AB^2 \Rightarrow \widehat{ADB} = 120^\circ$, so D is also on the circle. Applying Ptolemy's theorem to the cyclic quadrilateral $ADBC$ we obtain:

$$AB \cdot DC = AD \cdot BC + DB \cdot AC \quad \text{i.e.} \quad 7 \cdot DC = 3 \cdot 7 + 5 \cdot 7 \quad \text{i.e.} \quad DC = 8.$$

Thus $\{A, B, C, D\}$ is an integral set. By adding the points E and F with distances $AF = CE = 5$; $FC = EB = 3$ as shown in Figure 7 we obtain an integral set of six points on the circle.

$AB = BC = CA = 7 \Rightarrow OA = OD = 7/\sqrt{3}$, additionally $DA = 3$ therefore

$$\sin\frac{\beta}{2} = \frac{3}{2OA} = \frac{3\sqrt{3}}{14} \Longrightarrow \cos\beta = 1 - 2\sin^2\frac{\beta}{2} = \frac{71}{98}.$$

It follows that,

$$0 < \beta < \frac{\pi}{2} \quad \text{and} \quad \beta = \arccos\frac{71}{98}. \tag{3.1.1}$$

This particular angle is a key to our construction. We shall show that we can rotate $n-1$ times an equilateral triangle with side 7^{n-1} about its center, by an angle β, to obtain an integral set of $3n$ points on the circle.

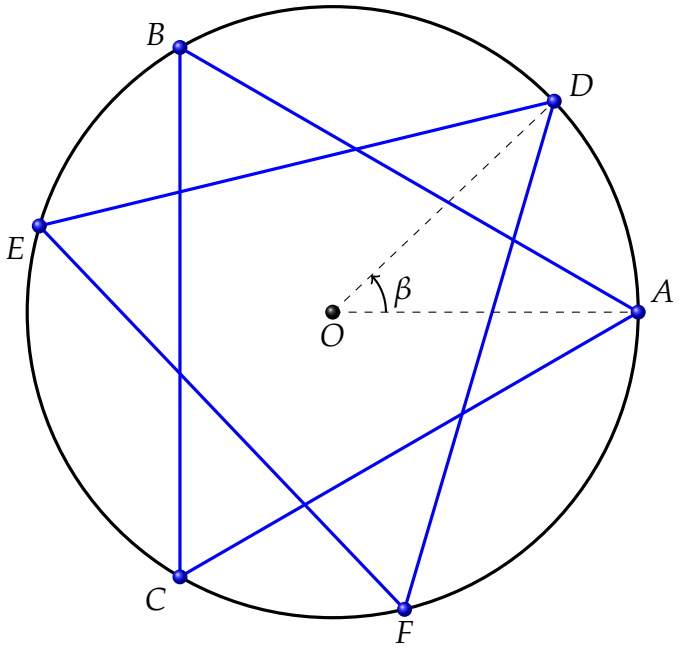


Figure 7: An integral set with 6 points on a circle.

This construction was originated in 1993 by H. Harborth, A. Kemnitz and M. Moller (see [2]). Later, in 1996, L. Piepemeyer used this construction to produce an integral set of n points in $\mathbb{R}^2$ that maximizes the number of odd distances among any set of n points in the plane.

We present here an elementary proof of this construction which uses elementary complex numbers and recurrence relations which should make it accessible to high school students.

3.1.2 Proof of the main results

We first need to set-up some preparations. Let $S = \{A_p, B_p, C_p\}, p = 0, \ldots, n-1$ be a set of $3n$ points on a circle $\mathbb{C}$ with radius $R = 7^{n-1}/\sqrt{3}$, centered at $(0,0)$, A_0 located on the x-axis ($A_0 = (R, 0)$) (see Figure 8).

Let $\beta = \arccos \frac{71}{98}$ and let the $3n$ points have coordinates:

$$A_p = (R\cos p\beta, R\sin p\beta)\,, \tag{3.1.2}$$

$$B_p = \left(R\cos\left(p\beta + \frac{2\pi}{3}\right), R\sin\left(p\beta + \frac{2\pi}{3}\right)\right), \tag{3.1.3}$$

$$C_p = \left(R\cos\left(p\beta + \frac{4\pi}{3}\right), R\sin\left(p\beta + \frac{4\pi}{3}\right)\right). \tag{3.1.4}$$

We first note that the triangles $\Delta A_p B_p C_p$ are equilateral with side 7^n and each such triangle is obtained by rotating $\Delta A_0 B_0 C_0$ about the origin by an angle $p \cdot \beta$.

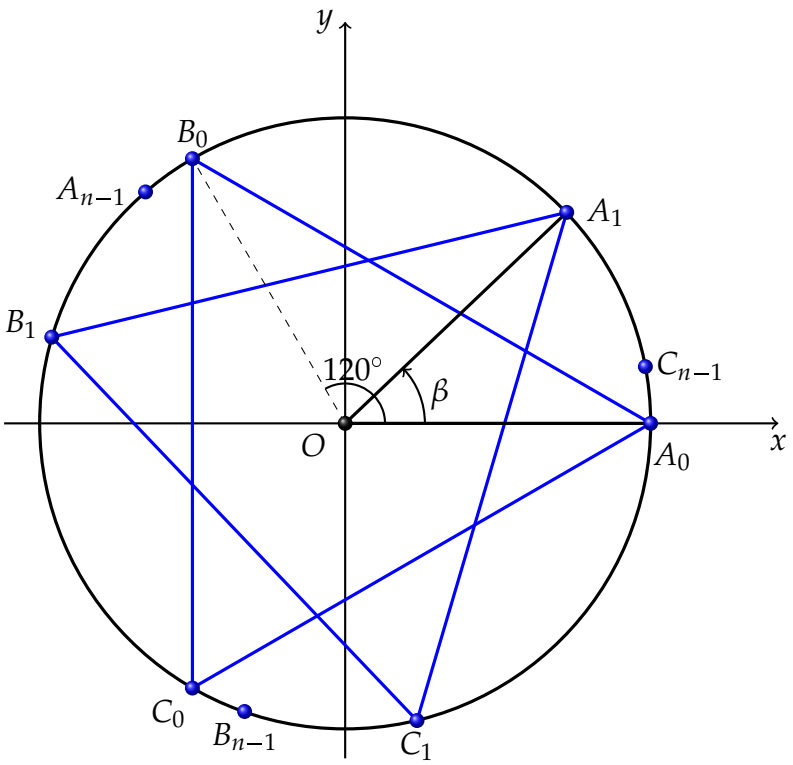


Figure 8: An integral con-cyclic set of $3n$ points.

We have 6 types of distances among the above $3n$ points

$$A_kB_l, C_kA_l, B_kC_l, A_kA_l, C_kC_l, B_kB_l, \quad k, l = 0, 1, \ldots, n-1.$$

We want to prove that all of them are integers. We first note that it is enough to prove that:

$$A_kA_l, A_kB_l \in \mathbb{Z}, \quad k, l = 0, 1, \ldots, n-1.$$

Indeed:

1. $A_lB_l = B_lC_l = C_lA_l = 7^{n-1}$.
2. $A_kA_l = C_kC_l = B_kB_l$ as these segments come from a counter clockwise rotation about the origin by $|k-l| \cdot \beta$.
3. $A_kB_l = B_kC_l$ as these segments come from a counter clockwise rotation about the origin by $|k-l| \cdot 2\pi/3$.
4. $A_kB_l = C_kA_l$ as these segments come from a counter clockwise rotation about the origin by $|k-l| \cdot 4\pi/3$.

$$
\begin{aligned}
A_kA_l &= R\sqrt{(\cos k\beta - \cos l\beta)^2 + (\sin k\beta - \sin l\beta)^2} \\
&= R\sqrt{2 - 2\cos k\beta\cos l\beta - 2\sin k\beta\sin l\beta} \\
&= R\sqrt{2 - 2\cos(k-l)\beta} = 2R\left|\sin\frac{(k-l)\beta}{2}\right| \\
&= \pm 2R\sin\frac{m\beta}{2}, \quad m = |k-l| = 0, 1, \ldots, n-1.
\end{aligned}
$$

Similarly,

$$
\begin{aligned}
A_kB_l &= R\sqrt{\left(\cos k\beta - \cos\left(l\beta + \frac{2\pi}{3}\right)\right)^2 + \left(\sin k\beta - \sin\left(l\beta + \frac{2\pi}{3}\right)\right)^2} \\
&= R\sqrt{2 - 2\cos k\beta\cos\left(l\beta + \frac{2\pi}{3}\right) - 2\sin k\beta\sin\left(l\beta + \frac{2\pi}{3}\right)} \\
&= R\sqrt{2 - 2\cos\left((k-l)\beta - \frac{2\pi}{3}\right)} = 2R\left|\sin\left(\frac{(k-l)\beta}{2} - \frac{\pi}{3}\right)\right| \\
&= \pm 2R\sin\left(\frac{m\beta}{2} \pm \frac{\pi}{3}\right), \quad m = |k-l| = 0, 1, \ldots, n-1.
\end{aligned}
$$

Note that $R = 7^{n-1}/\sqrt{3}$ so in order to prove that $A_kA_l, A_kB_l \in \mathbb{Z}$ it suffices to prove that

$$
2\cdot\frac{7^{n-1}}{\sqrt{3}}\sin\frac{m\beta}{2} \in \mathbb{Z} \tag{3.1.5}
$$

$$
2\cdot\frac{7^{n-1}}{\sqrt{3}}\sin\left(\frac{r\beta}{2} \pm \frac{\pi}{3}\right) \in \mathbb{Z} \tag{3.1.6}
$$

$$
m, r = 0, 1, \ldots, n-1.
$$

The following lemma is a key step for proving our results.

Lemma 3.3 *For all $s \in \mathbb{Z}, s \geqslant 0$ the following expressions are integers:*

$$
\begin{aligned}
X_s &= 2\cdot\frac{7^s}{\sqrt{3}}\sin\frac{s\beta}{2} \\
Y_s &= 2\cdot\frac{7^s}{\sqrt{3}}\sin\left(\frac{s\beta}{2} + \frac{\pi}{3}\right) \\
Z_s &= 2\cdot\frac{7^s}{\sqrt{3}}\sin\left(\frac{s\beta}{2} - \frac{\pi}{3}\right).
\end{aligned}
$$

■

Note that Lemma 4.6 implies (3.1.5) and (3.1.6).

PROOF (Proof of Lemma 1) Recall that β is an acute angle such that $\cos\beta = 71/98$. We first show that $X_s \in \mathbb{Z}$. Let

$$
X_s' = 2\cdot\frac{7^s}{\sqrt{3}}\cos\frac{s\beta}{2}.
$$

$$T_s = X'_s + iX_s = \frac{2 \cdot 7^s}{\sqrt{3}} \left(\cos \frac{s\beta}{2} + i \sin \frac{s\beta}{2} \right) = \frac{2 \cdot 7^s}{\sqrt{3}} \exp \left(i \frac{s\beta}{2} \right) [13]. \tag{3.1.7}$$

Note that X_s and X'_s are the imaginary and real part of the complex number T_s. Besides,

$$\sin \frac{\beta}{2} = \sqrt{\frac{1 - \cos \beta}{2}} = \frac{3\sqrt{3}}{14}, \quad \cos \frac{\beta}{2} = \sqrt{\frac{1 + \cos \beta}{2}} = \frac{13}{14}.$$

Hence:

$$T_s = 2 \cdot \frac{7^s}{\sqrt{3}} \left[\exp \left(i \frac{\beta}{2} \right) \right]^s = 2 \cdot \frac{7^s}{\sqrt{3}} \left(\frac{13}{14} + \frac{3\sqrt{3}}{14} i \right)^s = \frac{2}{\sqrt{3}} \left(\frac{13}{2} + \frac{3\sqrt{3}}{2} i \right)^s.$$

$$T_{s+1} = \frac{2}{\sqrt{3}} \left(\frac{13}{2} + \frac{3\sqrt{3}}{2} i \right)^{s+1} = \left(\frac{13}{2} + \frac{3\sqrt{3}}{2} i \right) T_s = \left(\frac{13}{2} + \frac{3\sqrt{3}}{2} i \right) (X'_s + iX_s)$$
$$X'_{s+1} + iX_{s+1} = \left(\frac{13}{2} X'_s - \frac{3\sqrt{3}}{2} X_s \right) + i \left(\frac{3\sqrt{3}}{2} X'_s + \frac{13}{2} X_s \right)$$

Comparing the real and imaginary parts we obtain for $s \in \mathbb{Z}, s \geqslant 0$,

$$\begin{aligned} X'_{s+1} &= \frac{13}{2} X'_s - \frac{3\sqrt{3}}{2} X_s \\ X_{s+1} &= \frac{3\sqrt{3}}{2} X'_s + \frac{13}{2} X_s. \end{aligned} \tag{3.1.8}$$

Therefore,

$$\begin{aligned} X_{s+2} &= \frac{3\sqrt{3}}{2} X'_{s+1} + \frac{13}{2} X_{s+1} = \frac{3\sqrt{3}}{2} \left(\frac{13}{2} X'_s - \frac{3\sqrt{3}}{2} X_s \right) + \frac{13}{2} \left(\frac{3\sqrt{3}}{2} X'_s + \frac{13}{2} X_s \right) \\ &= 13 \cdot \frac{3\sqrt{3}}{2} X'_s + \frac{71}{2} X_s = 13 \left(\frac{3\sqrt{3}}{2} X'_s + \frac{13}{2} X_s \right) - 49 X_s = 13 X_{s+1} - 49 X_s. \end{aligned} \tag{3.1.9}$$

In addition,

$$\begin{aligned} T_0 &= \frac{2}{\sqrt{3}} \left(\frac{13}{2} + \frac{3\sqrt{3}}{2} i \right)^0 = \frac{2}{\sqrt{3}}, \\ T_1 &= \frac{2}{\sqrt{3}} \left(\frac{13}{2} + \frac{3\sqrt{3}}{2} i \right) = \frac{13}{\sqrt{3}} + 3i. \end{aligned} \tag{3.1.10}$$

It follows that, $X_0 = 0$ and $X_1 = 3$. This condition and (3.1.9) give us the linear recurrence relation:

$$\begin{aligned} &X_0 = 0, X_1 = 3, \\ &X_{s+2} = 13 X_{s+1} - 49 X_s, \ \forall s \in \mathbb{Z}^+ \end{aligned} \tag{3.1.11}$$

which is a recursion relation for the sequence $\{X_s\}$, proving that $X_s \in \mathbb{Z}$ as claimed.

[13] ($i = \sqrt{-1}$.)

Next, we show that $Y_s, Z_s \in \mathbb{Z}\ \forall s \in \mathbb{Z}^+$. We observe that

$$Y_s = \frac{2 \cdot 7^s}{\sqrt{3}} \sin\left(\frac{s\beta}{2} + \frac{\pi}{3}\right) = \frac{2 \cdot 7^s}{\sqrt{3}} \sin\frac{s\beta}{2}.\frac{1}{2} + \frac{2 \cdot 7^s}{\sqrt{3}} \cos\frac{s\beta}{2}.\frac{\sqrt{3}}{2} = \frac{1}{2}X_s + \frac{\sqrt{3}}{2}X'_s. \quad (3.1.12)$$

From this point on, in order to find a recurrence relation for $\{Y_s\}$ we will find a recurrence relation for $\{X'_s\}$.

From (3.1.8) we get:

$$\begin{aligned} X'_{s+2} &= \frac{13}{2}X'_{s+1} - \frac{3\sqrt{3}}{2}A_{s+1} = \frac{13}{2}\left(\frac{13}{2}X'_s - \frac{3\sqrt{3}}{2}X_s\right) - \frac{3\sqrt{3}}{2}\left(\frac{3\sqrt{3}}{2}X'_s + \frac{13}{2}X_s\right) \\ &= \frac{71}{2}X'_s - 13.\frac{3\sqrt{3}}{2}X_s = 13\left(\frac{13}{2}X'_s - \frac{3\sqrt{3}}{2}X_s\right) - 49X_s \\ X'_{s+2} &= 13X'_{s+1} - 49X'_s. \end{aligned}$$

Furthermore, from (3.1.10) we have $X'_0 = 2/\sqrt{3}$ and $X'_1 = 13/\sqrt{3}$. They produce a recursion relation of sequence $\{X'_s\}$ as follows:

$$\begin{aligned} &X'_0 = 2/\sqrt{3}, X'_1 = 13/\sqrt{3}, \\ &X'_{s+2} = 13X'_{s+1} - 49X'_s, \quad s \in \mathbb{Z}, s \geqslant 0. \end{aligned} \quad (3.1.13)$$

Surprisingly, two sequences $\{X_s\}$ and $\{X'_s\}$ have the same recurrence relation. They only differ in their initial values. As a consequence, we immediately find that:

$$\begin{aligned} &Y_0 = 1, Y_1 = 8, \\ &Y_{s+2} = 13Y_{s+1} - 49Y_s, \quad s \in \mathbb{Z}, s \geqslant 0. \end{aligned} \quad (3.1.14)$$

Thus $Y_s \in \mathbb{Z}$.

Similarly, we can use the same process to obtain a recurrence relation for the sequence $\{Z_s\}$. As in (3.1.12) we get:

$$Z_s = 2 \cdot \frac{7^s}{\sqrt{3}} \sin\left(\frac{s\beta}{2} - \frac{\pi}{3}\right) = \frac{1}{2}X_s - \frac{\sqrt{3}}{2}X'_s.$$

Once again, the sequence $\{Z_s\}$ has the same recurrence relation as the sequences $\{Y_s\}$, $\{X_s\}$ but differ in its initial values.

$$\begin{aligned} &Z_0 = -1, Z_1 = -5, \\ &Z_{s+2} = 13Z_{s+1} - 49Z_s, \quad s \in \mathbb{Z}, s \geqslant 0. \end{aligned} \quad (3.1.15)$$

Lemma 4.6 is therefore proved. ∎

So the set $\{A_p, B_p, C_p\}$ is an integral set. But are all points distinct? To prove it, it is enough to show that all distances are positive integers.

This can be easily proved by induction as follows: $X_1 = 3 \not\equiv 0 \bmod 7$. From the recurrence relation 3.1.11 it follows immediately that if $X_s \not\equiv 0 \bmod 7$ then $X_{s+1} \not\equiv 0 \bmod 7$, thus $X_s \neq 0, \forall s \geqslant 1$. The same argument applies to Y_s and Z_s.

3.1.3 Nam's proof

3.1.3.1 Preliminary Notions

First, we familiarize ourselves with some notions:

1. A *geometric graph* $G(M, D)$ is a graph whose vertices belong to a metric space M and two vertices are connected by an edge if their distance belongs to a specified set $D \subset \mathbb{R}^+$ of distances.
2. One of the most famous graphs in this category is the unit-distance graph: $G(\mathbb{R}^2, \{1\})$, (two points in the plane $\mathbb{R}^2$ are connected by an edge if their distance is 1).
3. The odd-distance graph: $G(\mathbb{R}^2, \{1, 3, 5, \ldots\})$
4. *An integral distance graph* is a geometric graph such that every pair of vertices whose distance is an integer are connected by an edge.

Therefore, constructing integral distance complete graphs such that all vertices are on a circle means constructing a configuration of points on a circle such that the distance between every pair of distinct points is a positive integer.

3.1.3.2 Some Propositions

A useful tool we shall use repeatedly is Ptomey's theorem:

Theorem 3.4 (Ptolmey's theorem) *If A, B, C, D are the vertices of a quadrilateral inscribed on a circle then:*

$$\| AB \| \cdot \| CD \| + \| BC \| \cdot \| AD \| = \| AC \| \cdot \| BD \|$$ ∎

Let $C(\frac{2p^{n-1}}{\sqrt{3}})$ be a circle of diameter $\frac{2p^{n-1}}{\sqrt{3}}$. We shall construct $3n$ points on this circle, such that all distances among them are integers. Furthermore, these points can be divided into n triples X_k, Y_k, Z_k $k = 0, 1, ...n-1$ such that:

1. $X_0Y_0Z_0$ is an equilateral triangle of side p^{n-1}.
2. X_k, Y_k, Z_k is obtained by rotating the equilateral triangle $X_{k-1}Y_{k-1}Z_{k-1}$ so that the distances $\| X_{k-1}, Z_k \| = a_k$ $\forall k \geqslant 1$ (the sequence a_k will be constructed in the next section).
3. The $3n$ points will form an *integral set* of points.

The following example demonstrates our strategy for 9 points; $k = 2$.

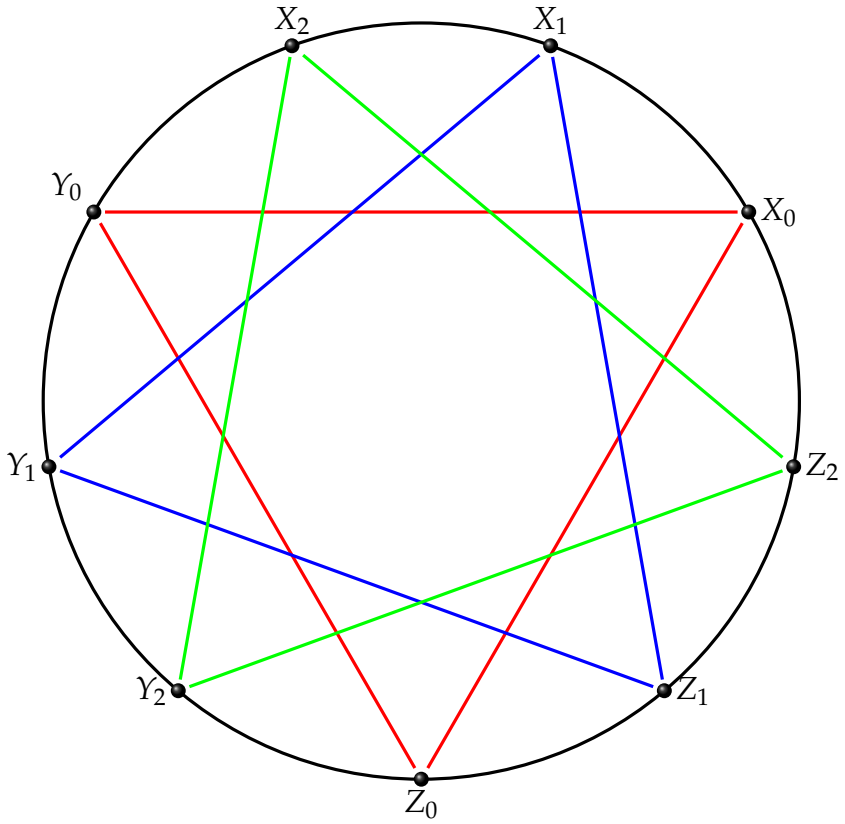


Figure 1: 9 integral points on a circle of diameter $\frac{2\cdot 7^2}{\sqrt{3}}$.

Figure 1 shows a configuration of 9 points on a circle of radius $\frac{49}{\sqrt{3}}$. It is obtained as follows: we start with an equilateral triangle $X_0Y_0Z_0$ of side 7 inscribed in a circle with diameter $\frac{14}{\sqrt{3}}$. By rotating it about its center so that $\parallel X_0X_1 \parallel = 3$ we get another triangle $X_1Y_1Z_1$. Using Ptolmey's theorem, it is not difficult to see that the distances among the six points are: $3, 5, 7, 8$. We leave the details to the reader.

We now expand the circle by 7 to obtain the equilateral triangles $X_0Y_0Z_0$ and $X_1Y_1Z_1$ with side 49 that form an integral set of six points. We add a third triangle by rotating $X_1Y_1Z_1$ so that $\parallel X_0X_2 \parallel = 39$. All other distances can be determined by applying the cosine law using the observation that for every point W on the short arc (X_0, Y_0) : $\angle X_0WY_0 = \frac{2\pi}{3}$ and Prolmey's theorem to various quadrilaterals. We shall demonstrate this for the distances among the points $\{X_0, Z_1, Y_2, Y_0\}$.

1. By the law of cosines:

$$\parallel X_0X_1 \parallel^2 + \parallel X_1Y_0 \parallel^2 + \parallel X_0X_1 \parallel \cdot \parallel X_1Y_0 \parallel = \parallel X_0Y_0 \parallel^2 \Longrightarrow \tag{3.1.16}$$
$$21^2 + \parallel X_1Y_0 \parallel^2 + 21 \cdot \parallel X_1Y_0 \parallel = 49^2 \Longrightarrow \parallel X_1Y_0 \parallel = 35.$$

2. Similarly, by rotating the second triangle so that $\parallel X_0X_2 \parallel = 39$:

$$39^2 + \parallel X_2Y_0 \parallel^2 + 39 \cdot \parallel X_2Y_0 \parallel = 49^2 \Longrightarrow \parallel Y_2Y_0 \parallel = 16.$$

3. The following distances can also be easily established:
   $\| Z_1Y_2 \| = 21,\ \| X_0Y_1 \| = \| Y_1Z_2 \| = \| Y_0Z_1 \| \| Z_0Y_2 \| = 56$

The remaining distances can be easily calculated using Ptolmey's theorem applied to quadrilaterals inscribed in the circle obtaining an integral set of 9 points as claimed.

3.1.3.3 The main result

In this section we prove that we can place n points on a circle in $\mathbb{R}^2$ such that:

1. They form an integral set.
2. The set of odd distances among them maximizes the number of odd distances among any set of n points in $\mathbb{R}^2$.

First, we recall a proposition on the existence of roots for the integer equation:

$$a^2 + ab + b^2 = c^2 \tag{3.1.17}$$

from the article *"Relatively prime solutions of the equation $a^2 + ab + b^2 = c^2$"*

Proposition 3.5 *Let p be a prime number for which there exist integers (a_1, b_1) such that $a_1^2 + b_1^2 + a_1b_1 = p^2$; then for every $k \geqslant 1$ the equation:*

$$a_k^2 + a_kb_k + b_k^2 = p^{2k} \tag{3.1.18}$$

has at least one solution (a_k, b_k) such that a_k, b_k, p are pairwise relatively prime. ■

We shall call such a pair a *prime root* of ths equation.

Proposition 3.6 *Let $(a_k, b_k), (a_{k-1}, b_{k-1})$ be prime roots of the equations:*

$$x^2 + y^2 + xy = p^{2k},\ x^2 + y^2 + xy = p^{2k-2} \text{ respectively.}$$

Then

$$p^{k-1} \mid a_kb_{k-1} - b_ka_{k-1} \ \text{ or } \ p^{k-1} \mid a_ka_{k-1} - b_kb_{k-1}$$ ■

PROOF $a_k^2 + b_k^2 + a_kb_k = p^{2k}$ and $a_{k-1}^2 + b_{k-1}^2 + a_{k-1}b_{k-1} = p^{2k-2}$.

$$\begin{aligned} &\Rightarrow (a_k^2 + b_k^2 + a_kb_k)b_{k-1}^2 = (a_{k-1}^2 + b_{k-1}^2 + a_{k-1}b_{k-1})b_k^2 \mod p^{2k-2} \\ &\Rightarrow (a_kb_{k-1} - b_ka_{k-1})(a_kb_{k-1} + b_ka_{k-1} + b_kb_{k-1}) = 0 \mod p^{2k-2} \end{aligned} \tag{3.1.19}$$

Similarly, we have:

$$\begin{aligned}
&\Rightarrow (a_k^2 + b_k^2 + a_k b_k) a_{k-1}^2 = (a_{k-1}^2 + b_{k-1}^2 + a_{k-1} b_{k-1}) b_k^2 \mod p^{2k-2} \\
&\Rightarrow (a_k a_{k-1} - b_k b_{k-1})(a_k a_{k-1} + b_k b_{k-1} + b_k a_{k-1}) = 0 \mod p^{2k-2}
\end{aligned} \tag{3.1.20}$$

Assume that neither $p^{k-1} \mid a_k b_{k-1} - b_k a_{k-1}$ nor $p^{k-1} \mid a_k a_{k-1} - b_k b_{k-1}$. From (4) and (5) we have:

$$p^{k-1} \mid a_k b_{k-1} + b_k a_{k-1} + b_k b_{k-1} \quad \text{and} \quad p^{k-1} \mid a_k a_{k-1} + b_k b_{k-1} + b_k a_{k-1}$$

$\Rightarrow p^{k-1} \mid a_k a_{k-1} - a_k b_{k-1}$. Since $GCD(a_k, p) = 1$:
$\Rightarrow p^{k-1} \mid a_{k-1} - b_{k-1}$
$\Rightarrow p^{k-1} \mid (a_{k-1} - b_{k-1})^2 = (a_{k-1}^2 + b_{k-1}^2 + a_{k-1} b_{k-1}) - 3 a_{k-1} b_{k-1}$
$\Rightarrow p^{k-1} \mid 3 a_{k-1} b_{k-1}$ (a contradiction since $GCD(a_{k-1}, p) = GCD(b_{k-1}, p) = 1$) ∎

Comment 3.7 We note that (a_k, b_k) and (b_k, a_k) are both prime roots of $x^2 + xy + y^2 = p^{2k}$. So we can always choose the prime root (a_k, b_k) so that $p^{k-1} \mid a_k b_{k-1} - b_k a_{k-1}$.

Proposition 3.8 *Let $(a_k, b_k), (a_n, b_n)$ be prime roots of the equations: $a^2 + b^2 + ab = p^{2k}$ and $a^2 + b^2 + ab = p^{2n}$, respectively . Then*

$$p^n \mid a_n b_k - b_n a_k \quad (n < k)$$ ∎

PROOF We shall prove the claim by induction on k.

For $k = 2$, the claim follows from Proposition 3.6.

Assume that for all $i < k - 1$: $\quad p^i \mid a_i b_{k-1} - b_i a_{k-1}$.

We need to prove that: $\forall i < k$: $\quad p^i \mid a_i b_k - b_i a_k$.

Assume that the claim is true for $k - 1$. Thus, $\forall i < k - 1$, we have:

$$p^i \mid a_{k-1} b_i - b_{k-1} a_i \Rightarrow a_{k-1} b_i = b_{k-1} a_i \mod p^i$$

$$p^{k-1} \mid a_k b_{k-1} - b_k a_{k-1} \text{ (Proposition 3.6)}$$

$$p^{k-1} \mid a_k b_{k-1} - b_k a_{k-1} \Rightarrow a_k b_{k-1} = b_k a_{k-1} \mod p^{k-1}$$

$$\Rightarrow a_{k-1} b_i a_k b_{k-1} = b_{k-1} a_i b_k a_{k-1} \mod p^i$$

$$\Rightarrow b_i a_k = a_i b_k \mod p^i \Rightarrow p^i \mid b_i a_k - a_i b_k$$

The last steps are justified since a_{k-1}, b_{k-1} are relatively prime to p. ∎

Proposition 3.9 *For every $k < n$:*

$$p^k \mid a_n a_k + b_n b_k + b_n a_k \ \ and \ \ p^k \mid a_n a_k + b_n b_k + a_n b_k$$ ■

PROOF By proposition 3.8: $p^k \mid a_n b_k - b_n a_k$

If $p^k \mid a_n a_k - b_n b_k$ then:

$p^k \mid a_n b_k - b_n a_k - (a_n a_k - b_n b_k) \Rightarrow p^k \mid (a_k - b_k)(a_n - b_n)$ (P-4)

If $p \mid a_n - b_n$, then $(a_n - b_n)^2 = (a_n^2 + b_n^2 + a_n b_n) - 3a_n b_n \Longrightarrow$

$p \mid 3a_n b_n$ (contradiction, a_n, b_n are relatively prime to p).

So $p \mid a_n - b_n$ and similarly $p \mid a_k - b_k \Rightarrow p \mid (a_n - b_n)(a_k - b_k)$.
contradicting P-4.

Thus: $p^k \mid a_n a_k - b_n b_k$ (P-5).

$$\begin{aligned}(a_n^2 + b_n^2 + a_n b_)a_k^2 &= (a_k^2 + b_k^2 + a_k b_k)b_n^2 \mod p^{2k} \\ \Rightarrow a_n^2 a_k^2 - b_n^2 b_k^2 + a_n b_n a_k^2 + a_k b_k b_n^2 &= 0 \mod p^{2k} \\ \Rightarrow (a_n a_k - b_n b_k)(a_n a_k + b_n b_k + b_n a_k) &= 0 \mod p^{2k}\end{aligned}$$

Since $p^k \mid a_n a_k - b_n b_k$ (P-5), we must have $p^k \mid a_n a_k + b_n b_k + b_n a_k$

Similarly, $p^k \mid a_n a_k + b_n b_k + a_n b_k$. ■

3.1.3.4 Constructing K_{3n} on a circle of diameter $\frac{2p^{n-1}}{\sqrt{3}}$

Construction:

1. Draw an equilateral triangle XYZ of side p and let C be its circumscribed circle. Its diameter is $\frac{2p}{\sqrt{3}}$.
2. Choose X_1, Y_1, Z_1 on arcs YZ, ZX, XY, respectively such that

   $$\| X_1Y \| = \| Y_1Z \| = \| Z_1X \| = a_1 \text{ and } \| X_1Z \| = \| Z_1Y \| = \| Y_1X \| = b_1$$

   where a_1 and b_1 are a prime root of $a_1^2 + b_1^2 + 2a_1b_1 = p^2$.
3. Assume we constructed the configuration $X, Y, Z, X_1, Y_1, Z_1, \ldots, X_{k-1}, Y_{k-1}, Z_{k-1}$.
4. We expand the current configuration by a factor of p and add 3 points X_k, Y_k, Z_k such that:

   $$\| X_kY_{k-1} \| = \| Y_kZ_{k-1} \| = \| Z_kX_{k-1} \| = a_k \text{ and } \| X_kZ_{k-1} \| = \| Z_kY_{k-1} \| = \| Y_kX_{k-1} \| = b_k$$

   where (a_k, b_k) is a prime root of $x^2 + xy + y^2 = p^{2k}$ and (a_k, b_k) are selected as in comment 3.7.

Conclusion 3.10 $\| X_kX_n \|, \| X_kY_n \|, \| X_kZ_n \| \in \mathbb{Z}\ \forall n < k.$ ■

PROOF $\| XX_k \| = \| YY_k = \| ZZ_k \| = a_k + b_K$ by Ptolemy's Theorem.

Applying Ptolemy's theorem to the quadrangle YX_kX_nZ, we have:

$$\| X_kX_n \| = \frac{|\| X_kZ \| \cdot \| X_nY \| - \| X_kY \| \cdot \| X_nZ \||}{\| YZ \|} = \frac{| a_nb_k - b_na_k |}{p^k} \in \mathbb{Z} \text{ (by Proposition 3)}$$

Applying Ptolemy's theorem to the quadrangle YX_kZY_n, we have:

$$\| X_kY_n \| = \frac{\| X_kZ \| \cdot \| Y_nY \| + \| X_kY \| \cdot \| Y_nZ \|}{\| YZ \|} = \frac{b_k(a_n + b_n) + a_na_k}{p^k} \in \mathbb{Z} \text{ (by Proposition 4)}$$

Applying Ptolemy's theorem to the quadrangle YX_kZZ_n, we have:

$$\| X_kZ_n \| = \frac{\| X_kZ \| \cdot \| Y_nY \| + \| X_kY \| \cdot \| Z_nZ \|}{\| YZ \|} = \frac{b_nb_k + a_k(a_n + b_n)}{p^k} \in \mathbb{Z} \text{ (by Proposition 4)}$$

Thus every edge of the above configuration of K_{3n+3} has integer length.

3.1.4 Final remarks

Note that in both proofs the set of odd distances realize the graph $K_{n,n,n}$ in $\mathbb{R}^2$ hence they maximize the number of odd distances among any number of points in $\mathbb{R}^2$ as noted in 3.1.

Constructing integral points in the plane is an *elementary problem*, easily understood by high school students. As such, it is desirable to have an easily understood elementary construction for it. Our proof accomplishes this goal. H. Harbroth et. al. (see [2]) were the first to prove the existence of integral sets of $3n$ points on a circle of radius $\frac{7^{n-1}}{\sqrt{3}}$. They used more advanced topics such as roots of unity in number fields and complex numbers.

For $p = 7$ (the smallest prime for which equation (2) has a solution) , this note shows that we can construct an integral set of n points on a circle of diameter $\frac{2.7^{[\frac{n-4}{3}]}}{\sqrt{3}}$, but we do not know whether or not another construction with smaller diameter exists.

A more careful inspection of our construction shows that all distances among the points $\{W_1, W_2, \ldots, W_n\}$ $W = X, Y, Z$ are even integers while all the other distances are odd integers. This gives us an alternative, elementary proof that the maximum number of odd integral distances among $3n$ points in the plane is $3n^2$ (see [3]).

Bibliography

[1] N. H. Anning and P. Erdos : *I*ntegral distances , Bull. Am. Math. Soc., 51:598óÀẼ600, 1945.

[2] H. Harborth, A. Kemnitz, M. Moller: *A*n Upper Bound of the Minimum Diameter of Integral Point Sets, Discrete Comput. Geom. (1993) 427-432.

[3] L. Piepemeyer: *T*he maximum number of odd integral distances between points in the plane, Discrete Comput. Geom. (1996) 156-159.

3.2 Erdős-Mordell inequality

Tran Nhat Tan

Abstract

In this chapter we present two proofs of the Erdős-Mordell inequality and introduce a new approach for proving the generalized Erdős-Mordell inequality for star-shaped polygons.

3.2.1 Introduction

In a talk Paul Erdős gave at the international conference on Geometry and Differential Geometry in 1979 in Haifa, Israel (see [11]) he said:

> ...many new results have been found on geometric inequalities - I won't deal with them in this paper and state only one of them, the so called Erdős - Mordell inequality (which was one of my first conjectures - I conjectured it in 1932).

Erdős' conjecture was first published in the Amer. Math. Monthly in 1935:

3740. Proposed by Paul Erdős, The University, Manchester, England.

> From a point O inside a given $\triangle ABC$ the perpendiculars OP, OQ, OR are drawn to its sides. Prove that:
>
> $$OA + OB + OC \geqslant 2(OP + OQ + OR).$$

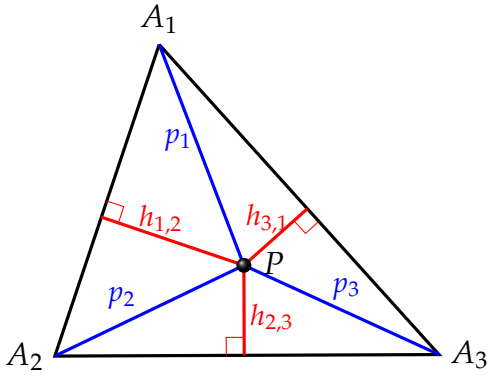
It is noteworthy that out of his many conjectures and results, Erdős chose to single out this problem. Indeed it led to many published alternative proofs of the original Erdős-Mordell (EM) triangle inequality. The first proof was published by Barrow and Mordell in 1937 (see [7]); it was not *elementary*. The first *elementary* proof using Pappus' theorem was found by D.K. Kazarinoff in 1945 (first published in 1957 see [9]). Other proofs continued to be discovered and published by many other researchers, the latest by Akira Sakurai as recent as 2012 (see [1]). In this paper the author introduced a vector analysis tool that was related to Pappus' theorem. In 2010 Jeremy Hamilton in his Master Thesis (see [2]) gave a nice historical account of the EM-triangle inequality. The EM inequality is also known by other names such as: *the original Erdős - Mordell inequality, the famous Erdős - Mordell inequality, the classical Erdős - Mordell inequality, the celebrated Erdős - Mordell inequality* and probably more.

To help us with the investigation of this problem and its generalizations we shall use the following notation: let $\triangle A_1A_2A_3$ be a triangle, and let P be an interior point of this triangle. We denote the distances from P to the vertices by $PA_i = p_i,\ i = 1,2,3$ and the distances from P to the sides A_1A_2, A_2A_3, A_3A_1 by $h_{1,2}, h_{2,3}, h_{3,1}$, respectively.

Theorem 3.11 (The Erdős-Mordell inequality) *The famous EM inequality asserts that :*

$$p_1 + p_2 + p_3 \geqslant 2\,(h_{1,2} + h_{2,3} + h_{3,1}) \tag{3.2.1}$$

with equality holding if and only if the triangle is equilateral and the point P is its center. ■



We wondered, did P. Erdős ever think that this elementary geometric question will generate so much interest?

3.2.2 Two proofs of the Erdős-Mordell inequality

In this section we give two different proofs of the EM inequality which originally dealt with triangles. The first proof, known as the first elementary proof, was found by D. K. Kazarinoff in 1945 (see [9]). The latest proof by A. Sakurai using vector analysis concepts was published in 2012 (see [1]).

3.2.2.1 The first geometric elementary proof

This proof is based on the solution by D. K. Kazarinoff (see [9]) and the talk N. Alonso III gave at Dickinson State University in 2012 (see [5]). In this presentation Alonso gave a nice history of the EM inequality and also a nice description of Kazarinoff's proof which we present here. We start by a lemma recalling Pappus generalization of the Pythagorean theorem.

Lemma 3.12 (Pappus Theorem) *Suppose parallelograms A_2A_1DE and A_1A_3FG are drawn outside the triangle $A_1A_2A_3$, and ED and FG are extended to meet at H. If we add two points I, J such that $HA_1 = A_2J = A_3I,\ HA_1 \parallel A_2J \parallel A_3I$ as shown in Figure 9 below then the sum of the areas of A_2A_1DE and A_1A_3FG is equal to the area of the parallelogram A_2A_3IJ.* ■

PROOF : Figure 9 is a short sketch of the proof (almost without words) of Pappus' Theorem.

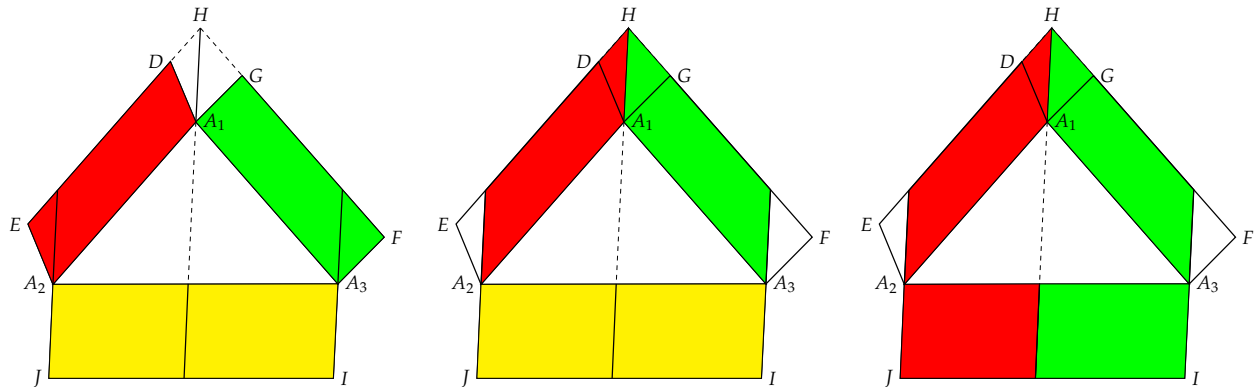


Figure 9: Brief description of Pappus' Theorem.

The four red parallelograms in Figures 9(a), 9(b) 9(c) have the same area and so do the four green parallelograms. ■

Note that when the given triangle is a right triangle and the given parallelograms are squares on its legs, Pappus' Theorem reduces to the Pythagorean theorem.

We now employ Pappus' theorem to prove the EM inequality.

PROOF Recall that in Figure 10 we need to prove the following inequality:

$$p_1 + p_2 + p_3 \geqslant 2\,(h_{1,2} + h_{2,3} + h_{3,1})\,.$$

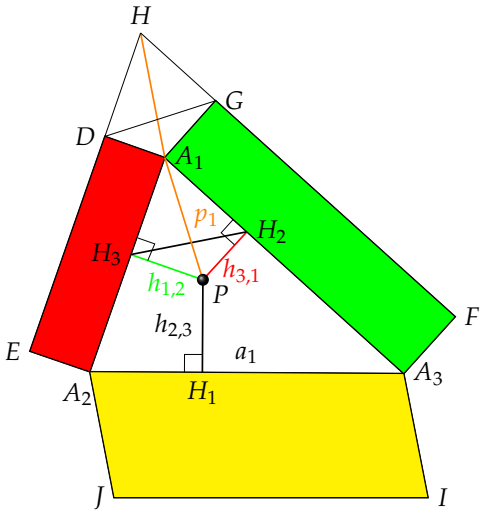


Figure 10: Proof of the EM inequality using Pappus' Theorem.

Suppose the lengths of the sides A_2A_3, A_3A_1, A_1A_2 of triangle $\triangle A_1A_2A_3$ are a_1, a_2, a_3, respectively. Let H_i be the foot of the perpendicular from P to the side opposite $A_i, i = 1, 2, 3$. The above figure is set-up as follows: on side A_1A_2 construct rectangle A_2A_1DE with width $h_{3,1}$ and on side A_1A_3 construct rectangle A_1A_3FG with width $h_{1,2}$; extend ED and FG so that they intersect at the point H. The two triangles DA_1G and H_2PH_3 are congruent since $PH_2 = A_1D, PH_3 = A_1G$ and $\angle DA_1G = \angle H_2PH_3$. To see this we note that $\angle H_2A_1H_3 + \angle H_2PH_3 = \angle DA_1G + \angle H_2A_1H_3 = \pi$. Clearly both $DHGA_1$ and $PH_2A_1H_3$ are con-cyclic therefore their circumscribed cycles have the same diameter. Hence A_1H and $PA_1 = p_1$.

On side A_2A_3 construct a parallelogram A_2A_3IJ such that $A_2J = HA_1 = A_3I$ and A_2J, HA_1, A_3I are pairwise parallel. By Pappus' theorem

$$\text{Area}(A_2A_1DE) + \text{Area}(A_1A_3FG) = \text{Area}(A_2A_3IJ).$$

Besides, $\text{Area}(A_2A_1DE) = a_3h_{3,1}$, $\text{Area}(A_1A_3FG) = a_2h_{1,2}$, $\text{Area}(A_2A_3IJ) \leqslant a_1.A_2J$ therefore $a_3h_{3,1} + a_2h_{1,2} \leqslant a_1p_1$. Thus,

$$p_1 \geqslant \frac{a_3}{a_1}h_{3,1} + \frac{a_2}{a_1}h_{1,2} \tag{3.2.2}$$

with equality if and only if $A_2J \perp A_2A_3$ or equivalently $HA_1 \perp A_2A_3$.

Similar to (3.2.2), we have

$$p_2 \geqslant \frac{a_3}{a_2}h_{2,3} + \frac{a_1}{a_2}h_{1,2}$$
$$p_3 \geqslant \frac{a_1}{a_3}h_{3,1} + \frac{a_2}{a_3}h_{2,3}$$

Adding these three inequalities yields

$$p_1 + p_2 + p_3 \geqslant \left(\frac{a_2}{a_1} + \frac{a_1}{a_2}\right)h_{1,2} + \left(\frac{a_3}{a_2} + \frac{a_2}{a_3}\right)h_{2,3} + \left(\frac{a_3}{a_1} + \frac{a_1}{a_3}\right)h_{3,1}. \tag{3.2.3}$$

Since $x + \frac{1}{x} \geqslant 2$ for every $x > 0$ with equality if and only if $x = 1$ the coefficients of $h_{1,2}, h_{2,3}$, and $h_{3,1}$ are each at least 2 and are equal to 2 if and only if $a_1 = a_2 = a_3$ i.e. the triangle $A_1A_2A_3$ is equilateral.

To prove that P must be the center of the equilateral triangle consider another location for P inside the triangle. We have:

$$h_{1,2} = p_2 \cdot \sin\angle PA_2A_1 = p_1 \cdot \sin(\pi/3 - \angle PA_1A_3)$$
$$h_{2,3} = p_3 \cdot \sin\angle PA_3A_2 = p_2 \cdot \sin(\pi/3 - \angle PA_2A_1)$$
$$h_{3,1} = p_1 \cdot \sin\angle PA_1A_3 = p_3 \cdot \sin(\pi/3 - \angle PA_3A_2)$$

Set $\angle PA_1A_3 = \alpha, \angle PA_2A_1 = \beta, \angle PA_3A_2 = \gamma, 0 \leqslant \alpha, \beta, \gamma \leqslant \pi/3$. Hence:

$$2(h_{1,2} + h_{2,3} + h_{3,1}) = p_1(\sin\alpha + \sin(\pi/3 - \alpha)) + p_2(\sin\beta + \sin(\pi/3 - \beta)) + p_3(\sin\gamma + \sin(\pi/3 - \gamma))$$

We claim that $\sin t + \sin(\pi/3 - t) \leqslant 1$ for $0 \leqslant t \leqslant \pi/3$ with equality if and only if $t = \pi/6$. To see this we write

$$\sin t + \sin\left(\frac{\pi}{3} - t\right) = \sin t + \frac{\sqrt{3}}{2}\cos t - \frac{1}{2}\sin t = \frac{1}{2}\sin t + \frac{\sqrt{3}}{2}\cos t = \sin\left(t + \frac{\pi}{3}\right) \leqslant 1.$$

Hence equality holds in the EM inequality if and only if the triangle is equilateral and P is its center. ∎

3.2.3 Vector analysis proof

This proof uses the $1/2$-*power of plane vectors* recently introduced by Akira Sakurai in 2012 (see [1]) to provide yet another proof of the EM inequality. For the reader's convenience we will repeat it here. We also chose to include it for two reasons: it is a time line history of the active interest in the EM inequality, starting in 1935 and still active today and also because it is the main tool we use in this paper.
Let $\mathbf{p} = (x, y)$ represent non-zero vectors in $\mathbb{R}^2$. We prefer to work in $\mathbb{R}^3$. Thus we have:

$$\mathbf{p} = (x, y, 0) = (p\cos\phi, p\sin\phi, 0).$$

where $p = +\sqrt{x^2 + y^2} > 0, \quad 0 \leqslant \phi < 2\pi, \quad \phi = \tan^{-1}(y/x)$. p, ϕ are called the polar coordinates of the vector $\mathbf{p}$, p is the length (radius) and ϕ is the polar angle.

Definition 2 (1/2-power of a plane vector)

$$\boldsymbol{p}^{1/2} := \left(\sqrt{p}\cos\frac{\phi}{2}, \sqrt{p}\sin\frac{\phi}{2}, 0\right).$$

∎

Let $\mathbf{p}_i = (p_i\cos\phi_i, p_i\sin\phi_i, 0), \mathbf{p}_j = (p_j\cos\phi_j, p_j\sin\phi_j, 0)$ be non-zero vectors so that

$$\mathbf{p}_i^{1/2} = \left(\sqrt{p_i}\cos\frac{\phi_i}{2}, \sqrt{p_i}\sin\frac{\phi_i}{2}, 0\right) \quad \text{and} \quad \mathbf{p}_j^{1/2} = \left(\sqrt{p_j}\cos\frac{\phi_j}{2}, \sqrt{p_j}\sin\frac{\phi_j}{2}, 0\right).$$

The following two lemmas are from A. Sakurai's paper:

Lemma 3.13

(a) $\boldsymbol{p}_i^{1/2} \cdot \boldsymbol{p}_i^{1/2} = p_i = \|\boldsymbol{p}_i\|$.

(b) $\boldsymbol{p}_i \times \boldsymbol{p}_j = 2\left(\boldsymbol{p}_i^{1/2} \cdot \boldsymbol{p}_j^{1/2}\right)\left(\boldsymbol{p}_i^{1/2} \times \boldsymbol{p}_j^{1/2}\right)$.

(c) $\|\boldsymbol{p}_i - \boldsymbol{p}_j\| \geqslant 2\|\boldsymbol{p}_i^{1/2} \times \boldsymbol{p}_j^{1/2}\|$, *with equality holding if and only if* $p_i = p_j$. ∎

PROOF Recall that if $\mathbf{x} = (x_1, x_2, x_3)$ and $\mathbf{y} = (y_1, y_2, y_3)$ then

$$\mathbf{x} \cdot \mathbf{y} = x_1y_1 + x_2y_2 + x_3y_3$$
$$\mathbf{x} \times \mathbf{y} = (x_2y_3 - x_3y_2, x_3y_1 - x_1y_3, x_1y_2 - x_2y_1)$$

Let $\phi_{i,j} := \phi_j - \phi_i$ then we have the following equations

$$\mathbf{p}_i \cdot \mathbf{p}_j = p_ip_j \cos\phi_i \cos\phi_j + p_ip_j \sin\phi_j \sin\phi_i = p_ip_j \cos(\phi_j - \phi_i) = p_ip_j \cos\phi_{i,j}, \tag{3.2.4}$$

$$\mathbf{p}_i^{1/2} \cdot \mathbf{p}_j^{1/2} = \sqrt{p_jp_j} \cos\frac{\phi_i}{2} \cos\frac{\phi_j}{2} + \sqrt{p_jp_j} \sin\frac{\phi_i}{2} \sin\frac{\phi_j}{2} = \sqrt{p_jp_j} \cos\frac{\phi_{i,j}}{2}, \tag{3.2.5}$$

$$\mathbf{p}_i \times \mathbf{p}_j = (0, 0, p_ip_j \cos\phi_i \sin\phi_j - p_ip_j \cos\phi_j \sin\phi_i) = (0, 0, p_ip_j \sin\phi_{i,j}), \tag{3.2.6}$$

$$\mathbf{p}_i^{1/2} \times \mathbf{p}_j^{1/2} = \left(0, 0, \sqrt{p_jp_j} \cos\frac{\phi_i}{2} \sin\frac{\phi_j}{2} - p_ip_j \cos\frac{\phi_j}{2} \sin\frac{\phi_i}{2}\right) = \left(0, 0, \sqrt{p_jp_j} \sin\frac{\phi_{i,j}}{2}\right). \tag{3.2.7}$$

(a) The proof of (a) is clear since $\phi_{i,i} = 0$ and from (3.3.1) $\mathbf{p}_i^{1/2} \cdot \mathbf{p}_i^{1/2} = p_i = \|\mathbf{p}_i\|$.

(b) We have:

$$\begin{aligned}\mathbf{p}_i \times \mathbf{p}_j &= (0, 0, p_ip_j \sin\phi_{i,j}) = \left(0, 0, 2p_ip_j \sin\frac{\phi_{i,j}}{2} \cos\frac{\phi_{i,j}}{2}\right) \\ &= 2\sqrt{p_jp_j} \cos\frac{\phi_{i,j}}{2} \left(0, 0, \sqrt{p_jp_j} \sin\frac{\phi_{i,j}}{2}\right) = 2\left(\mathbf{p}_i^{1/2} \cdot \mathbf{p}_j^{1/2}\right)\left(\mathbf{p}_i^{1/2} \times \mathbf{p}_j^{1/2}\right)\end{aligned}$$

(c) $\|\mathbf{p}_i - \mathbf{p}_j\|^2 = p_i^2 + p_j^2 - 2p_ip_j \cos\phi_{i,j} \geqslant 2p_ip_j(1 - \cos\phi_{i,j}) = 4p_ip_j \sin^2\frac{\phi_{i,j}}{2} = 4\|\mathbf{p}_i^{1/2} \times \mathbf{p}_j^{1/2}\|^2$, the inequality arises from $p_i^2 + p_j^2 \geqslant 2p_ip_j$, and this becomes an equality if and only if $p_i = p_j$. ∎

Lemma 3.14 *Let PA_iA_j be a triangle such that $\overrightarrow{PA_i} = \boldsymbol{p}_i$ and $\overrightarrow{PA_j} = \boldsymbol{p}_j$. Then the distance $h_{i,j}$ of P to the line A_iA_j satisfies the relation*

$$h_{i,j} = \frac{\|\boldsymbol{p}_i \times \boldsymbol{p}_j\|}{\|\boldsymbol{p}_i - \boldsymbol{p}_j\|} \leqslant \left|\boldsymbol{p}_i^{1/2} \cdot \boldsymbol{p}_j^{1/2}\right|, \tag{3.2.8}$$

with equality if and only if $p_i = p_j$. ∎

PROOF The area of the parallelogram spanned by $\mathbf{p}_i$ and $\mathbf{p}_j$ is $\|\mathbf{p}_i \times \mathbf{p}_j\|$, which equals $\|\mathbf{p}_i - \mathbf{p}_j\| \cdot h_{i,j}$. The equality in (3.2.8) is therefore clear. Next, by (b) and (c) in Lemma 3.13, we have

$$h_{i,j} = \frac{2\left|\mathbf{p}_i^{1/2} \cdot \mathbf{p}_j^{1/2}\right| \|\mathbf{p}_i^{1/2} \times \mathbf{p}_j^{1/2}\|}{\|\mathbf{p}_i - \mathbf{p}_j\|} \leqslant \left|\mathbf{p}_i^{1/2} \cdot \mathbf{p}_j^{1/2}\right|.$$

Equality holds if and only if the inequality in Lemma 3.13(c) is an equality, which happens if and only if $p_i = p_j$. ∎

The following is a proof of the EM inequality based on the A. Sakurai's solution.

$$p_1 + p_2 + p_3 \geqslant 2\left(h_{1,2} + h_{2,3} + h_{3,1}\right).$$

PROOF Without loss of generality, we may assume that $P = (0,0,0)$, $A_1 = (p_1,0,0)$, $A_2 = (b_1,b_2,0)$ with $b_2 > 0$, and $A_3 = (c_1,c_2,0)$ with $c_2 < 0$ (see Figure 11).

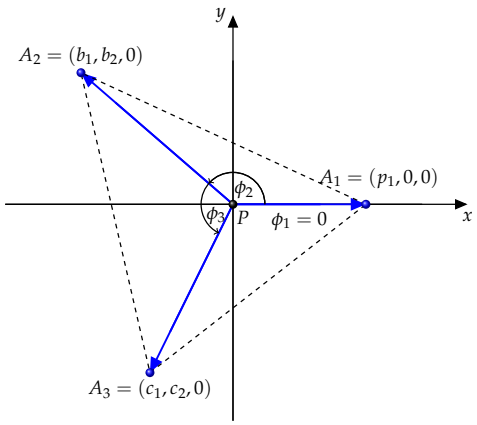


Figure 11: Sakurai's set-up for the triangle.

We further set

$$\overrightarrow{PA_i} = \mathbf{p}_i = (p_i \cos\phi_i, p_i \sin\phi_i, 0), \quad i = 1,2,3.$$

It follows that

$$\phi_1 = 0, \quad 0 < \phi_2 < \pi, \quad \pi < \phi_3 < 2\pi,$$

additionally since P is an interior point

$$0 < \phi_2 - \phi_1 < \pi, \quad 0 < \phi_3 - \phi_2 < \pi, \quad \pi < \phi_3 - \phi_1 < 2\pi. \tag{3.2.9}$$

Now from Lemma 3.13(a), Lemma 3.14 and (3.2.9) above, A. Sakurai derived the following

$$\begin{aligned}
&p_1 + p_2 + p_3 - 2\left(h_{1,2} + h_{2,3} + h_{3,1}\right) \\
&\geqslant \mathbf{p}_1^{1/2}\cdot\mathbf{p}_1^{1/2} + \mathbf{p}_2^{1/2}\cdot\mathbf{p}_2^{1/2} + \mathbf{p}_3^{1/2}\cdot\mathbf{p}_3^{1/2} - 2\mathbf{p}_1^{1/2}\cdot\mathbf{p}_2^{1/2} - 2\mathbf{p}_2^{1/2}\cdot\mathbf{p}_3^{1/2} + 2\mathbf{p}_3^{1/2}\cdot\mathbf{p}_1^{1/2} \qquad (3.2.10)\\
&= \left(\mathbf{p}_1^{1/2} - \mathbf{p}_2^{1/2} + \mathbf{p}_3^{1/2}\right)\cdot\left(\mathbf{p}_1^{1/2} - \mathbf{p}_2^{1/2} + \mathbf{p}_3^{1/2}\right) \\
&= \|\mathbf{p}_1^{1/2} - \mathbf{p}_2^{1/2} + \mathbf{p}_3^{1/2}\|^2 \geqslant 0. \qquad (3.2.11)
\end{aligned}$$

Which implies that

$$p_1 + p_2 + p_3 \geqslant 2\left(h_{1,2} + h_{2,3} + h_{3,1}\right).$$

Next, we establish the condition for the equality of the EM inequality (i.e., for the two inequalities in (3.2.10) and (3.2.11) to both be equalities). The inequality in (3.2.10) is due

to the three inequalities $h_{1,2} \leqslant \left|\mathbf{p}_1^{1/2} \cdot \mathbf{p}_2^{1/2}\right| = \mathbf{p}_1^{1/2} \cdot \mathbf{p}_2^{1/2}, h_{2,3} \leqslant \left|\mathbf{p}_2^{1/2} \cdot \mathbf{p}_3^{1/2}\right| = \mathbf{p}_2^{1/2} \cdot \mathbf{p}_3^{1/2}$ and $h_{3,1} \leqslant \left|\mathbf{p}_3^{1/2} \cdot \mathbf{p}_1^{1/2}\right| = -\mathbf{p}_3^{1/2} \cdot \mathbf{p}_1^{1/2}$. These three all depend on Lemma 3.14, and the equality condition there implies $p_1 = p_2 = p_3$. We therefore obtain that the inequality in (3.2.10) is an equality if and only if vertices A_1, A_2, A_3 lie on a circle centered at P. Let us assume that this condition holds for the remainder of this proof. Now consider the inequality of (3.2.11). Clearly, this becomes an equality if and only if $\mathbf{p}_2^{1/2} = \mathbf{p}_1^{1/2} + \mathbf{p}_3^{1/2}$, where $\|\mathbf{p}_1^{1/2}\| = \|\mathbf{p}_2^{1/2}\| = \|\mathbf{p}_3^{1/2}\|$ and $\phi_1 = 0$. Hence, one sees at once that $\mathbf{p}_1^{1/2}$ and $\mathbf{p}_3^{1/2}$ generate a parallelogram with all four sides equal, where $\mathbf{p}_2^{1/2}$ is its diagonal, also of equal size (see Figure 12). We conclude that the EM inequality becomes an equality if and only

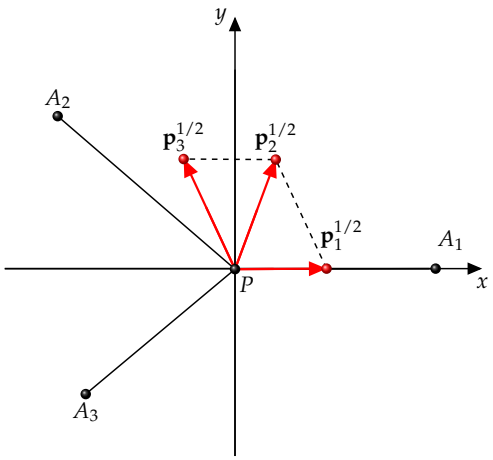


Figure 12: 1/2-power of plane vectors generate a parallelogram.

if tips A_1, A_2 and A_3 of the vectors $\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3$ rooted at P form an equilateral triangle with its center at P. ■

3.2.4 Erdös-Mordell inequality for polygons

3.2.4.1 Erdös-Mordell inequality for convex polygons

Several geometric inequalities can be extended in many different ways. One common approach is to increase the size of the object. In 1957, Florian proved the EM inequality for convex quadrilaterals and conjectured for convex polygons the following (see [8]).

Conjecture 3.15 *Let $A_1A_2 \ldots A_n$ be a convex polygon, let P be an interior point of the polygon. Let the distances from P to vertices A_k be p_k and let those to sides A_kA_{k+1} be $h_{k,k+1}$, (the index k is taken modulo n). Then*

$$\sum_{k=1}^{n} p_k \geqslant \frac{1}{\cos(\pi/n)} \sum_{k=1}^{n} h_{k,k+1},$$

with equality if and only if the polygon is regular and P is its center. ■

His conjecture was a challenging problem until recently. To the best of our knowledge, the first time this conjecture was proved was in 2005 by S. Gueron and I. Shafrir (see [4]). They actually proved a more general inequality involving weights. Two years later in 2007, M. Dinca provided a simpler proof of Florian's conjecture but did not address the second part of the conjecture namely when equality holds (see [3]). Another paper published in 2012 by A. Vandanjav, B. Tserendorj and B. Undrakh described many generalizations of the EM inequality; but their presentation of the EM inequality for convex polygons was still incomplete avoiding the equality case (see [10]). In this section, we establish a new and complete proof to the EM inequality for convex polygons. Our proof can be regarded as an adaptation of A. Sakurai's tools (see [1] and Section 3.2.3) and M. Dinca's method (see [3]).

Definition 3 (Geometric interpretation of angles) *The geometric angle generated by two non-zero vectors* $\boldsymbol{p}_i = (p_i \cos\phi_i, p_i \sin\phi_i, 0, \boldsymbol{p}_j = (p_j \cos\phi_j, p_j \sin\phi_j, 0)$ *is defined as:*

$$\theta_{i,j} := \begin{cases} |\phi_j - \phi_i| & \text{if} \quad 0 \leqslant |\phi_j - \phi_i| < \pi \\ 2\pi - |\phi_j - \phi_i| & \text{if} \quad \pi \leqslant |\phi_j - \phi_i| < 2\pi \end{cases} . \tag{3.2.12}$$

■

From the above definition we see that $0 \leqslant \theta_{i,j} \leqslant \pi$. In addition, given three points P, A_i, A_j in $xy-$plane such that $\overrightarrow{PA_i} = \mathbf{p}_i, \overrightarrow{PA_j} = \mathbf{p}_j$, we know that $\angle A_i P A_j$ denotes the size of the positive angle less than or equal to π which is generated by vectors $\overrightarrow{PA_i}$ and $\overrightarrow{PA_j}$. As a result, $\theta_{i,j} = \theta_{j,i} = \angle A_i P A_j$.

PROOF Without loss of generality, we may assume that $P = (0,0,0)$, A_1 is located on the $x-$axis (see Figure 13).

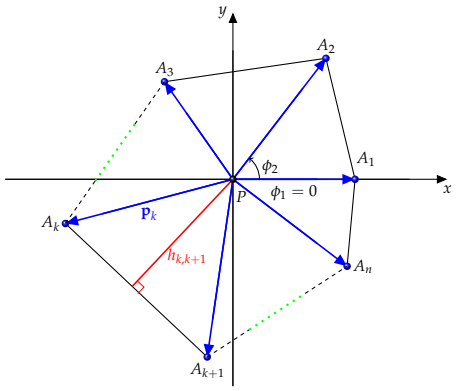


Figure 13: A set-up for the convex polygon.

Let

$$\overrightarrow{PA_k} = \mathbf{p}_k = (p_k \cos\phi_k, p_k \sin\phi_k, 0), \quad k = 1, 2, \ldots, n.$$

The polar angles ϕ_i are oriented counter clockwise in the $xy-$plane so that

$$0 = \phi_1 < \phi_2 < \ldots < \phi_{n-1} < \phi_n < 2\pi.$$

Since P is an interior point

$$0 < \phi_{k+1} - \phi_k < \pi, \quad \pi < \phi_n - \phi_1 < 2\pi, \quad k = 1, 2, \ldots, n-1, \tag{3.2.13}$$

additionally,

$$\theta_{1,2} + \cdots + \theta_{i,i+1} + \cdots + \theta_{n-1,n} + \theta_{n,1} = 2\pi. \tag{3.2.14}$$

Now from Lemma 3.14 in Section 3.2.3 and (3.2.13) above, we have

$$\begin{aligned} h_{k,k+1} &\leqslant \left|\mathbf{p}_k^{1/2} \cdot \mathbf{p}_{k+1}^{1/2}\right| = \mathbf{p}_k^{1/2} \cdot \mathbf{p}_{k+1}^{1/2}, \quad k = 1, 2, \ldots, n-1, \\ h_{n,1} &\leqslant \left|\mathbf{p}_n^{1/2} \cdot \mathbf{p}_1^{1/2}\right| = -\mathbf{p}_n^{1/2} \cdot \mathbf{p}_1^{1/2}. \end{aligned} \tag{3.2.15}$$

Therefore,

$$\sum_{k=1}^{n-1} \mathbf{p}_k^{1/2} \cdot \mathbf{p}_{k+1}^{1/2} - \mathbf{p}_n^{1/2} \cdot \mathbf{p}_1^{1/2} \geqslant \sum_{k=1}^{n} h_{k,k+1}. \tag{3.2.16}$$

We shall prove a stronger inequality than the EM inequality for convex polygons (**??**)

$$\cos\frac{\pi}{n} \sum_{k=1}^{n} p_k \geqslant \sum_{k=1}^{n-1} \mathbf{p}_k^{1/2} \cdot \mathbf{p}_{k+1}^{1/2} - \mathbf{p}_n^{1/2} \cdot \mathbf{p}_1^{1/2}. \tag{3.2.17}$$

This inequality is equivalent to

$$\cos\frac{\pi}{n} \sum_{k=1}^{n} p_k - \sum_{k=1}^{n-1} \mathbf{p}_k^{1/2} \cdot \mathbf{p}_{k+1}^{1/2} + \mathbf{p}_n^{1/2} \cdot \mathbf{p}_1^{1/2} \geqslant 0. \tag{3.2.18}$$

For every $k = 1, 2, \ldots, n-2$ we consider the following expressions

$$E(k, k+1, n) = \frac{1}{2\sin\frac{k\pi}{n}\sin\frac{(k+1)\pi}{n}} \left(\sin\frac{(k+1)\pi}{n}\mathbf{p}_k^{1/2} - \sin\frac{k\pi}{n}\mathbf{p}_{k+1}^{1/2} + \sin\frac{\pi}{n}\mathbf{p}_n^{1/2}\right)^2. \tag{3.2.19}$$

These quadratic forms are taken from M. Dinca's proof (in [3]) infused with A. Sakurai's vector analysis tools. Our purpose is to complete her proof using her ideas until the EM inequality for convex polygons is proved. From this point we will be able to prove the second part (when equality holds) of Florian's conjecture.

The triple $(k, k+1, n)$ describes the order of the vectors $\mathbf{p}_k, \mathbf{p}_{k+1}, \mathbf{p}_n$ as we move from the $x-$axis ($\mathbf{p}_1$) counter clock-wise.
We start with the following identity:

$$\cos\frac{\pi}{n} \sum_{k=1}^{n} p_k - \sum_{k=1}^{n-1} \mathbf{p}_k^{1/2} \cdot \mathbf{p}_{k+1}^{1/2} + \mathbf{p}_n^{1/2} \cdot \mathbf{p}_1^{1/2} = \sum_{k=1}^{n-2} E(k, k+1, n). \tag{3.2.20}$$

To prove this, we compute the coefficients of terms which appear in both sides of (3.2.20). First, we expand $E(k,k+1,n)$:

$$E(k,k+1,n) = \frac{\sin\frac{(k+1)\pi}{n}}{2\sin\frac{k\pi}{n}}p_k + \frac{\sin\frac{k\pi}{n}}{2\sin\frac{(k+1)\pi}{n}}p_{k+1} + \frac{\sin^2\frac{\pi}{n}}{2\sin\frac{k\pi}{n}\sin\frac{(k+1)\pi}{n}}p_n$$
$$- \mathbf{p}_k^{1/2}\cdot\mathbf{p}_{k+1}^{1/2} - \frac{\sin\frac{\pi}{n}}{\sin\frac{(k+1)\pi}{n}}\mathbf{p}_{k+1}^{1/2}\cdot\mathbf{p}_n^{1/2} + \frac{\sin\frac{\pi}{n}}{\sin\frac{k\pi}{n}}\mathbf{p}_k^{1/2}\cdot\mathbf{p}_n^{1/2}. \tag{3.2.21}$$

We can now identify the coefficients of

$$p_k, \quad p_{k+1}, \quad p_n, \quad \mathbf{p}_k^{1/2}\cdot\mathbf{p}_{k+1}^{1/2}, \quad \mathbf{p}_k^{1/2}\cdot\mathbf{p}_n^{1/2}, \quad \mathbf{p}_{k+1}^{1/2}\cdot\mathbf{p}_n^{1/2}$$

in the expansion of $E(k,k+1,n)$ for every $k = 1,2,\ldots,n-2$.

- The coefficient of p_1 appears only in $E(1,2,n)$ (take $k=1$ in (3.2.21)), it is
$$\frac{\sin\frac{2\pi}{n}}{2\sin\frac{\pi}{n}} = \cos\frac{\pi}{n}.$$
- For $k = 2,3,\ldots,n-2$ the coefficients of p_k appear in $E(k-1,k,n), E(k,k+1,n)$, it is
$$\frac{\sin\frac{(k-1)\pi}{n}}{2\sin\frac{k\pi}{n}} + \frac{\sin\frac{(k+1)\pi}{n}}{2\sin\frac{k\pi}{n}} = \frac{2\sin\frac{k\pi}{n}\cos\frac{\pi}{n}}{2\sin\frac{k\pi}{n}} = \cos\frac{\pi}{n}.$$
- The coefficient of p_{n-1} appears only in $E(n-2,n-1,n)$ (take $k=n-2$ in (3.2.21)), it is
$$\frac{\sin\frac{(n-2)\pi}{n}}{2\sin\frac{(n-1)\pi}{n}} = \frac{\sin\frac{2\pi}{n}}{2\sin\frac{\pi}{n}} = \cos\frac{\pi}{n}.$$
- The coefficient of p_n appear in $E(1,2,n),\ldots,E(k,k+1,n),\ldots,E(n-2,n-1,n)$, it is
$$\sum_{k=1}^{n-2}\frac{\sin^2\frac{\pi}{n}}{2\sin\frac{k\pi}{n}\sin\frac{(k+1)\pi}{n}} = \sum_{k=1}^{n-2}\frac{\sin\frac{\pi}{n}}{2}\left(\cot\frac{k\pi}{n} - \cot\frac{(k+1)\pi}{n}\right)$$
$$= \frac{1}{2}\sin\frac{\pi}{n}\cdot\left(\cot\frac{\pi}{n} - \cot\frac{(n-1)\pi}{n}\right) = \frac{1}{2}\sin\frac{\pi}{n}\cdot 2\cot\frac{\pi}{n} = \cos\frac{\pi}{n}.$$
- For $k = 1,\ldots,n-2$ the coefficient of $\mathbf{p}_k^{1/2}\cdot\mathbf{p}_{k+1}^{1/2}$ appears in $E(k,k+1,n)$, it is -1.
- The coefficient of $\mathbf{p}_{n-1}^{1/2}\cdot\mathbf{p}_n^{1/2}$ appears in $E(n-2,n-1,n)$, so it is
$$-\frac{\sin\frac{\pi}{n}}{\sin\frac{(n-1)\pi}{n}} = -\frac{\sin\frac{\pi}{n}}{\sin\frac{\pi}{n}} = -1.$$

- The coefficient of $\mathbf{p}_n^{1/2} \cdot \mathbf{p}_1^{1/2}$ appears only in $E(1;2,n)$, it is

$$\frac{\sin\frac{\pi}{n}}{\sin\frac{\pi}{n}} = 1.$$

- For $k = 2, \ldots, n-2$ then the coefficients of $\mathbf{p}_k^{1/2} \cdot \mathbf{p}_n^{1/2}$ appear in $E(k-1,k,n)$, $E(k,k+1,n)$, it is

$$\frac{\sin\frac{\pi}{n}}{\sin\frac{k\pi}{n}} - \frac{\sin\frac{\pi}{n}}{\sin\frac{k\pi}{n}} = 0.$$

This completes the proof of the identity (3.2.20). $E(k,k+1,n) \geqslant 0$ for every $k = 1,2,\ldots,n-2$, thus the inequality (3.2.18) is proved and also the EM inequality for convex polygons is proved.

Next, we establish the condition for the equality to hold. We first need the equality in (3.2.16) to be equality i.e. all n inequalities in (3.2.15) to be equalities. They all depend on Lemma 3.14 Section 3.2.3, and the equality condition there implies $p_1 = p_2 = \cdots = p_n$. We therefore conclude that the EM inequality for convex polygons is an equality if vertices $A_1, A_2, \ldots, A_n$ lie on a circle centered at P. Without loss of generality we may suppose that the circle has radius 1, i.e. $p_1 = p_2 = \cdots = p_n = 1$. Let us assume that this condition holds for the remainder of this proof. Subsequently, the inequality in (3.2.17) becomes an equality if and only if

$$E(k,k+1,n) = 0, \quad \text{for all } k = 1,2,\ldots,n-2.$$

In particular, $E(1,2,n) = 0$ implies that

$$\sin\frac{2\pi}{n}\mathbf{p}_1^{1/2} - \sin\frac{\pi}{n}\mathbf{p}_2^{1/2} + \sin\frac{\pi}{n}\mathbf{p}_n^{1/2} = 0. \tag{3.2.22}$$

Equation (3.2.22) is described in Figure 14.

$$\text{Let } \overrightarrow{PN} = \sin\frac{\pi}{n}\mathbf{p}_n^{1/2}, \quad \overrightarrow{PM} = \sin\frac{\pi}{n}\mathbf{p}_2^{1/2}, \quad \overrightarrow{PQ} = \sin\frac{2\pi}{n}\mathbf{p}_1^{1/2}.$$

Note that for $i = 1,2,\ldots,n$ $p_i = 1$ hence

$$\|PM\| = \|PN\| = \sin\frac{\pi}{n}, \quad \|PQ\| = \sin\frac{2\pi}{n}.$$

Relation (3.2.22) implies that $\overrightarrow{PM} = \overrightarrow{PN} + \overrightarrow{PQ}$ so $MNPQ$ is a parallelogram therefore $\|PM\| = \|PN\| = \|QM\|$. Using the law of cosine for $\triangle MPQ$ we get

$$\cos\angle MPQ = \frac{\|PM\|^2 + \|PQ\|^2 - \|MQ\|^2}{2\|PQ\| \cdot \|PM\|} = \frac{\sin^2\frac{2\pi}{n}}{2\sin\frac{2\pi}{n}\sin\frac{\pi}{n}} = \cos\frac{\pi}{n} \quad \text{i.e.} \quad \angle MPQ = \frac{\pi}{n}.$$

Additionally, since $\phi_1 = 0, 0 < \phi_2 < \pi$ then

$$\frac{\phi_2 - \phi_1}{2} = \angle MPQ = \frac{\pi}{n} \quad \text{i.e.} \quad \phi_2 = \frac{2\pi}{n}.$$

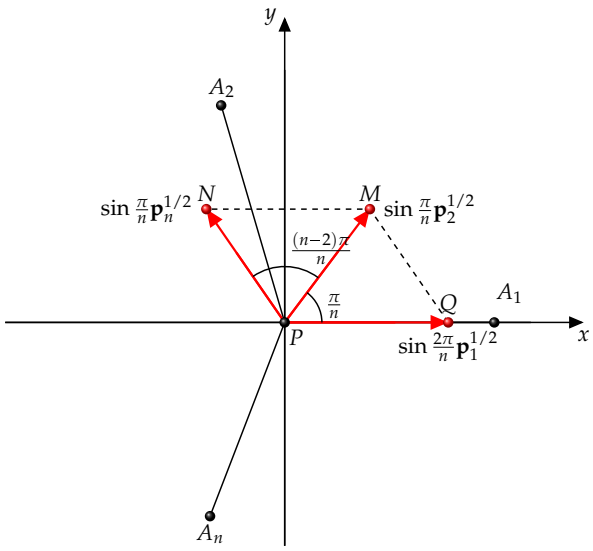


Figure 14: Description of equation (3.2.22).

It follows that,

$$\theta_{1,2} = \frac{2\pi}{n}. \tag{3.2.23}$$

Besides, $\triangle MNP$ is isosceles with base MN and $\angle MPQ = \pi/n$ therefore both two base angles equal π/n. Therefore,

$$\angle NPM = \frac{(n-2)\pi}{n} \quad \text{thus} \quad \phi_n = 2\angle NPQ = 2\angle NPM + 2\angle MPQ = \frac{2(n-1)\pi}{n}.$$

In addition, $\theta_{n,1} = 2\pi - \phi_n$ thus

$$\theta_{n,1} = \frac{2\pi}{n}. \tag{3.2.24}$$

Moreover, for $k = 2, \ldots, n-2$, the condition $E(k, k+1, n) = 0$ is equivalent to

$$\sin\frac{(k+1)\pi}{n}\mathbf{p}_k^{1/2} - \sin\frac{k\pi}{n}\mathbf{p}_{k+1}^{1/2} + \sin\frac{\pi}{n}\mathbf{p}_n^{1/2} = 0 \tag{3.2.25}$$

The above equation is described in Figure 15.

$$\text{Let } \overrightarrow{PF} = \sin\frac{\pi}{n}\mathbf{p}_n^{1/2}, \quad \overrightarrow{PE} = \sin\frac{k\pi}{n}\mathbf{p}_{k+1}^{1/2}, \quad \overrightarrow{PG} = \sin\frac{(k+1)\pi}{n}\mathbf{p}_k^{1/2}.$$

Note that $p_i = 1, i = 1, 2, \ldots, n$ so that

$$\|PF\| = \sin\frac{\pi}{n}, \quad \|PE\| = \sin\frac{k\pi}{n}, \quad \|PG\| = \sin\frac{(k+1)\pi}{n}.$$

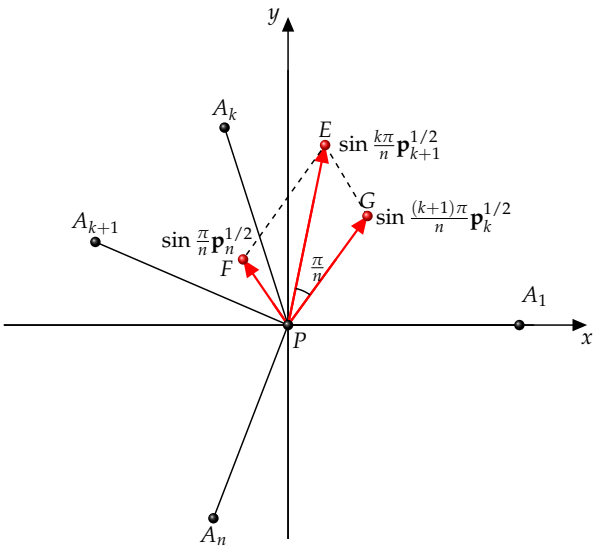


Figure 15: Description of the equation (3.2.25).

The relation (3.2.25) implies that $\overrightarrow{PE} = \overrightarrow{PF} + \overrightarrow{PG}$ so $EFPQ$ is a parallelogram therefore $\|PF\| = \|EG\|$. Using the law of cosine for the $\triangle EPG$ we have

$$\begin{aligned}
\cos\angle EPG &= \frac{\|PE\|^2 + \|PG\|^2 - \|EG\|^2}{2\|PE\| \cdot \|PG\|} = \frac{\sin^2\frac{k\pi}{n} + \sin^2\frac{(k+1)\pi}{n} - \sin^2\frac{\pi}{n}}{2\sin\frac{k\pi}{n}\sin\frac{(k+1)\pi}{n}} \\
&= \frac{1 - \cos\frac{2k\pi}{n} + 1 - \cos\frac{2(k+1)\pi}{n} - 2\sin^2\frac{\pi}{n}}{4\sin\frac{k\pi}{n}\sin\frac{(k+1)\pi}{n}} = \frac{2 - 2\sin^2\frac{\pi}{n} - \left(\cos\frac{2k\pi}{n} + \cos\frac{2(k+1)\pi}{n}\right)}{4\sin\frac{k\pi}{n}\sin\frac{(k+1)\pi}{n}} \\
&= \frac{2\cos^2\frac{\pi}{n} - 2\cos\frac{(2k+1)\pi}{n}\cos\frac{\pi}{n}}{4\sin\frac{k\pi}{n}\sin\frac{(k+1)\pi}{n}} = \frac{2\cos\frac{\pi}{n}\left(\cos\frac{\pi}{n} - \cos\frac{(2k+1)\pi}{n}\right)}{4\sin\frac{k\pi}{n}\sin\frac{(k+1)\pi}{n}} \\
&= \frac{2\cos\frac{\pi}{n}.2\sin\frac{k\pi}{n}\sin\frac{(k+1)\pi}{n}}{4\sin\frac{k\pi}{n}\sin\frac{(k+1)\pi}{n}} = \cos\frac{\pi}{n} \quad \text{i.e.} \quad \angle EPG = \frac{\pi}{n}.
\end{aligned}$$

It follows that,

$$\frac{\phi_{k+1} - \phi_k}{2} = \angle EPG = \frac{\pi}{n} \quad \text{i.e.} \quad \phi_{k+1} - \phi_k = \frac{2\pi}{n}.$$

Therefore,

$$\theta_{k,k+1} = \frac{2\pi}{n}, \quad \text{for all } k = 2, 3, \ldots, n-2. \tag{3.2.26}$$

Combining the relations (3.2.23), (3.2.24) and (3.2.26) implies that

$$\theta_{1,2} = \cdots = \theta_{k,k+1} \cdots = \theta_{n-2,n-1} = \theta_{n,1} = \frac{2\pi}{n}. \tag{3.2.27}$$

Therefore the remaining geometric angle $\theta_{n-1,n}$ must be $2\pi/n$ because they sum up to 2π (see (3.2.14)) i.e.

$$\theta_{1,2} = \cdots = \theta_{k,k+1} \cdots = \theta_{n-1,n} = \theta_{n,1} = \frac{2\pi}{n}. \tag{3.2.28}$$

We conclude that the condition for the equality in the EM inequality for convex polygons is that $A_1, A_2, \dots A_n$ of the vectors $\mathbf{p}_1, \mathbf{p}_2, \dots, \mathbf{p}_n$ rooted at P form a regular polygon with its center at P, as conjectured by Florian 56 years ago! ■

3.2.5 Erdös-Mordell inequality for star-shaped polygons

From the results discussed in Section 3.2.4.1 we will prove an extension of the EM inequality for star shaped polygons. One sees that the most important point that we used in the previous section is the condition (3.2.14), that is $\theta_{1,2} + \dots + \theta_{i,i+1} + \dots + \theta_{n-1,n} + \theta_{n,1} = 2\pi$. This implies that the convexity of polygons is not absolutely strict. The point P and vertices $A_1, A_2, \dots, A_n$ only have to satisfy the condition (3.2.14) to ensure that the EM inequality for convex polygons and its equality case hold. From this point we can extend the convex polygons class to a more general class.

Definition 4 (Star-shaped polygons) *A polygon $\mathcal{P}_n$ with vertices $A_1, \dots, A_n$ is star-shaped, if there exists a point P such that for each point Q of $\mathcal{P}_n$ the segment PQ lies entirely within $\mathcal{P}_n$ (every point of the polygon is "visible" from P).* ■

The set of all points P from which each point of $\mathcal{P}_n$ is visible is called the kernel of $\mathcal{P}_n$ and denoted by $\mathcal{K}$. The kernel $\mathcal{K}$ is divided into two parts: the interior $int(\mathcal{K})$ and boundary $\partial\mathcal{K}$. The kernel is a proper subset of $\mathcal{P}_n$ which can be obtained in the following way.

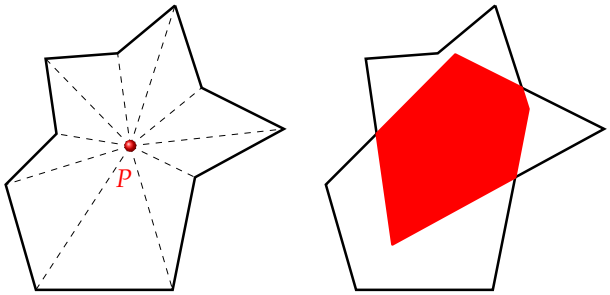


Figure 16: A star-shaped polygon (left). Its kernel is colored at right.

Each edge e of $\mathcal{P}_n$ defines two half-planes, an inner one which locally contains points of the interior of $\mathcal{P}_n$, and an outer one. The kernel of $\mathcal{P}_n$ is known to be the intersection of all inner half-planes. Each half-plane is convex and the intersection of convex sets is again convex so the intersection of n half-planes is a convex set. In particular, the kernel is convex. As another consequence, convex polygons are star-shaped, and a convex polygon coincides with its own kernel.

Lemma 3.16 *A simple polygon $\mathcal{P}_n$ with n vertices $A_1, A_2, \dots, A_n$ is star-shaped if and only if there exists a point P inside it such that*

$$\theta_{1,2} + \dots + \theta_{i,i+1} + \dots + \theta_{n-1,n} + \theta_{n,1} = 2\pi.$$

PROOF Recall that $\theta_{i,i+1} = \angle A_i P A_{i+1}$ where the index i is taken modulo n. If polygon $\mathcal{P}_n$ is star-shaped then its kernel $\mathcal{K}$ is not empty hence we can take a point P in $\mathcal{K}$. As discussed, $\mathcal{K}$ is the intersection of all inner half-planes so that every vertex of $\mathcal{P}_n$ is visible from P. In other words, rays $PA_1, PA_2, \ldots, PA_n$ lie entirely in $\mathcal{P}_n$. Thus, $\theta_{1,2} + \cdots + \theta_{i,i+1} + \cdots + \theta_{n-1,n} + \theta_{n,1} = 2\pi$. Conversely, if there exists a point P in a simple polygon $\mathcal{P}_n$ whose internal angles at P sum up to 2π then vertex of $\mathcal{P}_n$ is visible from P. Otherwise, there exists at least one vertex which is not visible from P. This situation is described in Figure 17, (A_2 is not visible from P). Hence the segment PA_2 intersects the boundary of

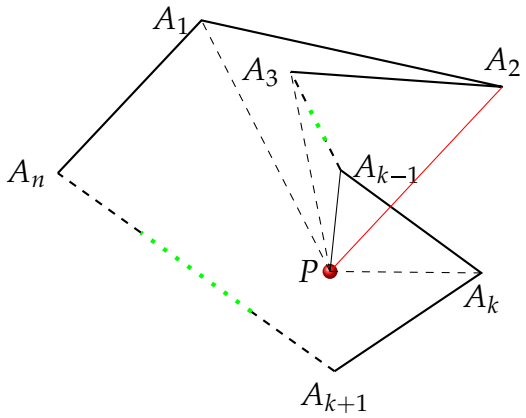


Figure 17: Illustration of a point (A_2) is not visible from P.

$\mathcal{P}_n$, say $A_{k-1}A_k$ for which $4 \leqslant k \leqslant n$. It is clear in Figure 17 that

$$\theta_{1,2} + \theta_{2,3} + \cdots + \theta_{k-1,k} > X$$

where expression X is defined as follows:

$$X = \begin{cases} \theta_{1,k} & \text{if} \quad \theta_{1,2} + \theta_{2,3} + \cdots + \theta_{k-1,k} \leqslant \pi \\ 2\pi - \theta_{1,k} & \text{if} \quad \pi < \theta_{1,2} + \theta_{2,3} + \cdots + \theta_{k-1,k} \leqslant 2\pi \end{cases} .$$

Therefore

$$\begin{aligned} &\theta_{1,2} + \theta_{2,3} + \cdots + \theta_{k-1,k} + \theta_{k,k+1} + \cdots + \theta_{n-1,n} + \theta_{n,1} \\ &> X + \theta_{k,k+1} + \cdots + \theta_{n-1,n} + \theta_{n,1} \geqslant 2\pi, \end{aligned}$$

However, it contradicts our assumption that

$$\theta_{1,2} + \theta_{2,3} + \cdots + \theta_{k-1,k} + \theta_{k,k+1} + \cdots + \theta_{n-1,n} + \theta_{n,1} = 2\pi.$$

As a result, every vertex of $\mathcal{P}_n$ is visible from P. Now take an edge A_iA_{i+1}, $1 \leqslant i \leqslant n$ and consider the triangle PA_iA_{i+1}. Since $\mathcal{P}_n$ is simple and A_i, A_j are visible from P so that no edge of $\mathcal{P}_n$ can intersect the boundary of triangle PA_iA_{i+1}. Therefore, the line segment

from P to any point on edge A_iA_{i+1} lies entirely in the triangle. Consequently, every point in triangle PA_iA_{i+1} is visible from P for every $1 \leqslant i \leqslant n$. It follows that every point in $\mathcal{P}_n$ is visible from P. We conclude that $\mathcal{P}_n$ is a star-shaped polygon and P is in its kernel. ∎

We come back to our main objective: to generalize the EM inequality for convex polygons. Using the proof of the EM inequality for convex polygons and Lemma 3.16 we have the following:

Corollary 3.17 *Let $A_1A_2\dots A_n$ be a star-shaped polygon, let $P \in int(\mathcal{K})$. Let the distances from P to the vertices A_k be p_k. Then*

$$\sum_{k=1}^{n} p_k \geqslant \frac{1}{\cos(\pi/n)} \left(\sum_{k=1}^{n-1} \boldsymbol{p}_k^{1/2} \cdot \boldsymbol{p}_{k+1}^{1/2} - \boldsymbol{p}_n^{1/2} \cdot \boldsymbol{p}_1^{1/2} \right), \tag{3.2.29}$$

equality holding if and only if for $i = 1, \dots, n$ the geometric angles $\theta_{i,i+1}$ at P, are equal. ∎

PROOF Since P lies in $int(\mathcal{K})$ of the star-shaped polygon $A_1A_2\dots A_n$ then the Lemma 3.16 ensures that the geometric angles $\theta_{i,i+1}$ at P sum up to 2π. From there, process of the proof the EM inequality for convex polygons (proof of Florian's conjecture- Conjecture 3.15) will be repeated until the condition (3.2.17) is proved then the inequality (3.2.29) is consequently proved. Afterwards, using the result of (3.2.28) gives us the geometric angles at P are equal then the proof of Corollary 3.17 follows. ∎

Corollary 3.18 (The EM inequality for star-shaped polygons) *Let $A_1A_2\dots A_n$ be a star-shaped polygon, let P be a point in its $int(\mathcal{K})$. Let the distances from P to vertices A_k be p_k and let those to sides A_kA_{k+1} be $h_{k,k+1}$, for which index k is taken modulo n. Then*

$$\sum_{k=1}^{n} p_k \geqslant \frac{1}{\cos(\pi/n)} \sum_{k=1}^{n} h_{k,k+1}, \tag{3.2.30}$$

equality holds if and only if the polygon is regular and P is its center. ∎

PROOF Recall from (3.2.15) that

$$\begin{aligned} h_{k,k+1} &\leqslant \left| \mathbf{p}_k^{1/2} \cdot \mathbf{p}_{i+1}^{1/2} \right| = \mathbf{p}_k^{1/2} \cdot \mathbf{p}_{i+1}^{1/2}, \quad k = 1, 2, \dots, n-1, \\ h_{n,1} &\leqslant \left| \mathbf{p}_n^{1/2} \cdot \mathbf{p}_1^{1/2} \right| = -\mathbf{p}_n^{1/2} \cdot \mathbf{p}_1^{1/2}. \end{aligned}$$

Therefore,

$$\sum_{k=1}^{n-1} \mathbf{p}_k^{1/2} \cdot \mathbf{p}_{k+1}^{1/2} - \mathbf{p}_n^{1/2} \cdot \mathbf{p}_1^{1/2} \geqslant \sum_{k=1}^{n} h_{k,k+1} \tag{3.2.31}$$

The above n inequalities become equalities if and only if $p_1 = p_2 = \cdots = p_n$. Hence the equality case of (3.2.31) holds if and only if $p_1 = p_2 = \cdots = p_n$.

Using corollary 3.17 and inequality (3.2.31) above we have

$$\sum_{k=1}^{n} p_k \geqslant \frac{1}{\cos(\pi/n)} \left(\sum_{k=1}^{n-1} \mathbf{p}_k^{1/2} \cdot \mathbf{p}_{k+1}^{1/2} - \mathbf{p}_n^{1/2} \cdot \mathbf{p}_1^{1/2} \right) \geqslant \frac{1}{\cos(\pi/n)} \sum_{k=1}^{n} h_{k,k+1}.$$

It proves our Corollary 3.18. ∎

We end this section with the following proposition:

Proposition 3.19 *Inequality* (3.2.30) *in Corollary 3.18 is also true when the point $P \in \partial\mathcal{K}$ of the star-shaped polygon $A_1A_2 \ldots A_n$.* ∎

PROOF We will prove this result by using Real Analysis concepts. Define a function $f : \mathcal{K} \to \mathbb{R}$ via

$$f(P) = \sum_{k=1}^{n} p_k - \frac{1}{\cos(\pi/n)} \sum_{k=1}^{n} h_{k,k+1},$$

By Corollary 3.18, we proved that

$$f(P) \geqslant 0, \quad \forall P \in int(\mathcal{K}).$$

Now our goal is showing that

$$f(P) \geqslant 0, \quad \forall P \in \partial\mathcal{K}.$$

The kernel $\mathcal{K}$ of star-shaped polygon $A_1A_2 \ldots A_n$ is convex then f is a real-valued continuous function defined on a convex set. Suppose to the contrary that we have a point $P_0 \in \partial\mathcal{K}$ and $f(P_0) < 0$. Since it is a point in boundary of a convex polygon, therefore for every $\delta > 0$ we can find a point $P_1 \in \text{Circle}(P_0, \delta)$ for which $P_1 \in int(\mathcal{K})$. On the other hand, since f is continuous on $\mathcal{K}$, for every $\epsilon > 0$ there exists some number $\delta > 0$ such that for all $P \in \text{Circle}(P_0, \delta)$ then $f(P_0) - \epsilon < f(P) < f(P_0) + \epsilon$. For sufficiently small ϵ we have $f(P) < f(P_0) + \epsilon < 0$. This means that $f(P_1) < 0$ for some $P_1 \in int(\mathcal{K})$, a contradiction. ∎

Bibliography

[1] Akira Sakurai, *Vector Analysis Proof of Erdös-Mordell Inequality for Triangles*, The American Mathematical Monthly, Vol. 119, No. 8 (October 2012), pp. 682-684.

[2] Jeremy M. Hamilton, *An Exploration of the Erdös-Mordelll inequality*, Partial Fulfillment of the Requirements for the Degree of Master of Science in the Mathematics Program, August, 2010. Available at: http://etd.ohiolink.edu/send-pdf.cgi/Hamilton%20Jeremy.pdf?ysu1287605197

[3] Marian Dinca, *A simple proof of the Erdös-Mordelll inequality for Polygons in N-dimensional spaces*.

[4] Shay Gueron and Itai Shafrir, *A Weighted Erdös-Mordelll Inequality for Polygons*, The American Mathematical Monthly, Vol. 112, No. 3 (Mar., 2005), pp. 257-263.

[5] Nicomedes Alonso III, *A Modern Application of An Acient Theorem*, Department of Mathematics and Computer Science, Dickinson State University.

[6] P. Erdös, *Problem 3740*, The American Mathematical Monthly **42** (1935) 396.

[7] L. J. Mordell and D. F. Barrow, *Solution 3740*, The American Mathematical Monthly **44** (1937) 252-254.

[8] A. Florian, Zu einem Satz von P. Erdös, Eelemente der Mathematik, 1955, pp. 55-59.

[9] D.K. Kazarinoff *A Simple Proof of the Erdös-Mordell inequality for Triangles.* Michigan Mathematical Journal 4 (1957), pp. 97-98.

[10] A. Vandanjav, B. Tserendorj, B. Undrakh,*On some weighted Erdös-Mordell type inequalities for polygons.* International Journal of Geometry Vol.1 (2012), No. 2, 15 - 21.

[11] P. Erdös, *Some combinatorial problems in geometry*, Geometry and differential geometry (Proc. Conf., Univ. Haifa, Haifa, 1979), pp. 466ÀË53, Lecture Notes in Math., 792, Springer, Berlin, 1980. .

3.3 Forbidden subgraphs of the Odd Distance Graph

Le Tien Nam

Abstract

In [1] page 252 the authors claimed that:

"...the existence of a K_4 is the only obstruction. That is, every finite K_4-free graph can be represented by odd-distances in the plane." In this article we disprove this claim by showing that the $5-$ wheel is not a subgraph of the odd-distance graph, that is it cannot be embedded in $\mathbb{R}^2$ so that vertices connected by an edge are placed in pints whise Euclidean distance is an odd integer.

3.3.1 Introduction

The odd-distance graph G^{odd} is the infinite graph whose vertices are the points of the Euclidean plane $\mathbb{R}^2$, two vertices connected by an edge if their distance is an odd integer. The "birth" of this graph happened in a conversation with P. Erdős in 1994 at the conference on Graph Theory, Combinatorics and Computation in Boca Raton, Florida. In [3] and [5] it was noted that G^{odd} does not contain K_4 as a subgraph. We asked: "what is the chromatic number of G^{odd}?" Erdős added: "How many distances among n points in the plane can be odd integers?"

Thus started the pursuit of unveiling the mysteries of G^{odd}, whose "close cousin," the unit-distance graph, has been haunting mathematicians since its introduction in 1950. Since every finite subgraph of G^{odd} is K_4-free, it follows from Turán's theorem that the maximum number of odd-distances among n points in the plane is $T(n, 4)$, the number of edges in the complete tri-partite graph on n vertices whose three partitions are "as equal as possible". L. Piepemeyer, [4] proved that this maximum is attained by showing that the complete tri-partite graph $K_{m,m,m}$ (and therefore any $K_{m,n,k}$) is a subgraph of G^{odd}.

As for the chromatic number, we believe that it is not finite, that is G^{odd} contains finite subgarphs with arbitrary chromatic number. They are waiting to be discovered. The best known lower bound is 5. A 5-chromatic subgraph of G^{odd} with 21 vertices was constructed in [**?**]. Interestingly, if we require every mono-chromatic set to be Lebesgue measurable, then it follows from a result of H. Furstenberg, Y. Katzenelson and B. Weiss, [2] that G^{odd} is not finitely measure-colorable. Using spectral techniques, J. Steinhardt [6] also proved that there is no finite measurable coloring of G^{odd}.

We believe that proving that W_5 is not a subgraph of G^{odd} will attract others to explore other forbidden subgraphs.

3.3.2 Notation and preliminary observations.

Let $\mathbb{Q}$ be the set of rational numbers, $\mathbb{N}^+$ the positive integers, $\mathbb{Z}$ the integers and $\mathbb{R}^2$ the Euclidean plane. We consider all hypothetical embeddings of W_5 in $\mathbb{R}^2$

We assume that O is at the origin and the coordinates of the points A_i are (x_i, y_i). If these figures represent W_5 in G^{odd} then we have:

$$| _i | = r_i = 1 \bmod 2 \tag{3.3.1}$$

$$| _i, A_{i+1} | = r_{i,i+1} = 1 \bmod 2 \tag{3.3.2}$$

$$\angle A_i O A_j = \theta_{i,j} \tag{3.3.3}$$

$$2(x_i x_j + y_i y_j) = 2 r_i r_j \cos\theta_{i,j} = m_{i,j} \tag{3.3.4}$$

$$m_{i,i+1} = r_i^2 + r_{i+1}^2 - | _i, A_{i+1} |^2 = 1 \bmod 8. \tag{3.3.5}$$

($m_{i,i+1} \neq 0$; all index arithmetic is done mod 5)

Definition 5 *We call six points $O, A_0, A_1, A_2, A_3, A_4$ satisfying (3.3.1) to (3.3.5) a representation of W_5.* ■

For every $0 \leqslant i < j < k \leqslant 4$, let:

$$M_{i,j,k} = 2 \begin{pmatrix} x_i & y_i \\ x_j & y_j \\ x_k & y_k \end{pmatrix} \begin{pmatrix} x_i & x_j & x_k \\ y_i & y_j & y_k \end{pmatrix} = \begin{pmatrix} m_i & m_{i,j} & m_{i,k} \\ m_{i,j} & m_j & m_{j,k} \\ m_{i,k} & m_{j,k} & m_k \end{pmatrix}$$

($m_i = 2r_i^2$). The ten matrices $M_{i,j,k}$ have rank $\leqslant 2$ so $Det(M_{i,j,k}) = 0$.
We will refer to these 10 matrices as the matrices associated with the corresponding representation of W_5.

We will show that if the ten edges of W_5 are to be odd integers at least one of these determinants is not zero, a contradiction.

3.3.3 The main result

Let $M_{i,j,k}$, $0 \leqslant i < j < k \leqslant 4$ be the matrices associated with a representation of W_5.

Lemma 3.20 *If $m_{i,i+2} \in \mathbb{Q}$ then $r_{i+1}^2 m_{i,i+2} \in \mathbb{Z}$.* ■

PROOF We first note that in all representations of W_5 we have:
$\cos\theta_{i,i+2} = \cos(\theta_{i,i+1} \pm \theta_{i+1,i+2})$. Without loss of generality, we may assume that $m_{1,3} \in \mathbb{Q}$.

$$2r_1 r_2 \sin\theta_{1,2} = \sqrt{(2r_1 r_2)^2 - (2r_1 r_2 \cos\theta_{1,2})^2} = \sqrt{(2r_1 r_2)^2 - m_{1,2}^2}$$

Similarly, $\quad 2r_2 r_3 \sin\theta_{2,3} = \sqrt{(2r_2 r_3)^2 - m_{2,3}^2}$

$$2r_2^2 m_{1,3} = (2r_2^2)2r_1r_3\cos(\theta_{1,2} \pm \theta_{2,3})$$
$$= (2r_1r_2\cos\theta_{1,2})(2r_2r_3\cos\theta_{2,3}) \mp (2r_1r_2\sin\theta_{1,2})(2r_2r_3\sin\theta_{2,3})$$
$$= m_{1,2}m_{2,3} \mp \sqrt{\{(2r_1r_2)^2 - m_{1,2}^2\}\{(2r_2r_3)^2 - m_{2,3}^2\}} \in \mathbb{Q} \tag{3.3.6}$$
$$\implies \sqrt{\{(2r_1r_2)^2 - m_{1,2}^2\}\{(2r_2r_3)^2 - m_{2,3}^2\}} \in \mathbb{N}^+ \tag{3.3.7}$$

Since the square root of an integer is either an integer or irrational.

$$r_i \bmod 2 = m_{i,i+1} \bmod 2 = 1 \implies (2r_ir_{i+1})^2 - m_{i,i+1}^2 = -1 \bmod 4$$
$$\implies \{(2r_1r_2)^2 - m_{1,2}^2\}\{(2r_2r_3)^2 - m_{2,3}^2\} = 1 \bmod 4 \tag{3.3.8}$$

From (3.3.7),(3.3.8): $\sqrt{\{(2r_1r_2)^2 - m_{1,2}^2\}\{(2r_2r_3)^2 - m_{2,3}^2\}} = 1 \bmod 2.$

Thus, $m_{1,2}m_{2,3} \mp \sqrt{\{(2r_1r_2)^2 - m_{1,2}^2\}\{(2r_2r_3)^2 - m_{2,3}^2\}} = 0 \bmod 2.$

From (3.3.6) we get: $2r_2^2 m_{1,3} = 0 \bmod 2 \implies r_2^2 m_{1,3} \in \mathbb{Z}$ ∎

Corollary 3.21 *If there exists a representation of W_5 in $\mathbb{R}^2$ such that some $m_{i,i+2}$ are rational and some are irrational, then there exists a representation of W_5 such that all rational $m_{i,i+2}$ will be integers.* ∎

PROOF Let $O, A_1, A_2, A_3, A_4, A_5$ be the vertices of W_5 embedded in $\mathbb{R}^2$ and $m_{i,j}$ be its corresponding entries in the matrix M (see (3.4.2)).

Let $\alpha = (r_1r_2r_3r_4r_5)^2$. Then it follows from Lemma 3.20 that $O, \alpha A_1, \ldots, \alpha A_5$ is a representation of W_5 such that if $m_{i,j} \in \mathbb{Q},\ j = i+1, i+2$ then the corresponding $m'_{i,j}$ for this representation are integers. Since α is odd, all original odd-distances will remain odd in the new stretched representation. ∎

Lemma 3.22 *Let $O, A_0, \ldots, A_4$ be a representation of W_5. Assume that for some i, $m_{i,i+2} \in \mathbb{Z}$. Then*

$$m_{i,i+2} = 2 \text{ or } 3 \bmod 4$$

PROOF Without loss of generality, assume that $m_{1,3} \in \mathbb{Z}$.

Hence all entries in the matrix $M = \begin{pmatrix} m_1 & m_{1,2} & m_{1,3} \\ m_{1,2} & m_2 & m_{2,3} \\ m_{1,3} & m_{2,3} & m_3 \end{pmatrix}$ are integers.

$Det(M) = 0 \implies Det(M) \bmod 8 = 0.$

$$M \bmod 8 = \begin{pmatrix} 2 & 1 & m_{1,3} \\ 1 & 2 & 1 \\ m_{1,3} & 1 & 2 \end{pmatrix} \bmod 8$$

So $m_{1,3}$ is the root of the equation $2m_{1,3}^2 - 2m_{1,3} - 4 = 0 \bmod 8$ and therefore $m_{1,3} = 2$ or $3 \bmod 4$. ∎

Lemma 3.23 *If for some i, $m_{i,i+2} \notin \mathbb{Q}$ then for $i = 0, 1, 2, 3, 4$, $m_{i,i+2} \notin \mathbb{Q}$. In other words, either all five entries $m_{i,i+2}$ are rational or all are irrational.* ∎

PROOF Without loss of generality, assume that $m_{1,3} \notin \mathbb{Q}$.
$Det(M_{1,2,3}) = 0$ implies that $m_{1,3}$ is a root of the quadratic equation:

$$ax^2 + bx + c = 0$$

$a = m_2,\ b = -2m_{1,2}m_{2,3},\ c = -m_1m_2m_3 + m_{1,2}^2m_3 + m_1m_{2,3}^2,\ a, b, c \in \mathbb{Z}$.

$$m_{1,3} = \frac{2m_{1,2}m_{2,3} \pm \sqrt{b^2 - 4ac}}{2m_2} = s + p\sqrt{q} \tag{3.3.9}$$

Where $s = \frac{2m_{1,2}m_{2,3}}{2m_2} = 2r_1r_3 \cos\theta_{1,2} \cos\theta_{2,3},\ p, q \in \mathbb{Q}$ and $m_{1,3} \notin \mathbb{Q}$
$\Longrightarrow \sqrt{q} \notin \mathbb{Q}$.
Also, since $s = \frac{2m_{1,2}m_{2,3}}{2m_2}$ and $m_{1,2}, m_{2,3} \neq 0$ (see (3.3.5)) $s \neq 0$.

On the other hand, we have (see (3.4.2)):

$$m_{1,3} = 2r_1r_3 cos\theta_{1,3} = 2r_1r_3(\cos\theta_{1,2} \cos\theta_{2,3} \mp \sin\theta_{1,2} \sin\theta_{2,3}) \tag{3.3.10}$$

Comparing (3.3.9) and (3.3.10) we get:

$$p\sqrt{q} = \pm 2r_1r_3 \sin\theta_{1,2} \sin\theta_{2,3} \Longrightarrow \frac{\sqrt{q}}{\sin\theta_{1,2} \sin\theta_{2,3}} \in \mathbb{Q} \tag{3.3.11}$$

Assume that $m_{3,5} = m_{3,0} \in \mathbb{Q}$. By Corollary 3.20 we may assume that $m_{3,0} \in \mathbb{Z}$.

$$Det(M_{1,3,0}) = m_1m_3m_0 - m_1m_{3,0}^2 - m_{1,3}^2m_0 + 2m_{1,0}m_{1,3}m_{3,0} - m_3m_{1,0}^2 = 0$$
$$m_{3,0} \in \mathbb{Q} \Longrightarrow -m_0m_{1,3}^2 + 2m_{1,3}m_{1,0}m_{3,0} \in \mathbb{Q}$$

$$m_{1,3} = s + p\sqrt{q} \Longrightarrow -m_0(s + p\sqrt{q})^2 + 2(s + p\sqrt{q})m_{3,0}m_{1,0} \in \mathbb{Q}$$
$$\Longrightarrow -2m_0sp\sqrt{q} + 2m_{0,3}m_{1,0}p\sqrt{q} \in \mathbb{Q}\ (\sqrt{q} \notin \mathbb{Q}) \Longrightarrow m_0s = m_{0,3}m_{0,1}$$
$$2r_2^2s = m_{1,2}m_{2,3} = 1 \bmod 8 \Longrightarrow 2r_2^2sm_0 = 2 \bmod 8 \tag{3.3.12}$$

By Lemma 3.22, $m_{0,3} = 2$ or $3 \bmod 4 \Longrightarrow 2r_2^2m_{0,3}m_{0,1} = 4$ or $6 \bmod 8$, contradicting to (3.3.12). Hence $m_{0,3} \notin \mathbb{Q}$. ∎

Remark 2 *When $m_{i,i+2}$ is irrational we let $m_{i,i+2} = s_{i,i+2} + p_{i,i+2}\sqrt{q_{i,i+2}}$ where $s_{i,i+2}, p_{i,i+2}, q_{i,i+2} \in \mathbb{Q}$ $(s_{i,i+2}, p_{i,i+2}, q_{i,i+2} \neq 0)$.* ∎

Corollary 3.24 *From (3.3.11), if $m_{i,i+2} \notin \mathbb{Q}$ then:*

$$\frac{\sqrt{q_{i,i+2}}}{\sin\theta_{i,i+1}\sin\theta_{i+1,i+2}} \in \mathbb{Q} \tag{3.3.13}$$

■

Lemma 3.25 *If $a, b \in \mathbb{Q}$, $\sqrt{a}, \sqrt{b} \notin \mathbb{Q}$ and there are rational numbers x, y, z, w not all zero, such that $x\sqrt{a} + y\sqrt{b} + z\sqrt{ab} = w$ then $\sqrt{ab} \in \mathbb{Q}$.* ■

PROOF

$$x\sqrt{a} + y\sqrt{b} + z\sqrt{ab} = w \implies x\sqrt{a} + y\sqrt{b} = w - z\sqrt{ab} \tag{3.3.14}$$

$$\begin{aligned}(x\sqrt{a} + y\sqrt{b})(x\sqrt{a} - y\sqrt{b}) &= x^2a - y^2b = (w - z\sqrt{ab})(x\sqrt{a} - y\sqrt{b}) \\ &= (wx + zyb)\sqrt{a} - (wy + zxa)\sqrt{b} \\ &= h_1\sqrt{a} + h_2\sqrt{b} = h_3 \ (h_i \in \mathbb{Q}). \qquad (3.3.15)\end{aligned}$$

$$(h_1\sqrt{a} + h_2\sqrt{b})(h_1\sqrt{a} - h_2\sqrt{b}) = ah_1^2 - bh_2^2 = h_3(h_1\sqrt{a} - h_2\sqrt{b}) \in \mathbb{Q}$$

If $h_3(h_1\sqrt{a} - h_2\sqrt{b}) \neq 0$ then $h_1\sqrt{a} - h_2\sqrt{b} \in \mathbb{Q}$
Combining this with (3.3.15) we get: $\sqrt{a} \in \mathbb{Q}$, a contradiction.

$$h_3(h_1\sqrt{a} - h_2\sqrt{b}) = 0 \implies (w - z\sqrt{ab})(x\sqrt{a} - y\sqrt{b}) = 0$$

- If $w - z\sqrt{ab} \neq 0$ then $x\sqrt{a} - y\sqrt{b} = 0$ and $x, y \neq 0$.
  $(x\sqrt{a} - y\sqrt{b})\sqrt{b} = x\sqrt{ab} - yb \implies \sqrt{ab} \in \mathbb{Q}$
- If $w - z\sqrt{ab} = 0$ and $z \neq 0$ then $\sqrt{ab} \in \mathbb{Q}$
- If $w - z\sqrt{ab} = 0$ and $z = 0$ then $w = 0 \implies x\sqrt{a} + y\sqrt{b} = 0$
  By the assumptions $x, y \neq 0 \implies xa + y\sqrt{ab} = 0 \implies \sqrt{ab} \in \mathbb{Q}$ ■

We are now ready to prove the main theorem:

Theorem 3.26 *W_5 is not a subgraph of G^{odd}.* ■

PROOF Suppose by contradiction that W_5 is a subgraph of G^{odd} and let M be the M-matrix of the given realization of W_5. We have two cases:

1. $m_{1,3} \in \mathbb{Q}$
2. $m_{1,3} \notin \mathbb{Q}$.

In case 1, by Lemma 3.23, $m_{i,i+2} \in \mathbb{Q}$ $\forall i$. By Corollary 3.20, we may assume that $m_{i,i+2} \in \mathbb{Z}$ $\forall i$. By Lemma 3.22, $m_{i,i+2} = 2$ or $3 \bmod 4$.

As we have five integers $m_{i,i+2}$ and each can be either 2 or 3 mod 4 there must be an index i for which $m_{i,i+2} = m_{(i+3)+2,i+3} = m_{i,i+3} \bmod 4$.

Without loss of generality, assume that $m_{1,4} = m_{1,3} \bmod 4$. Assume first that $m_{1,3} = m_{1,4} = 2 \bmod 4$.

$$M_{3,4,1} = \begin{pmatrix} 2 & 1 & 2 \\ 1 & 2 & 2 \\ 2 & 2 & 2 \end{pmatrix} \bmod 4 \quad Det(M_{3,4,1}) \bmod 4 = 2.$$

Similarly, if $m_{1,3} = m_{1,4} = 3 \bmod 4 = 3$ or $7 \bmod 8$ we have up to symmetry, three possibilities:

1. $m_{1,3} = m_{1,4} = 3 \bmod 8$
2. $m_{1,3} = m_{1,4} = 7 \bmod 8$
3. $m_{1,3} = 3 \bmod 8,\ m_{1,4} = 7 \bmod 8.$

In the first case $M_{3,4,1} = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & 3 \\ 3 & 3 & 2 \end{pmatrix}$ $\quad Det(M_{3,4,1}) = -12 = 4 \bmod 8.$

It is easy to check that for the other two cases $Det(M_{3,4,1}) = 4 \bmod 8$, as well. In each case we found a matrix $M_{i,j,k}$ with non-zero determinant. Hence it is not possible to realize W_5 so that $m_{i,j}$ are rational.

In case 2, assume now that $m_{1,3} \notin \mathbb{Q}$. By Lemma 3.23, $m_{i,i+2} \notin \mathbb{Q}\ \forall i$. We will show that $Det(M_{1,3,4}) \neq 0$.

Claim: $\sin\theta_{i,i+1} \sin\theta_{i+2,i+3} \in \mathbb{Q}$.

To simplify notation, we will prove the claim for $i = 1$. It will be obvious from the proof that the same steps will be valid for all i.

$$M_{1,3,4} = \begin{pmatrix} m_1 & m_{1,3} & m_{1,4} \\ m_{1,3} & m_3 & m_{3,4} \\ m_{1,4} & m_{3,4} & m_4 \end{pmatrix}$$

$Det(M_{1,3,4}) = m_1 m_3 m_4 - m_1 m_{3,4}^2 - m_{1,3}^2 m_4 + 2 m_{1,3} m_{1,4} m_{3,4} - m_{1,4}^2 m_3 = 0.$

Substituting for $m_{1,3}$ and $m_{1,4}$ we get:

$$m_1 m_3 m_4 - m_1 m_{3,4}^2 - (s_{1,3} + p_{1,3}\sqrt{q_{1,3}})^2 m_4 +$$
$$2(s_{1,3} + p_{1,3}\sqrt{q_{1,3}})(s_{1,4} + p_{1,4}\sqrt{q_{1,4}}) m_{3,4} - (s_{1,4} + p_{1,4}\sqrt{q_{1,4}})^2 m_3 = 0$$

Expanding and collecting separately the rationals and irrationals we get:

$$\alpha + \beta\sqrt{q_{1,3}} + \gamma\sqrt{q_{1,4}} + \mu\sqrt{q_{1,3}q_{1,4}} = 0 \ (\alpha, \beta, \gamma, \mu \in \mathbb{Q},\ \mu = 2p_{1,3}p_{1,4}m_{3,4} \neq 0)$$

From Lemma 3.25, $\sqrt{q_{1,3}q_{1,4}} \in \mathbb{Q}$. Similarly, $\sqrt{q_{4,4+2}q_{4,4+3}} = \sqrt{q_{1,4}q_{2,4}} \in \mathbb{Q}$
$\implies \sqrt{q_{1,3}q_{1,4}}\sqrt{q_{1,4}q_{2,4}} = q_{1,4}\sqrt{q_{1,3}q_{2,4}} \in \mathbb{Q} \implies \sqrt{q_{1,3}q_{2,4}} \in \mathbb{Q}$.

From Corollary 3.24 we get:

$$\frac{\sqrt{q_{1,3}}}{\sin\theta_{1,2}\sin\theta_{2,3}} \text{ and } \frac{\sqrt{q_{2,4}}}{\sin\theta_{2,3}\sin\theta_{3,4}} \in \mathbb{Q} \implies \frac{\sqrt{q_{1,3}q_{2,4}}}{\sin\theta_{1,2}\sin^2\theta_{2,3}\sin\theta_{3,4}} \in \mathbb{Q}$$

$$m_{i,i+1} = 2r_i r_{i+1}\cos\theta_{i,i+1} \in \mathbb{Z} \implies \sin^2\theta_{i,i+1} \in \mathbb{Q} \tag{3.3.16}$$

$$\implies \sin\theta_{1,2}\sin\theta_{3,4} \in \mathbb{Q} \tag{3.3.17}$$

This proves the **claim**.

Using (3.3.17) we have:

$$\sin\theta_{1,2}\sin\theta_{3,4} \text{ and } \sin\theta_{3,4}\sin\theta_{0,1} \in \mathbb{Q} \implies \sin\theta_{0,1}\sin\theta_{3,4}^2\sin\theta_{1,2} \in \mathbb{Q}$$

From (3.3.16), $\sin\theta_{3,4}^2 \in \mathbb{Q} \implies \sin\theta_{0,1}\sin\theta_{1,2} \in \mathbb{Q}$

From Corollary 3.24, we have:

$$\frac{\sqrt{q_{0,2}}}{\sin\theta_{0,1}\sin\theta_{1,2}} \in \mathbb{Q} \implies \sqrt{q_{0,2}} \in \mathbb{Q} \implies m_{0,2} \in \mathbb{Q}$$

This contradicts Lemma 3.23; hence $Det(M_{1,3,4}) \neq 0$ and W_5 is not a subgraph of G^{odd}. ∎

Concluding remarks: Since every 3-colorable graph is a subgraph of G^{odd} all even wheels W_{2k} are subgraphs of G^{odd}. This leads us to ask whether $W_{2k+1}, k > 2$ are not subgraphs of G^{odd}, also are there triangle free graphs that are not subgraphs of G^{odd}?

Bibliography

[1] Brass, P., Moser, W., Pach, J., Research problems in discrete geometry, Springer–Verlag (2005) 234–244.

[2] H. Furstenberg, Y. Katznelson, and B. Weiss: Ergodic theory and configurations in sets of positive density, Mathematics of Ramsey theory, 184–198, Algorithms Combin., **5**, Springer, Berlin, 1990.

[3] R. Graham, B. Rothschild, E. Strauss:Are there n+2 points in E^n with odd integral distances? Am. Math. Month. **81**, 21-25, (1974).

[4] L. Piepemeyer: The maximum number of odd integral distances between points in the plane, Discrete Comput. Geom. **16** (1996) 156-159.

[5] M. Rosenfeld: The Odd-Distance Plane Graph, Geombinatorics, Vol. XIX (2) 2009, pp. 62-66.

[6] J. Steinhardt: On Coloring the Odd-Distance Graph, Electronic J. of Combinatorics **16** (2009) #N12

3.4 All 3-Colorable Graphs have a faithful representation in $\mathbb{G}(\mathbb{R}^2, \{odd\})$

Le Tien Nam

Abstract

We prove that every finite $3-$ colorable graph has an odd-distance faithful representation in the plane. In other words, we can draw it in the plane so that any two vertices are connected by an edge if and only if their distance is an odd integer.

Keywords: integral-distance graphs, odd-distance graph, faithful representation.

3.4.1 Introduction

The integral-distance graphs in the plane $\mathbb{G}(\mathbb{R}^2, \mathbf{D})$, are graphs whose vertices are points in the Euclidean plane $\mathbb{R}^2$, two vertices are connected by an edge if their distance is in $\mathbf{D} \subset \mathbb{R}^+$. The integral-distance graph $\mathbb{G}(\mathbb{R}^2, \mathbb{N})$ the unit-distance graph $\mathbb{G}(\mathbb{R}^2, \{1\})$ and the odd-distance graph $\mathbb{G}(\mathbb{R}^2, \{1, 3, 5, \ldots\})$ are three better known examples of such graphs.

It is known that every finite simple graph is a subgraph of the integral-distance graph even with various restrictions [3, 4].

Definition 3.27 *We say that a graph $\mathbb{G}$ has a **faithful representation** in an integral-distance graph $\mathbb{G}(\mathbb{R}^2, \mathbf{D})$ if two vertices are connected by edge **if and only if** their distance is in $\mathbf{D}$.* ■

In 1997, Maehara et al. [5] proved that every finite simple graph has a faithful representation in the integral-distance graph. However, the odd-distance graph, still hides many mysteries. Its only known subgraphs are all $3-$colorable graphs (see [9]), all subgraphs of the triangular lattice, the rational points, the unit distance graph and a few subgraphs with higher chromatic numbers (up to 5) (see [7]). In the book [1] the authors erroneously stated that the complete graph K_4 is the only forbidden subgraph of $\mathbb{G}(\mathbb{R}^2, \{odd\})$; this was disproved in [8] where it was proved that the $5-$wheel is another forbidden subgraph of the odd-distance graph.

Piepemeyer proved that $K_{n,n,n}$ is a subgraph of the the odd distance graph. This of course implies that every $3-$colorable graph is a subgraph of the odd distance graph. In 2012 Stéphan Thomassé asked whether every bipartite graph has a faithful representation in $\mathbb{G}(\mathbb{R}^2, \{1, 3, 5, \ldots\})$. In this paper we prove a stronger claim: every $3-$colorable graph has a faithful representation in $\mathbb{G}(\mathbb{R}^2, \{1, 3, 5, \ldots\})$.

The proof first constructs a representation of $K_{r,b,g}$ in $\mathbb{G}(\mathbb{R}^2, \{odd\})$ as follows:

Let $\mathbb{G}(V, E)$ be a 3−colorable graph with n vertices. Assume that $v_1, v_2, \ldots, v_r$ are the red colored vertices, $u_1, \ldots u_b$ the blue and $w_1, \ldots w_g$ the green colored vertices ($r + b + g = n$). Starting with an equilateral triangle with sides 1 inscribed in a circle, we partition its circumference into three equal arcs. In one arc we place r points, in the second b points and g points in the third. The points will be placed so that the distance between two points belonging to different arcs is a rational number $\frac{p}{q}$ with p, q odd while the distance between two points belonging to the same arc is a rational $\frac{t}{m}$ where m is odd and t is even.

By blowing this circle by the least common multiple of all denominators, we obtain an embedding of the complete 3−partite graph $K_{r,b,g}$ in the odd distance graph. We note that this is a different representation than Piepemeyer's . It is a *canonical* representation in the sense that each of the three mono-chromatic sets of vertices are grouped together in a single arc. As an aside, we also get an embedding of the complete graph K_n in $\mathbb{G}(\mathbb{R}^2, \mathbb{N})$. This gives another construction for an integral set in the plane that maximizes the number of odd distances among them.

We then show that for every subset of edges, we can "blow" the circle so that only the length of these edges will be odd integers.

An embedding of $K_{r,b,g}$ in the odd-distance graph.

Let $A_0A_1A_2$ be an equilateral triangle of side 1, inscribed in a circle. Let $P_0[x, y]$ denote points selected on the arc $\overset{\frown}{A_0, A_1}$, $P_1[s, t]$ points on the arc $\overset{\frown}{A_1, A_2}$ and $P_2[u, v]$ points on the arc $\overset{\frown}{A_2, A_0}$ as shown in Figure 1.

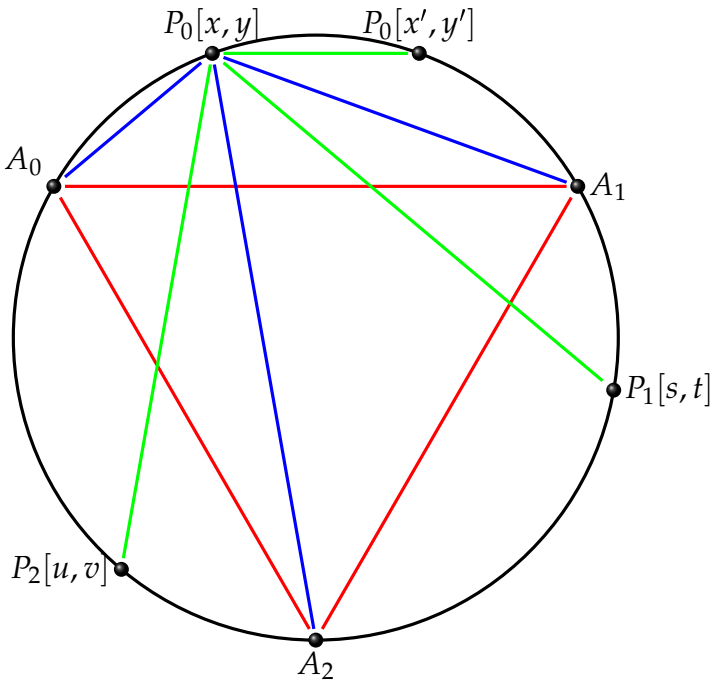


Figure 1.

We note that $\angle A_iP_i[x,y]A_{i+1} = \frac{2\pi}{3}$ $i = 0,1,2, (A_3 = A_0)$. Hence by the cosine law we have:

$$\| A_iP_i[x,y] \|^2 + \| P_i[x,y]A_{i+1} \|^2 + \|A_iP_i[x,y] \| \cdot \| P_i[x,y]A_{i+1} \| = 1 \qquad (3.4.1)$$
$$i = 0,1,2$$

Once the points $P_i[x,y]$ are selected we can calculate all distances among them using the cosine law or Ptolmey's theorem:

Theorem 3.28 (Ptolmey) *If A, B, C, D are the vertices of a quadrangle inscribed in a circle then:*

$$\| AB \| \cdot \| CD \| + \| BC \| \cdot \| AD \| = \| AC \| \cdot \| BD \| . \qquad \blacksquare$$

Applying Ptolmey's theorem to the quadrilaterals containing A_0, A_1, A_2 and $P_i[x,y]$ we get:

$$\begin{aligned} &\| A_2P_0[x,y] \| = \| A_0P_0[x,y] \| + \| P_0[x,y]A_1 \| \\ &\| A_0P_1[u,w]) \| = \| A_1P_1[u,w] \| + \| P_1[u,w]A_2 \| \\ &\| A_1P_2[s,t] \| = \| A_2P_2[s,t] \| + \| P_2[s,t]A_0 \| . \end{aligned} \qquad (3.4.2)$$

Let $P_i[a,b]$ be selected such that:

$$\| A_iP_i[a,b] \| = \frac{4ab}{a^2+3b^2}; \qquad a > 3b > 0; \qquad a^2 + 3b^2 \equiv 1 \bmod 2 \qquad (3.4.3)$$

Applying the cosine law to the triangles $\Delta A_iP_iA_{i+1}$ we get:

$$\| P_i[a,b]A_{i+1} \| = \frac{(a+b)(a-3b)}{a^2+3b^2}$$

(we beg the reader to believe us that $(\frac{4ab}{a^2+3b^2})^2 + \frac{4ab}{a^2+3b^2} \cdot \frac{(a+b)(a-3b)}{a^2+3b^2} + (\frac{(a+b)(a-3b}{a^2+3b^2})^2 = 1$; alternatively he is invited to verify it).

Applying Ptolmey's theorem to the quadrilaterals $A_iP_i[a,b]P_i[c,d]A_{i+1}$ we get:

$$\| P_i[a,b]P_i[c,d] \| = \| A_iP_i[c,d] \| \cdot \| A_{i+1}P_i[a,b] \| - \| A_iP_i[a,b] \| \cdot \| A_{i+1}P_i[c,d] \| =$$
$$\frac{4cd}{c^2+3d^2} \cdot \frac{(a+b)(a-3b)}{a^2+3b^2} - \frac{4ab}{a^2+3b^2} \cdot \frac{(c+d)(c-3d)}{c^2+3d^2} = \frac{4k}{(a^2+3b^2)(c^2+3d^2)} \qquad (3.4.4)$$

We next calculate the distances between points lying in different arcs.

In order to apply Ptolmey's theorem to the quadrilateral $P_0[a,b]A_1P_1[c,d]A_2$ we first need to calculate $\| A_2P_0[a,b] \|$:

From (3.4.2) we have: $\| A_2P_0[a,b] \| = \frac{4ab}{a^2+3b^2} + \frac{(a+b)(a-3b)}{a^2+3b^2} = \frac{(a-b)(a+3b)}{a^2+3b^2}$.

$$\| P_0[a,b]P_1[c,d] \| = \| P_0[a,b]A_1 \| \cdot \| P_1[c,d]A_2 \| + \| A_1P_1[c,d] \| \cdot \| A_2P_0[a,b] \| = \tag{3.4.5}$$

$$\frac{(a+b)(a-3b)}{a^2+3b^2} \cdot \frac{(c+d)(c-3d)}{c^2+3d^2} + \frac{4cd}{c^2+3d^2} \cdot \| A_2P_0(a,b) \| = \frac{(a+b)(a-3b)(c+d)(c-3d) + 4cd(a^2+2ab-3b^2)}{(a^2+3b^2)(c^2+3d^2)}$$

We get similar expressions for the distances $\| P_0[a,b]P_2[e,f] \|$ and $\| P_1[c,d]P_2[e,f] \|$.

Conclusion: If we select points $P_i[x,y]$ on the three arcs with distances from A_0, A_1, A_2 following (3.4.3), we obtain n points on the unit circle, the distances between points belonging to the same arc are $\frac{s}{t}$, with s even and t odd; the distances between points belonging to distinct arcs are also rational $\frac{k}{m}$, k and m are both odd.

If we blow the circle by the least common multiple of all denominators, which is an odd integer, we obtain an embedding of the complete 3−partite graph $K_{r,b,g}$ in the odd-distance graph. We also obtain an embedding of K_n in the integral distance graph with all points on a single circle.

This construction is different from the construction in Piepemeyer's paper [9]. It clearly highlights the 3 mono-chromatic partitions of $K_{r,b,g}$.

3.4.2 The ring of Eisenstein integers.

In this section we explore properties of Eisenstein integers that will help us select the parameters (a_k, b_k) of our n points $P_i[a_k, b_k]$ in preparation for the final "blow-up" of the circle that will yield the faithful embedding.

Let $\omega = e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{-3}}{2}$ (a cubic root of unity). The Eisenstein ring $\mathbb{Z}[w] = \{a + b\omega \mid a, b \in \mathbb{N}\}$ is a Euclidean domain, with unique factorization. The norm of $z = a + b\omega$ is $z \cdot \overline{z} = a^2 - ab + b^2$.

Prime numbers are not necessarily Eisenstein primes. For instance, $7 = (2+\sqrt{-3})(2-\sqrt{-3})$ but all primes $p = 2 \bmod 3$ are Eisenstein primes. We also note that every prime $p \equiv 1 \bmod 3$ can be represented as $p = a^2 + 3b^2 = (a + b\sqrt{-3})(a - b\sqrt{-3})$ hence they are not Eisenstein primes; also by Dirichlet's theorem the arithmetic progression $\{3k+1\}$ contains infinitely many primes. For each such prime p we have: $p = u^2 + 3v^2$ (see the article Representing primes of the form $a^2 + kb^2$). On the other hand, $p = \mid a + b\omega \mid^2 = a^2 - ab + b^2$. Solving for a, b we get $a = u + v,\ b = 2v$, hence the set $P_3 = \{z = a + b\sqrt{-3} \mid a, b \in Z^+, a^2 + 3b^2$ is prime $\}$ is an infinite set of Eisenstein primes.

Let $\beta_{i,j} \in P_3 \mid 1 \leqslant i < j \leqslant m$ be $\binom{m}{2}$ pairwise relatively prime Eisenstein integers such that

all $\mid \beta i,j \mid^2$ are different integers and let $\alpha_{i,j} = \beta_{i,j}^{r_{i,j}}$ [14].
Let:

$$z_i = \prod_{k=1}^{i-1} \alpha_{k,i} \prod_{k=i+1}^{m} \overline{\alpha_{i,k}} = a_i + b_i\sqrt{-3}.$$

$\{z_i\}$ is a set of m Eisenstein integers; each is a product of $m-1$ Eisenstein integers. It is easy to see that each $\alpha_{i,j}$ and each $\overline{\alpha_{i,j}}$ are factors in exactly one number z_i and both are not a factor of the same z_i.

$$z_i \cdot z_j = \mid \alpha_{i,j}^2 \mid \cdot \prod_{k=1}^{i-1} \alpha_{k,i}\alpha_{k,j} \prod_{k=i+1}^{j-1} \overline{\alpha_{i,k}}\alpha_{k,j} \prod_{k=j+1}^{m} \overline{\alpha_{j,k}\alpha_{i,k}}.$$

We note that $z_i \cdot z_j$ is divisible by $\mid \alpha_{i,j}^2 \mid$ but to any other $\alpha_{i',j'}$ it is relatively prime if $\{i,j\} \cap \{i',j'\} = \varnothing$ and is not divisible by $\mid \alpha_{i'j'} \mid^2$ otherwise.

Let:

$$S_{i,j} = \cap_{k=1}^{m}\{\{i,k\},\{k,j\}\}\backslash\{\{i,j\}\}.$$

$$P_{i,j} = \frac{1}{(a_i^2+3b_i^2)(a_j^2+3b_j^2)} = \frac{1}{\mid z_i \cdot z_j \mid^2} = \frac{1}{\mid \alpha_{i,j} \mid^4 \cdot \prod_{\{i',j'\}\in S_{i,j}} \mid \alpha_{i',j'} \mid^2}.$$

Conclusion 3.29 *Let:*

$$M \subset \{(i,j),\ 1 \leqslant i < j \leqslant m\} \text{ and } A_M = \prod_{\{i,j\}\in M} \mid \alpha_{i,j}^4 \mid \prod_{\{i,j\}\notin M} \mid \alpha_{i,j} \mid^2$$

Then $\frac{A_M}{|z_i\cdot z_j|^2}$ *is an odd integer if and only if* $(i,j) \in M$. ∎

PROOF Assume that $(i,j) \notin M$. Note that:

$$(a_i^2+3b_i^2)(a_j^2+3b_j^2) = \mid \alpha_{i,j} \mid^4 \cdot \prod_{\{i',j'\}\in S_{i,j}} \mid \alpha_{i',j'} \mid^2 .$$

Since $(i,j) \notin M$ we have:

$$\frac{A_m}{(a_i^2+3b_i^2)(a_j^2+3b_j^2)} = \frac{\prod_{\{m,n\}\in M} \mid \alpha_{n,m} \mid^4 \cdot \prod_{\{m,n\}\notin M} \mid \alpha_{n,m} \mid^2}{\mid \alpha_{i,j} \mid^4 \cdot \prod_{\{i',j'\}\in S_{i,j}} \mid \alpha_{i',j'} \mid^2} = \tag{3.4.6}$$

$$\frac{\prod_{\{m,n\}\in M} \mid \alpha_{n,m} \mid^4 \cdot \prod_{\{m,n\}\notin M\cup S_{i,j}\cup\{\{i,j\}\}} \mid \alpha_{n,m} \mid^2}{\mid \alpha_{i,j} \mid^2}. \tag{3.4.7}$$

Since all $\alpha_{i,j}$ are pairwise relatively prime this fraction is not an integer.

[14] The exponents $r_{i,j}$ will be dealt with later

On the other end, when $\{i,j\} \in M$:

$$\frac{A_m}{(a_i^2+3b_i^2)(a_j^2+3b_j^2)} = \left(\prod_{\{m,n\}\in M} \mid \alpha_{n,m} \mid^4 \cdot \prod_{\{m,n\}\notin M} \mid \alpha_{n,m} \mid^2\right) \Big/ \left(\mid \alpha_{i,j} \mid^4 \cdot \prod_{\{i',j'\}\in S_{i,j}} \mid \alpha_{i',j'} \mid^2\right)$$

$$= \prod_{\{m,n\}\in M\setminus\{\{i,j\}\}} \mid \alpha_{n,m} \mid^4 \cdot \prod_{\{m,n\}\notin M\cup S_{i,j}\cup\{\{i,j\}\}} \mid \alpha_{n,m} \mid^2 .$$

Since all $\mid \alpha_{i,j} \mid^2$ are odd integers this is an odd integer. ∎

Before proving our main theorem we need to choose the exponents. Our goal is to choose them so that for $z_i = a_i + b_i\sqrt{-3}, \quad a_i > 3b_i$.

Lemma 3.30 *Let $m > 3$ be a fixed integer. We can choose the Eisenstein integers $\alpha_{i,j}$ such that* $\arg(\alpha_{i,j}) < \frac{1}{(m-1)\sqrt{3}}$. ∎

PROOF Let $\mathbb{Z}_1 = \{z \in P_1 \mid \ arg(z) \neq \frac{h\pi}{12}\}$. There are infinitely many such Eisenstein primes. Let $z = a + b\sqrt{-3}$, $\arg z = \arctan\frac{b\sqrt{3}}{a} = \theta$. We have:

$$\sqrt{3}\tan\theta = 3b/a \in \mathbb{Q} \Longrightarrow \tan^2\theta \in \mathbb{Q} \ \Longrightarrow \cos(2\theta) = (1-\tan^2\theta)/(1+\tan^2\theta) \in \mathbb{Q}\,.$$

If $2\theta \neq h\pi/6$ and $\cos(2\theta) \in \mathbb{Q}$, then θ is irrational. Thus, we can choose the exponent l such that $\mid \arg(z^l) \mid = \mid l\cdot\theta \mid \bmod 2\pi < \frac{1}{(m-1)\sqrt{3}}$. ∎

Corollary 3.31 *For $z_i = a_i + b_i\sqrt{-3}$, $a_i > 3b_i$.* ∎

PROOF

$$z_i = \prod_{k<i}(\alpha_{k,i} + \sqrt{-3}) \cdot \prod_{k>i}(\alpha_{i,k} - \sqrt{-3}) = a_i + b_i\sqrt{-3} \quad i = 1,\ldots,n.$$

By Lemma 3.30

$$\mid \arg(z_i) \mid = \mid \sum_{k\neq i} \arg(\alpha_{i,k}) \mid < \frac{m-1}{(m-1)}\sqrt{3} = \frac{1}{\sqrt{3}}.$$

So $\arg(a_i + b_i\sqrt{-3}) = \frac{b_i\sqrt{3}}{a_i} < \frac{1}{\sqrt{3}} \Longrightarrow a_i > 3b_i$. ∎

3.4.3 The Main Theorem

Theorem 3.32 *Every finite, simple, 3-colorable graph admits a faithful representation in* $\mathbb{G}(\mathbb{R}^2, odd)$. ∎

PROOF Let $G(V,E)$ be a 3−colorable graph, $V = \{v_1,\ldots,v_r,v_{r+1},\ldots v_{r+g},v_{r+g+1},\ldots,v_{r+g+b}\}$ be the red green and blue vertices.

We place the red vertices v_i at $P_0[a_i,b_i], i = 1,\ldots r$ the green vertices v_j at $P_1[a_j,b_j], j = r+1,\ldots,r+g$ and the blue vertices v_k at $P_2[a_k,b_k], k = r+g+1,\ldots,(r+g+b=n)$. By corollary 3.31 $a_i > 3b_i$ hence all red vertices are placed on the arc $\widehat{A_0,A_1}$, the green vertices on the arc $\widehat{A_1,A_2}$ and the blue vertices on the arc $\widehat{A_2,A_0}$.

Let $M = \{\{i,j\} \mid (v_i,v_j) \in E(G)\}$ and let:

$$A_M = \prod_{\{i,j\}\in M} \mid \alpha_{i,j}^4 \mid \prod_{\{i,j\}\notin M} \mid \alpha_{i,j} \mid^2 .$$

We need to show that by blowing the initial circle by A_M we obtain a faithful representation of $G(V,E)$ in the odd distance graph. A_M is an odd integer. The distances between points belonging to the same arc are rational numbers with an odd denominator and even numerator hence they will not be odd integers after the expansion.

For edges (v_i,v_j) represented by $P_s[a_i,b_i], P_t[a_j,b_j],\ s \neq t$ belonging to distinct arcs, the distance $D_{i,j}$ between such vertices is:

$$D_{i,j} = \frac{(a_i+b_i)(a_i-3b_i)(a_j+b_j)(a_j-3b_j)+4a_jb_j(a_i^2+2a_ib_i-3b_i^2)}{(a_i^2+3b_i^2)(a_j^2+3b_j^2)} \text{ (see (5))}$$

When $(v_i,v_j) \in E(G),\ \{i.j\} \in M$. By Corollary 47:

$$A_m \cdot D_{i,j} = \Big(\prod_{\{m,n\}\in M\setminus\{\{i,j\}\}} \mid \alpha_{n,m} \mid^4 \cdot \prod_{\{m,n\}\notin M\cup S_{i,j}\cup\{\{i,j\}\}} \mid \alpha_{n,m} \mid^2\Big)\times$$

$$\frac{\big((a_i+b_i)(a_i-3b_i)(a_j+b_j)(a_j-3b_j)+4a_jb_j(a_i^2+2a_ib_i-3b_i^2)\big)}{(a_i^2+3b_i^2)(a_j^2+b_j^2)}$$

is an odd integer.

If $(v_i,v_j) \notin E(G)$ we need to prove that $A_M \cdot D_{i,j}$ is not an integer. Using Corollary 47, we need to show that:

$$\frac{(a_i+b_i)(a_i-3b_i)(a_j+b_j)(a_j-3b_j)+4a_jb_j(a_i^2+2a_ib_i-3b_i^2)}{\mid \alpha_{i,j} \mid^2} \text{ is not an integer.}$$

We shall do it by proving that:
$GCD((a_i+b_i)(a_i-3b_i)(a_j+b_j)(a_j-3b_j)+4a_jb_j(a_i^2+2a_ib_i-3b_i^2), \mid \alpha_{i,j} \mid^2) = 1.$

Note that $\mid \alpha_{i,j} \mid^2$ divides both $a_i^2 + 3b_i^2$ and $a_j^2 + 3b_j^2 \rightarrow a_k^2 \equiv -3b_k^2 \bmod \mid \alpha_{i,j} \mid^2,\ k = i, j.$

$$
\begin{aligned}
&(a_i + b_i)(a_i - 3b_i)(a_j + b_j)(a_j - 3b_j) + 4a_jb_j(a_i^2 + 2a_ib_i - 3b_i^2) \bmod \mid \alpha_{i,j} \mid^2 \\
&= (a_i^2 - 2a_ib_i - 3b_i^2)(a_j^2 - 2a_jb_j - 3b_j^2) + 4a_jb_j(a_i^2 + 2a_ib_i - 3b_i^2) \bmod \mid \alpha_{i,j} \mid^2 \\
&= (2a_i^2 - 2a_ib_i)(2a_j^2 - 2a_jb_j) + 4a_jb_j(2a_i^2 + 2a_ib_i) \bmod \mid \alpha_{i,j} \mid^2 \\
&= 4a_j \left[(a_i^2 - a_ib_i)(a_j - b_j) + b_j(2a_i^2 + 2a_ib_i) \right] \bmod \mid \alpha_{i,j} \mid^2 \\
&= 4a_j \left[a_i^2 - a_ib_ia_j - a_ib_j^2 + a_ib_ib_j + 2a_i^2b_j + 2a_ib_ib_j \right] \\
&= 4a_j \left[a_i^2a_j + a_i^2b_j - a_ib_ia_j + 3a_ib_ib_j \right] \bmod \mid \alpha_{i,j} \mid^2 \\
&= 4a_j(a_i + 3b_i)(a_ib_j - a_jb_i) \bmod \mid \alpha_{i,j} \mid^2 .
\end{aligned}
$$

We shall assume that $j > i$. To prove that this fraction is not an integer we will prove that each factor of the product $4a_j(a_i + 3b_i)(a_ib_j - a_jb_i)$ is not zero mod $\mid \alpha_{i,j} \mid^2$.

Recall that $\mid \alpha_{i,j} \mid^2 = \mid \beta_{i,j} \mid^{r_{i,j}} = p_{i,j}^{r_{i,j}}$ where $p_{i,j} = \mid \beta_{i,j} \mid^2$ is a prime number.

1. $GCD(4a_j, \mid \alpha_{i,j} \mid^2) = 1.$

   PROOF Assume that $\mid \alpha_{i,j} \mid^2$ divides $4a_j$. Then $p_{i,j} \mid a_j$ but $p_{i,j}$ also divides $a_j^2 + 3b_j^2$ hence $p_{i,j} \mid b_j$. But this means that $p_{i,j} = \beta_{i,j} \cdot \overline{\beta_i, j}$ divides $a_j + b_j\sqrt{-3}$ which contradicts the definition of $a_j + b_j\sqrt{-3}$. ∎

2. $GCD(a_i + 3b_i, \mid \alpha_{i,j} \mid^2) = 1.$

   PROOF Again, assume that $p_{i,j}$ divides $a_i + 3b_i$. That is $a_i \equiv -3b_i \bmod p_{i,j} \Longrightarrow a_i^2 \equiv 9b_i^2 \bmod p_{i,j}$. But $a^2 + 3b_i^2 \equiv 0 \bmod p_{i,j} \Longrightarrow p_{i,j} \mid 12b_i^2 \Longrightarrow p_{i,j} \mid b_i$ and we reach the same contradiction as in the previous case. ∎

3. $GCD((a_ib_j - a_jb_i), \mid \alpha_{i,j} \mid^2) = 1.$ *P*roof:
   Assume that $(a_ib_j - a_jb_i) \equiv 0 \bmod p_{i,j}$. This means that $\frac{a_i}{a_j} \equiv \frac{b_i}{b_j} \bmod p_{i,j} \Longrightarrow a_i = u \cdot a_j + m \cdot p,\ b_i = u \cdot b_j + n \cdot p \Longrightarrow a_i + b_i\sqrt{-3} = u(a_j + b_j\sqrt{-3}) + (m + n\sqrt{-3})p_{i,j}.$

   Since $i < j,\ \beta_{i,j} \mid a_j + b_j\sqrt{-3}$ and since $\beta_{i,j} \mid p_{i,j} \Longrightarrow \beta_{i,j} \mid a_i + b_i\sqrt{-3}$. But this is not possible by the definition of $a_i + b_i\sqrt{-3}$.

   Concluding remarks:

   This result offers some interesting questions.

   a) It is not difficult to find subgraphs of $\mathbb{G}(\mathbb{R}^2, \{1\})$ that do not have a faithful representation in the unit distance graph. We do not know such examples for the odd-distance graph.

b) There are infinite graphs for which every finite subgraph has a faithful representation in the odd-distance graph, but the graph itself is not a subgraph of the odd-distance graph.

c) The rectangular and triangular grids are subgraphs of the odd-distance graph. Every subgraph of these graphs is 3-colorable. Can they be faithfully represented in the odd-distance graph?

d) The unit-distance graph is a subgraph of the odd-distance graph, can it be faithfully represented in the odd-distance graph?

Bibliography

[1] P. Brass, W. Moser, J. Pach: Research Problems in Discrete Geometry, Springer 2005, 250-252.

[2] D.A. Cox: *Primes of the form* $x^2 + ny^2$, John Wiley & Son 1989, 7-12.

[3] N.H. Anning and P. Erdos: *Integral distances*, Bull. Amer. math. Soc. **51** (1945), 598-600.

[4] H. Harborth: *On the problem of P. Erdös concerning points with integral distance*, Anna. New York Aca. Sci. **175** (1770), 206-207.

[5] H. Maehara, K. Ota, and N. Tokushige: Every graph is an Integral distance graph in the plane. J. Combin. Theory A **80** (1997), 290-294

[6] R.L. Graham, B.L. Rothschild, and E.G. Straus, *Are there* $n + 2$ *points in* E^n *with odd integer distance?* Amer. Math. Monthly **81** (1974), 21-25

[7] H. Ardal, J. Manŭch, M. Rosenfeld, S. Shelah, L. Stacho: The Odd-Distance Plane Graph, Discrete Comput. Geom. **42** (2009), 132-141.

[8] M.Rosenfeld and T.N. Le: *Forbirden subgraph of the odd-distance graph*, J. Graph Theory, published online (2013).

[9] L. Piepemeyer: The maximum number of odd integral distances between points in the plane, Discrete Comput. Geom. **16** (1996), 156-159.

4 Combinatorics

4.1 Sperner's lemma

Tran Van Do

Abstract

The aim of this note is to give a proof of Sperner's theorem about the maximal size of a collection of subsets of $\{1, \ldots, n\}$ such that no subset is contained in another subset. The proof makes use of Hall's theorem.

We first restate Sperner's theorem.

Theorem 4.1 (Sperner) *Let $S = \{1...n\}, \mathcal{A} = \{X \subset S : \forall X, Y \in \mathcal{A}, X \nsubseteq Y\}$, Then:*

$$|\mathcal{A}| \leqslant \binom{n}{\lfloor \frac{n}{2} \rfloor}.$$

■

We call sets $\mathcal{A}$ satisfying the condition in Sperner's theorem *Sperner sets*.

It is easy to see that $S_{\lfloor \frac{n}{2} \rfloor}$, the set of all subsets of S of size $\lfloor \frac{n}{2} \rfloor$, is a Sperner set for which the above inequality is an equality.

We first need three graph theory definitions for later use.

Definition 4.2 (Bipartite Graph) *A graph $\mathbb{G}$ is called bipartite if the vertex set of $\mathbb{G}$ can be split into two disjoint sets X and Y so that each edge of $\mathbb{G}$ is adjacent to one vertex of X and one vertex of Y. We denote it by $\mathbb{G}(X, Y)$.* ■

Definition 4.3 (Neighborhood) *Let $\mathbb{G}$ be a graph, $T \subset V(\mathbb{G})$. The set of vertices $N(T) = \{v \mid (u, v) \in E(\mathbb{G}), u \in T\}$, is the neighborhood of T.* ■

Definition 4.4 (Matching) *Let $\mathbb{G}(X, Y)$ be a bipartite graph. $\mathbb{G}$ has a perfect matching from X into Y if there is a set S, of vertex disjoint edges in $\mathbb{G}$ (a matching), such that each vertex in X belongs to exactly one edge in S.* ■

The proof will be accomplished by constructing an injection from a Sperner set $\mathcal{A}$ to $S_{\lfloor \frac{n}{2} \rfloor}$. To do so we use Hall's theorem, also known as the *marriage theorem* or SDR (system of distinct representatives).

Theorem 4.5 (Phillip Hall) *Let $G(X, Y)$ be a bipartite graph. Then X has a perfect matching into Y if and only if for all:*

$$T \subseteq X : \ |N(T)| \geqslant |T|,$$

■

Proofs of Hall's theorem can be found in almost every book on combinatorics, graph theory or discrete optimization. A couple of references include P. Hall's original paper, see [1] the textbook [2] or our class lecture notes [3].

Let $S_k = \{X \subseteq S, |X| = k, 1 \leqslant k \leqslant n\}$.

Lemma 4.6 *There are injections f_k from S_k to S_{k+1} (where $1 \leqslant k < \lfloor \frac{n}{2} \rfloor$) such that for every $X \in S_k$, $f_k(X) \supset X$.* ∎

PROOF We construct a bipartite graph $\mathbb{G}(X, Y)$ as follows:

a) $X = S_k,\ Y = S_{k+1}$.

b) $(x, y) \in E(\mathbb{G})$ if $x \subset y$.

Let $T \subset X$. Every vertex $x \in T$ has $n - k$ neighbors in Y. Let $N(T)$ be the neighbors of T in Y. There are $(n-k) \cdot |T|$ edges with one vertex in T and the other in $N(T)$. Every vertex $y \in Y$ has $k + 1$ neighbors in X. Hence:

$$(n-k) \cdot |T| \leqslant (k+1) \cdot |N(T)|$$

Since $n - k \geqslant k + 1$ we must have $|N(T)| \geqslant |T|$.
By Hall's theorem there is a perfect matching (an injection) $f_k : X \to Y$. ∎

Lemma 4.7 *There are injections g_k from S_k to S_{k-1} (where $\lfloor \frac{n}{2} \rfloor < k \leqslant n$) such that for every $X \in S_k$, $g_k(X) \subset X$.* ∎

PROOF This follows directly from lemma 4.6. Let $X \in S_k,\ k > \lfloor \frac{n}{2} \rfloor$. Then $|S \backslash X| < \lfloor \frac{n}{2} \rfloor$. We leave it to the reader to see that:

$$g_k(X) := S \backslash f_k(S \backslash X)$$

Is an injection from $S_k \to S_{k-1}$ such that $g_k(X) \subset X$. ∎

We are now ready to prove Sperner's theorem.

PROOF Let $\mathcal{A}$ be a Sperner set. We decompose $\mathcal{A}$ into subsets $\mathcal{A}_t = \{X \subset \mathcal{A} \mid |X| = t\}$. For each $X \in \mathcal{A}_t$ let:

$$\kappa(X) = \begin{cases} f_t \circ f_{t+1} \circ \ldots \circ f_{\lfloor \frac{n}{2} \rfloor - 1} & \text{if } t < \lfloor \frac{n}{2} \rfloor \\ g_t \circ g_{t-1} \circ \cdots \circ g_{\lfloor \frac{n}{2} \rfloor + 1} & \text{if } t > \lfloor \frac{n}{2} \rfloor \\ X & \text{if } t = \lfloor \frac{n}{2} \rfloor \end{cases}$$

We first note that $\forall X \in \mathcal{A},\ \kappa(X) \in S_{\lfloor \frac{n}{2} \rfloor}$. It remains to show that κ is an injection, that is if $X_1 \neq X_2 \in \mathcal{A}$ then $\kappa(X_1) \neq \kappa(X_2)$.

Let $X_1 \in \mathcal{A}_t$ and $X_2 \in \mathcal{A}_{t'}$. Since $X_1 \neq X_2$ there is an element $x_0 \in X_1$ such that $x_0 \notin X_2$.

If $t = t' < \lfloor \frac{n}{2} \rfloor$ then $f_t(X_1) \neq f_t(X_2) \Rightarrow f_{t+1}(f_t(X_1)) \neq f_{t+1}(f_t(X_2) \ldots f_t \circ f_{t+1} \circ \ldots \circ f_{\lfloor \frac{n}{2} \rfloor - 1}(X_1) \neq f_t \circ f_{t+1} \circ \ldots \circ f_{\lfloor \frac{n}{2} \rfloor - 1}(X_2)$ or $\kappa(X_1) \neq \kappa(X_2)$.

If $t < t' < \lfloor \frac{n}{2} \rfloor - 1$ then:

Let $X_1' = f_t \circ f_{t+1} \circ \ldots \circ f_{t'-1}(X_1) \in \mathcal{A}_{t'}$; since $x_0 \notin X_2$, and $x_0 \in X_1' \Rightarrow X_1' \neq X_2$ and by the previous argument $\kappa(X_1) = \kappa(X_1') \neq \kappa(X_2)$.

If $t < \lfloor \frac{n}{2} \rfloor$ and $t' > \lfloor \frac{n}{2} \rfloor$ then $x_0 \in \kappa(X_1)$ while $x_0 \notin \kappa(X_2)$ since $\kappa(X_2) \subset X_2$ and $x_0 \notin X_2$.

The final case $t, t' > \lfloor \frac{n}{2} \rfloor$ can be handled similarly. We leave the simple details for the reader to verify. ∎

Bibliography

[1] Hall, Philip *O*n Representatives of Subsets, J. London Math. 1935, Soc. 10 (1): 26 - 30.

[2] van Lint, J. H.; Wilson, R.M. *A* Course in Combinatorics, Cambridge: Cambridge University, (1992)

[3] Moshe Rosenfeld, *L*ectures in Discrete Mathematics. [15]

[15] http://mim.hus.vnu.edu.vn/courses/login/index.php

4.2 The Salmon problem

Le Tien Nam

Abstract

A fictional story by Moshe Rosenfeld about salmon who lived in Lake Washington but devoted their whole life to finding the Ocean.

4.2.1 introduction

[by Moshe Rosenfeld] In 2007 at the Bled sixth International Conference on Graph Theory $(http://videolectures.net/sicgt07\_bled/)$ I proposed the "Salmon Problem". It was derived from a popular folklore riddle:

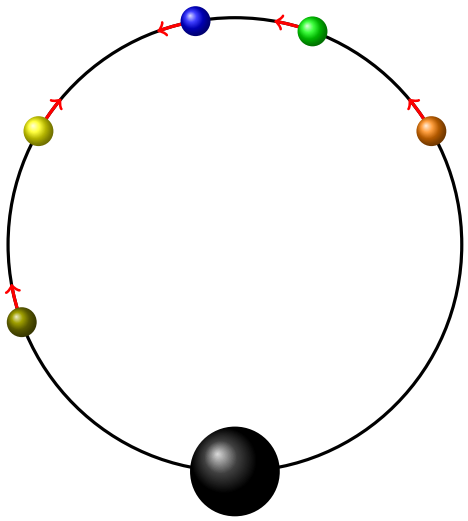


Figure 18: Ants on their way to purgatory.

101 ants on a circular track of length 100 cm start moving at the same time, in a preassigned direction, at a speed of 1 cm/sec. If they collide, they change direction. When they reach the "black hole" they drop to "purgatory". Can ants survive? If not, when will the last ant die? (see Figure 8)
This puzzle has a one line solution[16].

A slight variation is the "Roaming Salmon." The Salmon start their life in streams, swim to the ocean, return to their birth place and die. So in our variation, we made

[16]I do not know when this puzzle appeared first and who is the author. But you can find it at http://www.math.hmc.edu/funfacts/ffiles/20001.8.shtml

a slight change: the Salmon die when they reach their "birth place" with the additional rule that if two salmon meet at one's birthplace, death occurs first.

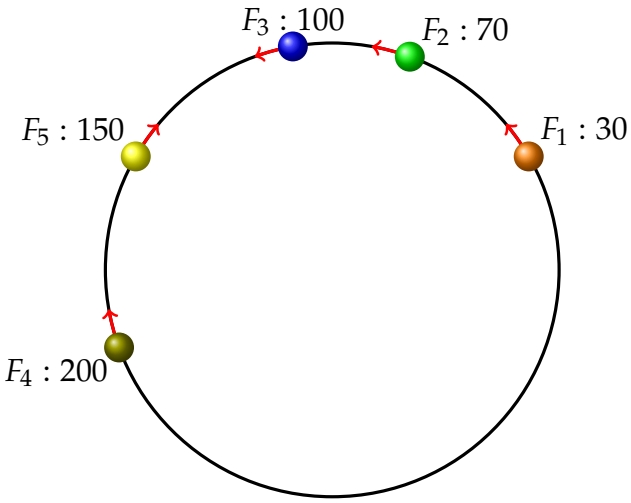


Figure 19: Salmon's journey.

Figure (9) shows an example of five Salmon on a circular track. The labels $F_i : n$ indicate the fish number and its location in degrees on the track. Can you tell whether any fish will survive? Or who will die first? last?
We can use the following table to track the journeys of these five fish:

Time	F_1	F_2	F_3	F_4	F_5	Action
0	30^+	70^+	100^+	200^-	150^-	
25	55^+	95^+	125^-	175^-	125^+	$F_3 : F_5$ collide
40	70^+	110^-	110^+	160^-	140^+	$F_3 : F_2$ collide
50	80^+	100^-	120^+	150^-	150^+	F_5 dies
60	90^-	90^+	130^+	140^-		$F_1 : F_2$ collide

The reader is invited to complete the table and determine the fate of the five fish in this example. In particular, we encourage the reader to check what is the situation at time 360 (time for a full cycle).
Nam Le Tien accepted the challenge to chronicle the Salmon journeys. Here is his story:

4.2.2 The Story

"Once upon a time, there were unlucky Salmon who were born in Lake Washington. Instinctively, they wanted to migrate to the Ocean to enjoy a luxurious life. They

started to move around the Lake to chase the call of the Ocean, but they were very changeable. Usually, one met another salmon, and stopped to inquire:

- Hey, comrade! Where are you going?

- Hello! I'm journeying to the Ocean. And you?

- Oh, me too. Where is it?

- I dunno. But I think u're on wrong direction because I've come from there.

- Oh, really? U're also on wrong direction because I've come from where u're going to.

Both thought that their friends were true and they changed their directions until they met other salmon... They move, move till one day, they realized they came back to where they were born. Despairing and exhausted, they died..."

Now, We assume that Lake Washington is round, salmon born at the same time and then move to one of two directions (clockwise or counter-clockwise) with the same speed. If there are only two or three fish, all of them will die. You can easily check it with pencil and paper. But surprisingly, if there are more than three fish, some of them will survive forever. How can they survive? how many can survive? and what happens if distances from each salmon to its neighbors are the same?... In this note, we continue to write the story of the salmon lives through math eyes.

4.2.3 Definitions and Notation

Definition 4.8

a1. At the beginning, fish are arranged in order of increasing index.

a2. The initial position of a fish is called hole and is indexed by the fish's index

a3. (-) denotes clockwise direction, and (+) counter-clockwise.

a4. A cycle is a period of time for a fish to move around the lake and return to the same position without any interference. Without loss of generality we may assume that a a cycle takes one minute to complete.

a5. We enumerate the cycles from the beginning: $1^{st}, 2^{nd}, .., .k^{th}$

a6. Assume that at the beginning of the journey, each fish F_i *wears a hat* H_i*. If two fish collide, they change hats; the fish reverse direction, the hats do not.*

a7. Each hat has an odometer. The odometer measures the distance traveled as follows: when a hat moves in the (+) direction it adds the distance traveled, when it moves in the (-) direction it subtracts.

a9. At the beginning of each cycle all odometers are reset to 0.

a10. The arc length between h_i, hole number i, and h_{i+1} is denoted by $d(h_i, h_{i+1})$, similarly, the arc length between h_i and h_j, $j > i$ is $d(h_i, h_j) = \sum_{k=0}^{j-1} d(h_{i+k}, h_{i+k+1})$ and $\sum_{k=0}^{n-1} d(h_{1+k}, h_{1+k+1}) = 1$ (assuming we have n holes and $h_{n+1} = h_1$). ■

4.2.4 Observations

b1. The relative order of the fish is never changed even after a collision.

b2. Hats keep moving in the same direction; all return to their initial hole at the end of each cycle.

b3. At the end of each cycle every hat H_i will be back at hole #i with odometer showing ± 1.

b4. This means that at the end of each cycle, every surviving fish will be at a hole of another fish wearing a hat. The relative order among the fish is retained.

b5. A fish always moves in the same direction as the hat it wears.

b6. During each cycle while no fish dies the number of fish moving in the (+) direction remains invariant.

4.2.5 The journey

Proposition 4.9 *At the beginning of a cycle, there are k (+) fish and l (-) fish. Assume that at the end of this cycle no one dies. Let fish $F_{i_0}, F_{i_1}, \ldots, F_{i_{m-1}}$ start in holes $h_{j_0}, h_{j_1}, \ldots, h_{j_{m-1}}$. At the beginning of the cycle, the fish will be wearing hats number $H_{j_0}, H_{j_1}, \ldots, H_{j_{m-1}}$. At the end of this cycle:*

p1. The sum of the hats' odometers will clearly be $k - l$.

p3. The fish F_{i_r} will be in hole number $h_{i_{r+k-l}}$ at the end of the cycle [17]. ■

PROOF Without loss of generality, we may assume that $k \geqslant l$. Since the hats never change direction at the end of a cycle they will return to their initial hole in the cycle with the odometer reading +1 if they moved in the counter clockwise direction and -1 if they moved in the clockwise direction. This proves p1.

Since fish always wear hats, and they move in the same direction as the hat they wear, the net distance the fish travel will be the same as the net distance the hats travel that is $k - l$.

[17] all index arithmetic to be done mod m, m the number of fish in the current cycle.

Since at the end of the cycle each hat H_{j_r} ends in the hole where it started the cycle, collectively, the fish will also end up in these holes. Assume that fish F_{i_0}, who started in h_{j_0}, lands at the end of the cycle in h_{j_s}. Since all fish will land at the end of the cycle in the initial holes and their relative order will not change, F_{i_1} will land in $h_{j_{s+1}}$, F_{i_2} will land in $h_{j_{s+2}} \ldots$ and $F_{i_{m-1}}$ will land in j_{m+s-1} .

As a whole group, the total net distance from the initial holes where the fish started the cycle till the end of the cycle is $k - l$. The net distance the fish F_{i_r} contributes to the sum of distances traveled by all fish combined is $d(h_{j_r}, h_{j_{r+s}})$. Thus every arc (h_j, h_{j+1}), between two adjacent holes, will be counted in the net distance exactly s times. It follows that the net distance traveled by all fish will be $s = k - l$. This proves p3. ∎

Corollary 4.10 *At the beginning of a cycle, if $k \neq l$ (without loss of generality we may assume that $k > l$), then after no more than $\lceil \frac{k+l}{k-l} \rceil$ cycles, at least one fish will die.* ∎

PROOF By proposition 1, if no fish dies during the cycle, they will end up in the original holes, shifting their positions by $k - l$ holes. Furthermore, the $\pm$ pattern will be preserved as it is the pattern of the hats that occupy the holes. So in the next cycle either a fish dies or each fish will move to a hole shifted by $k - l$ holes. But this means that after no more than $\lceil \frac{k+l}{k-l} \rceil$ some fish will come to its origin where it will die. This proves Cor 1. ∎

Corollary 4.11 *At the beginning of a cycle, if $k = l$, then all $k + l$ fish will survive forever or at least one of them will die during this cycle.* ∎

PROOF This follows easily from Proposition 1. If no fish dies during a cycle, if $k = l$ then all fish end at the holes where they started the cycle with the same orientations, thus this pattern repeats itself indefinitely. ∎

Corollary 4.12 *An odd number of fish cannot survive indefinitely.* ∎

PROOF This is a direct consequence of corollary 4.10. ∎

A rough upper bound of the time when all fish die or the remaining fish survive indefinitely.

Proposition 4.13 *If we start with n fish and m fish survive forever, then the procedure will take no more than $n^2 - mn$ cycles.* ■

PROOF By corollary 4.10 , it is easy to deduce that we need no more that n cycles to kill one more fish. Thus the time to get to a terminal configuration (all fish died, or a repeating cycle with k fish moving in the (+) direction and K moving in the (-) direction where no fish dies during the cycle) is no more than $n(n-m)$ cycles. ■

Conjecture 4.14 *We believe that the actual time to reach a terminal configuration is not more than $\frac{n}{2}$.* ■

4.2.6 Uniformly Distributed salmon

$\forall n \in M = \{1,2,3,4,5,6,8\}$, no salmon survive forever in every uniformly distributed n salmon on the cycle. In contrast, for $\forall n \notin M$, there exists a configuration of uniformly distributed n salmon on the cycle such that exactly 2 fish survive indefinitely.

We enumerate n uniformly distributed fish on the cycle in clockwise order.

Definition 4.15 *A configuration of uniformly distributed n salmon is coded $< n : a_1, a_2, ...a_k <$ if fish number $a_1, a_2, ...a_k$ go counter-clockwise at the initial time and all other fish go clockwise.*

For example: The configuration of uniformly distributed 5 salmon in which fish number $1,2,4$ go counter-clockwise and fish number $3,5$ go clockwise is coded $< 5 : 1,2,4 <$. ■

Proposition 4.16 *For every odd integer $n > 5$, there exists a configuration of uniformly distributed n salmon on the cycle such that exactly 2 survive forever.* ■

PROOF Let $n = 2m + 1$. Consider cases:

- For $n = 7$, the code is $< 7 : 1,2 <$
- For $n = 9$, the code is $< 9 : 1,2,5 <$
- For $n = 11$, the code is $< 11 : P1,2,5 <$
- For $n \geqslant 13$, the code is $< 13 : 1,4,8,11,13,15,...,n <$
  After $\frac{1}{n}$ cycles, these couples will die: $(3,4), (7,8), (2i, 2i+1),\ \forall 5 \leqslant i \leqslant m$. And only 5 fish: $1,2,5,6,9$ are active (survive after that).
  At time $\frac{n-8}{n}$, fish number 1 dies, and at time $\frac{n+4}{n}$ fish 6 and 9 die. Then fish

2 and 5 collide at position $m+4$ and collide again at the position 3.5 and they survive forever. ■

Proposition 4.17 *For every even integer $n > 8$, there exist a configuration of uniformly distributed n salmon on the cycle such that exactly 2 survive forever.* ■

PROOF Let $n = 2m$. Consider cases:

- For $n = 10$, the code is $< 10 : 1, 2, 3 <$
- For $n = 12$, the code is $< 12 : 1, 2, 3 <$
- For $n = 14$, the code is $< 14 : 1, 2, 3 <$
- For $n \geqslant 16$ and m is odd, the code is $< n : 1, 4, 7, 10, 12, ..., n <$
  After $\frac{1}{n}$ cycles, these couples will die: $(3, 4), (6, 7), (2i-1, 2i),\ \forall 5 \leqslant i \leqslant m$. And only 4 fish: $1, 2, 5, 8$ are still alive.
  At time $\frac{n-7}{n}$, fish number 1 dies, and at the time $\frac{n+6}{n}$, fish number8 dies. Then fish 2 and 5 collide at position $m+3$ and collide again at the position 3 and survive forever. ■

Proposition 4.18 *$\forall n \in M = \{1, 2, 3, 4, 5, 6, 8\}$, no salmon survive forever in uniformly distributed n salmon on the cycle.* ■

PROOF If two adjacent fish collide they die at time $\frac{1}{n}$; we call them an *inactive couple*. It is easy to see that every configuration of uniformly distributed salmon contains at least 1 inactive couple.

Without lost of the generality, we assume that $(1, 2)$ is an inactive couple. In order to reduce half of the number of tests, we can also assume that at the beginning, the number of fish moving clockwise is not smaller than the number of fish moving counter-clockwise.

- For $n = 1, 2, 3$: obvious.
- For $n = 4$: $(1, 2)$ are an inactive couple. For all configurations of $3, 4$, both of them will collide and die.
- For $n = 5$: Try 2^2 cases of placing $3, 4, 5$ we always get that all die.
- For $n = 6$: Try 2^3 cases of placing $3, 4, 5, 6$ we always get that all die.
- For $n = 8$: Try 2^5 cases of placing $3, 4, 5, 6, 7, 8$ we always get the that all die.

(Of course we can reduce the number of tests down to 10 times, but 32 times is small enough for computer) ■

Remark 4.19 *There are many unknown mysteries about the salmon journey. There are also some known stories that do not appear in this note.*

To be continued...

Thanks for following our story. ■