limo.fmf.nl | 050 - 363 41 55 | limo@fmf.nl

FMF

Solution Booklet

LIMO 2018

transtrend

University of Amsterdam

DIAMANT

TU Delft

FLOW TRADERS

KWG

Radboud University

university of groningen

KONINKLIJKE
HOLLANDSCHE MAATSCHAPPIJ
DER WETENSCHAPPEN

cbs

UNIVERSITY
OF TWENTE.

Table of contents

1. Even triangles are odd 4
2. Self-divisible numbers 6
3. Ramifixation 7
4. A Kurt Mahler style power series 9
5. Chebyshev polynomials 11
6. Medium competition in bisecting the altitude 14
7. Mathematicians like to play with colors 17
8. Typing a's and b's 19
9. Matrix-valued function in one variable 21
10. Rational points 24
11. How about this question? 25
12. Restrict the extension 27

This Solution Booklet is a product of the LIMO-committee 2018:
Carina Schoenmaker
Ruben IJpma
Josselin Kooij
Sven Cats
Leander van Beek

E-mail: limo@fmf.nl
Website: fmf.limo.nl

1. Even triangles are odd

Harry Smit MSc., Universiteit Utrecht

Suppose you have a triangle that is subdivided into other triangles, i.e. this triangle is completely tiled with smaller triangles, without any overlap. Furthermore, assume that no three vertices (not even those of different triangles) lie on a straight line.

(a) Let k be an odd positive integer. Prove that it is possible to make a subdivision into exactly k triangles.

(b) Let k be an even positive integer. Prove that it is impossible to make a subdivision into exactly k triangles.

Solution.

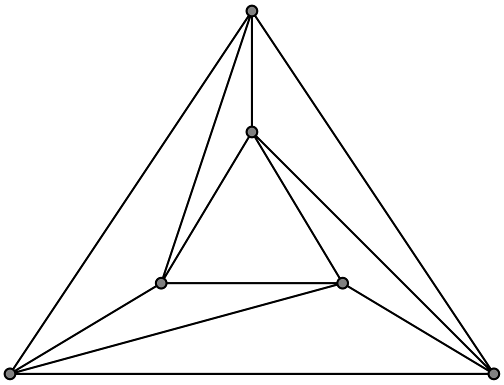
(a) We give a proof by induction. The trivial subdivision has one triangle. Suppose we have a subdivision into k triangles. Choose one of the triangles, and choose a point inside this triangle that does not lie on any line through two vertices (this is always possible, as we only have finitely many vertices). Then connect the new point with the vertices of the triangle it lies in, which subdivides this triangle into three triangles. Hence we've created a subdivision into $k + 2$ triangles. □

(b) As no three vertices lie on a line, every face of a triangle is adjacent to exactly three edges (no edge is split into two or more parts, as this would imply that there are three or more points on a line). Furthermore, every edge except the ones of the original triangle is adjacent to two faces, whilst the edges of the original triangle are adjacent to exactly one face. If E denotes the number of edges, and F denotes the number of faces (i.e. triangles), then

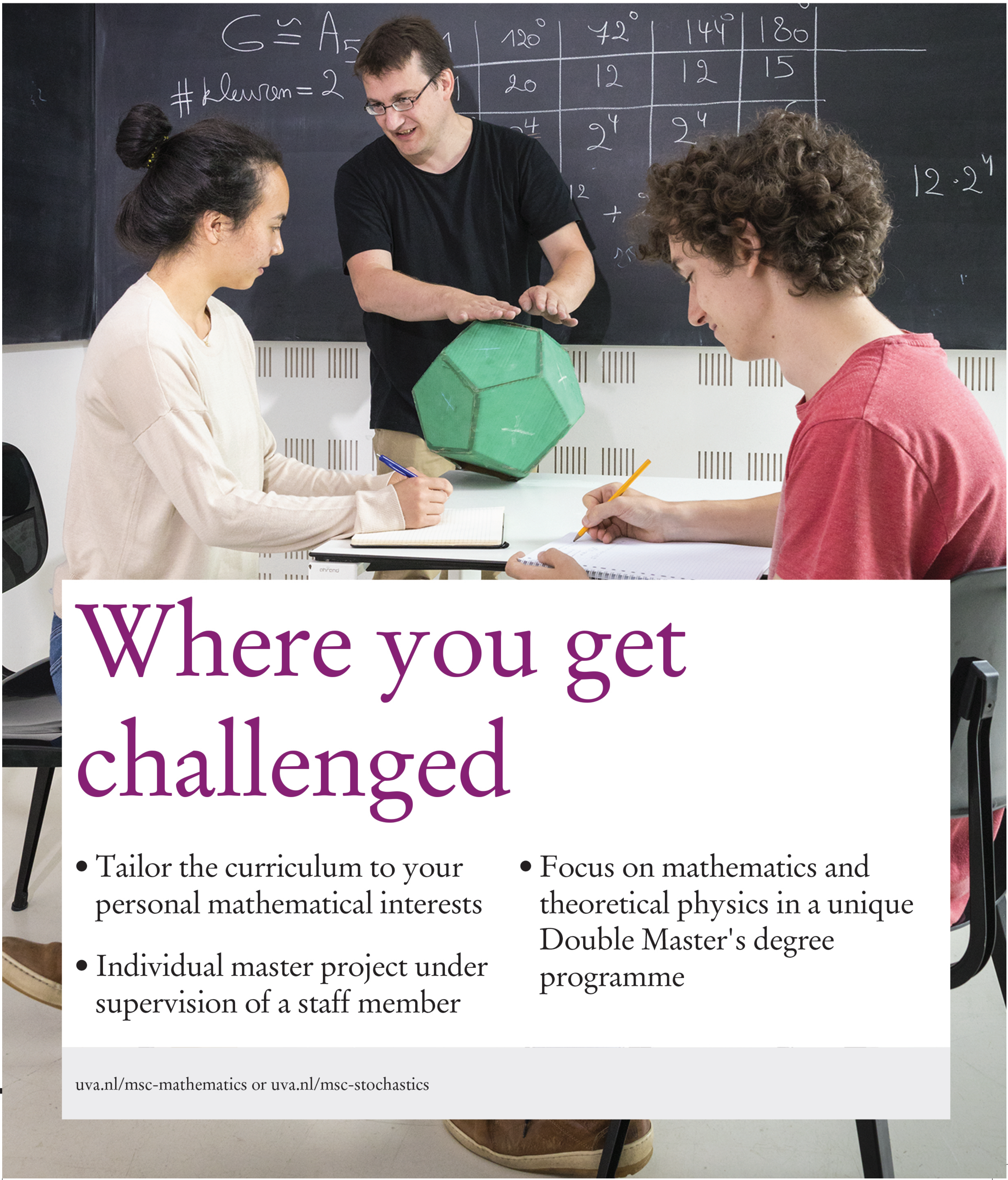
$$2E - 3 = 3F.$$

In particular, F is odd. □

Note: it is not in general true that there exists a point of a triangle that is adjacent to exactly three triangles. This means there exist subdivisions (like the one in the picture) that cannot be created using the "inductive" approach of the first part.



University of Amsterdam
Master's programmes Mathematics,
Stochastics and Financial Mathematics



Where you get challenged

- Tailor the curriculum to your personal mathematical interests
- Individual master project under supervision of a staff member
- Focus on mathematics and theoretical physics in a unique Double Master's degree programme

uva.nl/msc-mathematics or uva.nl/msc-stochastics

2. Self-divisible numbers

Ir. Harold de Boer, Transtrend BV

We define a positive integer to be self-divisible when each digit of the number (starting from the second digit) is a divisor of the number formed by the digits preceding it. For example, 42771 is self-divisible because 4 is a multiple of 2, 42 is a multiple of 7, 427 is a multiple of 7 and 4277 is a multiple of 1.
We define G_N as the set of self-divisible numbers that consist of N different digits. So, 42771 is an element of the set G_4.

(a) Determine the largest N for which the set G_N is not empty.

(b) Determine the smallest number in this particular set G_N.

Solution.
Applying the basic divisibility rules leads to the following for self-divisible numbers:

(i) They do not contain the digit 0.

(ii) The digit 5 can only follow another 5, or be the first digit. As a consequence, any 5s will be the first (few) digits.

(iii) An even digit cannot follow an odd digit. So a self-divisible number containing both odd and even digits will have all of its even digits preceding all of its odd digits.

(iv) From (iii) we can derive: a 4 and an 8 cannot follow either a 2 or a 6, and an 8 cannot follow a 4. So within the even digits any 8s must precede all of the 4s, with 2s and 6s following interchangeably.

From (ii) and (iii) together we can derive that a self-divisible number cannot contain any even digits if it contains a 5. Therefore the maximum number of different digits cannot exceed 8 - all digits excluding 0 or 5. We will show that the set G_8 is indeed not empty; immediately finding the smallest possible element of G_8.

If there is an 8-digit number, in which all the different digits (excluding 0 or 5) each occur only once, that satisfies the self-divisibility conditions, then that number must begin with the digital sequence 8462. The only odd digit that can then follow is 1, after which only 3 is possible. But neither 7 nor 9 will work as the next digit. So the number that we are looking for is at least a 9-digit number, with one digit occurring twice.

If the digit that occurs twice is an odd digit, then the self-divisible number will begin with 8462. It may be possible to construct a smaller 9-digit self-divisible number, if it starts with the digital sequence 842 or 844. This first option is not viable, because we will run into trouble fitting in a 6 without at least tripling the digit 2. Starting with 844 leads us to the only possible starting sequence, 84426. Both 1 and 3 are candidates for the next digit. Picking 1 next would leave us at a dead end, so 3 it is. The next digit can be 9, which will not have another chance without crossing into 10-digit territory. Next up must be 1. And closing off with a 7 fits the condition nicely. Which determines the smallest possible element of G_8: 844263917.

3. Ramifixation

Prof. dr. Hendrik Lenstra, Universiteit Leiden

A *tree* is a finite connected graph without cycles. An *automorphism* of a graph is a map σ that permutes both the set of vertices and the set of edges of the graph, in such a way that an edge e connects two vertices v and w if and only if $\sigma(e)$ connects $\sigma(v)$ and $\sigma(w)$.

Prove that every tree has a vertex or an edge that is mapped to itself by every automorphism of the tree.

Solution.
Let T be a tree. We give a proof by induction on the number of vertices of T. The case $n = 1$ is clear; for $n = 2$ the edge between the two vertices will be fixed by any automorphism. Now assume that $n > 2$ and that the statement holds for trees with less than n vertices. If $\sigma \in \mathrm{Aut}(T)$ and v is a leaf (a vertex connected to one edge), then $\sigma(v)$ is also a leaf. For if $\sigma(v)$ would be connected to more than one edge, v would be too. Now remove all the leafs. That you will have something left after this is not hard to see, because for any two neighboring vertices at least one of them is not a leaf (for $n > 2$ the rest of the tree has to "grow" out of one of them). The restriction of σ to this smaller tree is again an automorphism, which fixes either an edge or a vertex by the induction hypothesis. Therefore, so does σ, which completes the proof. □

university of groningen

founded in 1614 - top 100 university

The University of Groningen offers Master's degree in both Mathematics and Applied Mathematics. These degree programs provide you with the mathematical knowledge, skills and attitude needed to pursue a professional or research career. The emphasis is on abstraction and modelling. Since 2016 we offer a fully renewed program, with unique specializations: mathematics & complex dynamical systems, statistics & big data, science, business & policy, systems & control and computational mathematics. During the Master's program you will learn how to think in an abstract, logical, systematic and problem-oriented way. These qualities are highly appreciated by employers (academia, research institutes, companies, e.g.). Mathematics in Groningen is an internationally oriented, informal community. Our classes are small; you will be embedded in the research group of your choice. More information can be found on our websites www.rug.nl/masters/mathematics and www.rug.nl/masters/applied-mathematics. You can also email the academicadvisor.math@rug.nl for any questions.

Keuzegids Masters BEST GENERAL UNIVERSITY (fulltime) 2018

Keuzegids Universiteiten TOP-OPLEIDING 2017

Keuzegids Masters TOP-OPLEIDING 2018

CHOOSE YOUR MASTER IN TWENTE!

MASTER APPLIED MATHEMATICS

Specializations
- Mathematical Systems Theory, Applied Analysis and Computational Science
- Operations Research

www.utwente.nl/go/limo/am

4TU MASTER SYSTEMS & CONTROL

Specializations
- Biomechatronics
- Control Theory
- Robotics and Mechatronics
- Unmanned Aerial Vehicles

www.utwente.nl/go/limo/sc

UNIVERSITY OF TWENTE.

4. A Kurt Mahler[1] style power series

Prof. dr. Gunther Cornelissen, Universiteit Utrecht

Fix a prime number p. If an integer n is written as $n = p^r u$ where u is coprime to p, we define $|n|_p := p^{-r}$. Consider the power series

$$f(z) := \sum_{n \geq 1} |n|_p z^n.$$

(a) Show that the power series defining $f(z)$ converges for all complex numbers z with $|z| < 1$.

(b) Prove that for $|z| < 1$,

$$f(z) = \frac{z}{1-z} - \frac{z^p}{1-z^p} + \frac{1}{p} f(z^p).$$

(c) Prove that the series defining $f(z)$ diverges at a dense set of points in the complex unit circle by showing that

(i) it diverges at all p-power roots of unity, i.e., at all $z \in \mu_{p^\infty} := \{e^{2\pi ki/p^r} : k, r \in \mathbf{Z}\}$;

(ii) μ_{p^∞} is dense in the unit circle (i.e, for every $z_0 \in \{|z| = 1\}$ and $\varepsilon > 0$ there exists $\zeta \in \mu_{p^\infty}$ with $d(z_0, \zeta) < \varepsilon$ where d is distance along the circle).

Solution.

(a) Since $|n|_p \leq 1$, the series is majorised (absolutely) by $\sum_{n \geq 1} z^n$, which converges for $|z| < 1$ (to $z/(1-z)$). □

(b) Write the n in the summation variable as $n = p^e k$ where e runs over integers $e \geq 0$ and k over integers not divisible by p; then split of the term where $e = 0$:

$$\begin{aligned} f(z) &= \sum_{e \geq 0} \sum_{p \nmid k} p^{-e} z^{p^e k} \\ &= \sum_{p \nmid k} z^k + \sum_{e \geq 1} \sum_{p \nmid k} p^{-e} z^{p^e k} \end{aligned}$$

The first term can be written as the full sum over all k, minus the sum where k is divisible by p. The latter can be rewritten by a change of variables $k = p\ell$ with ℓ running over all integers. Both are then summed as a convergent geometric series for $|z| < 1$, and the second term is identified in terms of the orginal f:

$$\begin{aligned} f(z) &= \sum_{k \geq 1} z^k - \sum_{p | k} z^k + p^{-1} \sum_{e \geq 0} \sum_{p \nmid k} p^{-e} (z^p)^{p^e k} \\ &= \frac{z}{1-z} - \frac{z^p}{1-z^p} + \frac{1}{p} f(z^p). \end{aligned}$$

□

[1] The famous number theorist Kurt Mahler (1903-1988) studied these kinds of problems in the 1930's. Between 1934 and 1936 he worked - after from escaping Germany via Manchester - in Groningen, where he had a bicycle accident, after which he walked with a limp for the rest of his life.

(c) (i) The equation in the second part shows that f diverges at solutions satisfying $z^p = 1$. But the equation also shows that if f diverges at some z_0 with $|z_0| = 1$, then it does so too at all p-th roots of z_0. Iterating this reasoning, we find that f diverges at all z with $z^{p^m} = 1$ for some integer m.

(ii) The solutions of $z^{p^m} = 1$ are given by $e^{2\pi i k/p^m}$ for k running through the integers. If $z = e^{2\pi i\theta}$ for $\theta \in [0, 1)$ and $\varepsilon > 0$ are given, we need to prove that there exists (m, k) with $|\theta - k/p^m| < \varepsilon$. If θ is written in p-ary expansion as $\theta = \sum_{n\geq 1} a_n p^{-n}$ with $a_n \in \{0, \ldots, p-1\}$, then if we choose an integer m with $p^{-m} < \varepsilon$ and we set $k = \sum_{n=1}^{m} a_n p^{m-n}$, we find with $\theta_0 = k/p^m$ that

$$|\theta - \theta_0| = \sum_{n\geq m+1} a_n p^{-m} \leq p^{-m} < \varepsilon.$$

□

5. Chebyshev polynomials

Prof. dr. Jaap Top, Rijksuniversiteit Groningen

The wikipedia page describing ‘Chebyshev polynomials’ briefly mentions, besides the usual Chebyshev polynomials of the first kind T_n and the ones of the second kind U_n also a sequence of polynomials C_n. The sets of polynomials are related by $C_n(x) = 2T_n(\frac{x}{2})$ and $T_n' = nU_{n-1}$. This problem defines and asks for some properties of the polynomials C_n.

(a) Show that for any integer $n \geq 1$ a *unique* real polynomial C_n in one variable exists such that

$$x^n + x^{-n} = C_n(x + x^{-1})$$

(here x is also a variable).

(b) Show that $(4 - t^2)C_n''(t) - tC_n'(t) + n^2 C_n(t) = 0$.

(c) Show that for every $n \geq 2$ the polynomial C_n mod 2 (which has coefficients in $\mathbb{Z}/2\mathbb{Z}$) can be factored as a product $f^2 \cdot g$ for polynomials f, g with coefficients in $\mathbb{Z}/2\mathbb{Z}$ with moreover f of degree at least 1.

Solution.

(a) Denote $t = x + x^{-1}$. We see that $C_0(t) = 2$, $C_1(t) = t$ and these are the unique polynomials. We can find a recursive formula for $C_n(t)$. We note that

$$x^{n+1} + x^{-n-1} = (x^n + x^{-n})(x + x^{-1}) - x^{n-1} - x^{-n+1},$$

and conclude that

$$C_{n+1} = tC_n(t) - C_{n-1}(t).$$

Therefore, there exist a unique polynomial (by mathematical induction) $C_n(t)$ for each n, with required properties.

(b) When we differentiate the condition once and twice, we get

$$nx^{n-1} - nx^{-n-1} = (1 - x^{-2})C_n'(x + x^{-1}),$$

$$(n^2 - n)x^{n-2} + (n^2 + n)x^{-n-2} = 2x^{-3}C_n'(x + x^{-1}) + (1 - x^{-2})^2 C_n''(x + x^{-1}).$$

Denote the condition equation by C and derivative equations by F first, and by S second one. Looking at the left hand side of

$$n^2 \cdot C - x \cdot F - x^2 \cdot S = 0,$$

gives us that the right hand side of this term is zero again. When we compute the right hand side, we get

$$n^2 C_n(x + x^{-1}) - (x + x^{-1})C_n'(x + x^{-1}) - (x - x^{-1})^2 C_n''(x + x^{-1}) = 0.$$

When we replace $t = x + x^{-1}$, we get the desired formula because

$$(x - x^{-1})^2 = 2 - x^2 - x^{-2} = 4 - (x + x^{-1})^2 = 4 - t^2.$$

(c) Proving that a polynomial over a field has a (nontrivial, nonconstant) quadratic factor is equivalent to proving that the polynomial is not coprime with its derivative. By recursive formula, we conclude that $C_n(t)$ are monic polynomials of degree n, for each $n > 0$. Note that for any $P(x) \in \mathbb{F}_2[x]$, holds $P''(x) = 0$ (we multiply each coefficient by an even number). Therefore, over $\mathbb{F}_2$, formula in (b) becomes $n^2 C_n(t) - tC'_n(t) = 0$. If n is even, we conclude $C'_n(t) = 0$, so $C_n(t)$ and $C'_n(t)$ are not coprime (in fact their g.c.d. is $C_n(t)$, which remains to be a monic polynomial of degree n over $\mathbb{F}_2$), so in this case we have a required conclusion. When $n \geq 2$ is odd, we have a relation $C_n(t) = tC'_n(t)$, so again $C_n(t)$ and $C'_n(t)$ are not coprime (in fact their g.c.d. is $C'_n(t)$, which remains to be a monic polynomial of degree $n-1$ over $\mathbb{F}_2$) and this finishes the proof. □

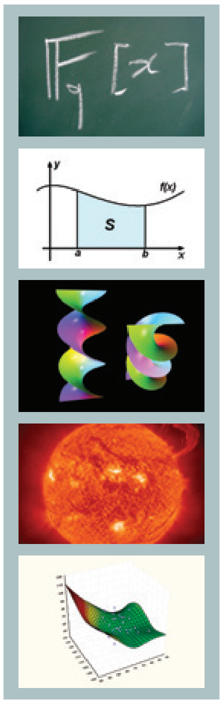
Katholieke Universiteit Leuven

De KU Leuven, gesticht in 1425, is de oudste universiteit van de lage landen. Meer dan 4.500 onderzoekers zijn er actief in wetenschappelijk onderzoek en onderwijs. Op 5 februari 2018 telde de KU Leuven in totaal 56.649 ingeschreven studenten. Van deze studenten heeft ongeveer 84% de Belgische nationaliteit, 16% zijn internationale studenten. Dit maakt van de gezellige provincie-hoofdstad Leuven een bruisende studentenstad met een rijk sociocultureel aanbod.

Onderzoek aan het Departement Wiskunde

Het onderzoek aan het departement Wiskunde is georganiseerd op het niveau van de onderzoeksafdelingen:

- Afdeling Algebra: het onderzoek situeert zich in de algebraïsche meetkunde, getaltheorie, algebraïsche topologie en groepentheorie.
- Afdeling Analyse: in deze afdeling doet men onderzoek in de klassieke analyse (reële en complexe analyse) en in de functionaalanalyse.
- Afdeling Meetkunde: het onderzoek is gecentreerd rond differentiaalmeetkunde, in het bijzonder Riemannse en pseudo-Riemannse meetkunde en deelvariëteiten.
- Afdeling Plasma-astrofysica: het onderzoeksdomein van deze afdeling is de wiskunde van vloeistoffen en plasma's, het voornaamste studieobject is de zon. Dit onderzoek is gesitueerd in de toegepaste en computationele wiskunde.
- Afdeling Statistiek: deze afdeling is actief in de wiskundige statistiek, in het bijzonder de theorie van extreme waarden, robuuste statistiek en niet-parametrische methoden. Ook stochastische processen en financiële wiskunde komen aan bod. De afdeling is bovendien ook actief in toegepaste consultatie voor bedrijven.



Meer info op http://wis.kuleuven.be

6. Medium competition in bisecting the altitude

Eduardo Ruíz Duarte MSc., Rijksuniversiteit Groningen

Find an example of a non-equilateral triangle ABC with integer sides for which the altitude from A, the bisector at B, and the median at C are concurrent, that is, they intersect at a single point. Hint: it is possible to find such a triangle with a perimeter no greater than 50.

Solution.
Assume the intersection point is inside the triangle (an inner bisector) and use Ceva's Theorem and the Angle Bisector Theorem.

(Ceva's Theorem) Given a triangle ABC with a point D on side BC, a point E on side AC and a point F on side AB, then the lines AD, BE and CF are concurrent, if and only if

$$\frac{|AF|}{|FB|} \cdot \frac{|BD|}{|DC|} \cdot \frac{|CE|}{|EA|} = 1. \tag{6.1}$$

(Angle Bisector Theorem) Suppose that in triangle ABC the point D is on side BC. Then

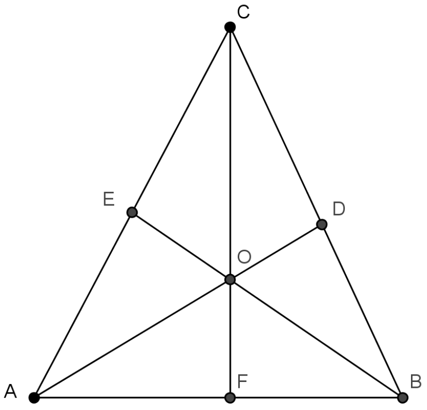


Figure 6.1: The triangle ABC

AD is an internal bisector, if and only if

$$\frac{|AB|}{|AC|} = \frac{|BD|}{|DC|}. \tag{6.2}$$

We will start with describing all possible albime triangles. Set $a = |BC|$, $b = |AC|$, and $c = |AB|$. We may assume that $b+c = 2$ without loss of generality. What we will try to do is find an expression for a in terms of c. Using the Angle Bisector theorem we get the following equality.

$$\frac{|AB|}{|AC|} = \frac{c}{2-c} = \frac{|BD|}{|DC|} \tag{6.3}$$

Since BE is a median, we have that $|CE| = |EA|$. This gives us

$$\frac{|CE|}{|EA|} = 1. \tag{6.4}$$

We also have the next equality.

$$\frac{|AF|}{|FB|} = \frac{|AF|}{c - |AF|} \tag{6.5}$$

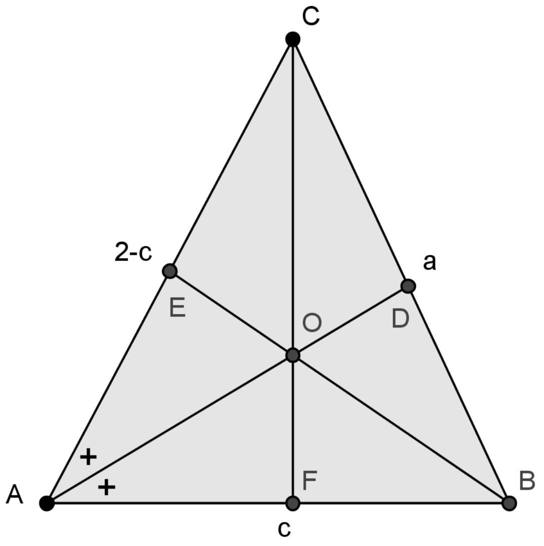


Figure 6.2: Albime triangle with sides a, $2 - c$ and c

Using this information and Ceva's theorem we can express $|AF|$ and $|FB|$ in terms of c.

$$\frac{|AF|}{c - |AF|} \cdot \frac{c}{2 - c} \cdot 1 = 1 \tag{6.6}$$

This leads us to an expression for $|AF|$, namely

$$|AF| = \frac{c(2 - c)}{2}. \tag{6.7}$$

We know $|BF| = c - |AF|$, thus we can also determine $|BF|$.

$$|BF| = c - \frac{2c - c^2}{2} \tag{6.8}$$

After some simple calculations we get

$$|BF| = \frac{c^2}{2}. \tag{6.9}$$

To find the length of BC we use the two right angled triangles that are in ΔABC, namely ΔAFC and ΔFBC. We will apply Pythagoras' theorem in both triangles and use the according side FC to give a value for a in terms of c.

In ΔAFC the Pythagorean theorem states $|FC|^2 = |AC|^2 - |AF|^2$. We know $|AC| = 2 - c$ and have already seen an expression for $|AF|$ in equation (6.7).

$$|FC|^2 = (2-c)^2 - \frac{c^2(2-c)^2}{4} \tag{6.10}$$

Eliminating the brackets gives

$$|FC|^2 = -\frac{c^4}{4} + c^3 - 4c + 4. \tag{6.11}$$

Doing the same for ΔFBC yields

$$|FC|^2 = a^2 - \frac{c^4}{4} \tag{6.12}$$

Combining the expressions of $|FC|^2$ found in equation (6.11) and (6.12) gives

$$a^2 - \frac{c^4}{4} = -\frac{c^4}{4} + c^3 - 4c + 4, \tag{6.13}$$

which can be written as

$$a^2 = c^3 - 4c + 4. \tag{6.14}$$

Hence, any albime triangle can be scaled to have sides c, $2-c$ and $\sqrt{c^3-4c+4}$. The equation $a^2 = c^3 - 4c + 4$ together with a point O at infinity defines an elliptic curve. It is also known as Guy's favorite elliptic curve.

This results in an equation of a cubic curve with rational point $A := (c, a) = (2, 2)$. Using the group law on such a curve one obtains $-4A = (1, 1), 7A = (10/9, 26/27), -10A = (88/49, 554/343)$, and $13A = (206/961, 52894/29791)$.

These give albime triangles with (rescaled) sides $(BC, AC, AB) =$
$(1, 1, 1), (13, 12, 15), (277, 35, 308), (26447, 26598, 3193)$.

7. Mathematicians like to play with colors

Stijn Cambie MSc., Radboud Universiteit Nijmegen

A *finite coloring* of the nonnegative integers is a map $f\colon \mathbb{N} \mapsto S : n \mapsto f(n)$, where S is a finite set. Given a coloring f, a set X is called *monochromatic* (MC) when every element is colored in the same color, i.e. for all $x_1, x_2 \in X$ one has $f(x_1) = f(x_2)$.
A theorem of Schur says that any finite coloring of $\mathbb{N}$ contains a MC set $\{x, y, x+y\}$, where $x, y \in \mathbb{N}$.

(a) Prove that any finite coloring of $\mathbb{N}$ contains a MC set $\{a, b, ab\}$ as well, where $a, b > 1$.

(b) Given a coloring $f\colon \mathbb{N} \mapsto \{B, W\}$. Does there exist a MC set of the form $\{a, b, ab+a\}$?

(c) Given a finite coloring of $\mathbb{N}$. Does there exists a MC set of the form $\{a, b, ab, a(b+2018)\}$?

Solution.

(a) Take a finite coloring $f\colon \mathbb{N} \to S$ and construct a second finite coloring $\tilde{f}\colon \mathbb{N} \to S\colon x \mapsto f(2^x)$. By Schur's theorem, there is a MC set $\{x, y, x+y\}$ for the coloring $\tilde{f}$, implying that $\{2^x, 2^y, 2^{x+y}\}$ is a MC set for the coloring f.

(b) Yes. First notice that if one of the two colors appear only a finite number of times, there is a number N such that $\{x \mid x > N\}$ is MC and hence in particular $\{a, b, a(b+1)\}$ for any $a, b > N$.
In the other case, there exists some $x < y$ such that $f(x-1) = B, f(x) = W$ and $f(y) = W, f(y+1) = B$. If $x(y+1)$ is colored in W, choosing $a = x, b = y$ gives a MC $\{a, b, ab+a\}$. If $x(y+1)$ is colored in B, then $\{a, b, ab+a\}$ is MC in the color B for $a = y+1, b = x-1$.

(c) There are multiple constructions for a finite coloring without a MC set $\{a, b, ab, a(b+1)\}$. We give one example using 5 colors. Let $S = \{1, 2, 3, odd, even\}$. If $4 \nmid n$, i.e. $n \equiv r \pmod 4$ for some $r \in \{1, 2, 3\}$, we choose $f(n) = r$. If $4 \mid n$, we set $f(n)$ equal to the parity of the 2-adic evaluation $v_2(n)$. One easily checks (considering the 5 possible colors) that no quadruple $\{a, b, ab, a(b+2018)\}$ can be MC for the coloring f.

If such a MC set would be using color $r \in \{1, 2, 3\}$, then for this r we would have $r \equiv r^2 \equiv r^2 + 2r \pmod 4$, which cannot happen.
If $4 \mid a, b$, then $v_2\left(a(b+2018)\right) = v_2(a) + 1$ and hence again $\{a, b, ab, a(b+2018)\}$ can't be MC for a color in $\{odd, even\}$.

Remark.

It is still not known if any finite coloring of $\mathbb{N}$ contains a MC set of the form $\{a, b, a(b+1)\}$ or $\{a, b, ab, a(b+1)\}$.

TU Delft

8. Typing a's and b's

Dr. Daniel Valesin, Rijksuniversiteit Groningen

I type letters at random in my keyboard. Each letter I type is equally likely to be any of the 26 (lowercase) letters of the alphabet, chosen independently of what has been typed before. I stop typing when I type the letter 'a' three times in succession (that is, with no other letter in between). What is the expected number of times I type the letter 'b'?

Solution.
We can view the typing string as a sequence of "trials" or attempts to type aaa before typing b. For instance, say after some time after starting the typing, I type the first b, and at that point I have not typed aaa; this means that the first trial failed. I then start the second trial (independently of what happened before), which can again be a success or a failure; if it is a failure (that is, if again I type b before typing aaa), I start the third trial, and so on. The number of b's I type on total is equal to the number of trials minus one (since each failed trial corresponds to exactly one b and the last trial, which is the only success, consists of achieving aaa without any b's).

Let p be the probability that a trial succeeds. The probability that the first success occurs on the k-th trial, $k = 1, 2, 3, \ldots$, is $p(1-p)^{k-1}$. Hence,

$$\begin{aligned}\mathbb{E}(\#\text{b's before aaa}) = \mathbb{E}(\#\text{trials } -1) &= \mathbb{E}(\#\text{trials}) - 1\\ &= -1 + \sum_{k=1}^{\infty} kp(1-p)^{k-1}\\ &= -1 + p\sum_{k=0}^{\infty}\left(-\frac{d}{dp}(1-p)^k\right)\\ &= -1 - p\frac{d}{dp}\sum_{k=0}^{\infty}(1-p)^k\\ &= -1 - p\frac{d}{dp}\left(\frac{1}{p}\right) = \frac{1-p}{p}. \qquad (\star)\end{aligned}$$

(alternatively to this computation, one can simply say that the number of trials is a random variable following the geometric distribution with parameter p, which has expectation $1/p$).

Now we need to find p. To this end, let us first give a definition. Given a (finite) string of letters, the *number of accumulated* a's in the string is the number of successive a's that can be found when the string is read from right to left, before any other letter is found. For instance, the strings

mathematics, matematica, matematicaa

respectively have zero, one and two accumulated a's (let us also say that the empty string has zero accumulated a's). With this terminology, we have

$$p = \mathbb{P}\,(\text{trial will succeed} \mid \text{zero accumulated a's})$$

and we can define

$$\begin{aligned} q &= \mathbb{P}\,(\text{trial will succeed} \mid \text{one accumulated } \mathsf{a}) \\ r &= \mathbb{P}\,(\text{trial will succeed} \mid \text{two accumulated } \mathsf{a}\text{'s}) \end{aligned}$$

Note that p is equal to

$$\begin{aligned} &\mathbb{P}\left(\begin{array}{c}\text{trial will}\\ \text{succeed}\end{array}\middle|\,\text{one accumulated } \mathsf{a}\right) \cdot \mathbb{P}\left(\begin{array}{l}\text{next letter}\\ \text{will be } \mathsf{a}\end{array}\middle|\,\text{zero accumulated } \mathsf{a}\text{'s}\right) \\ &+ 0 \cdot \mathbb{P}\left(\begin{array}{c}\text{next letter}\\ \text{will be } \mathsf{b}\end{array}\middle|\,\text{zero accumulated } \mathsf{a}\text{'s}\right) \\ &+ \mathbb{P}\left(\begin{array}{c}\text{trial will}\\ \text{succeed}\end{array}\middle|\,\text{zero accumulated } \mathsf{a}\text{'s}\right) \cdot \mathbb{P}\left(\begin{array}{c}\text{next letter will}\\ \text{not be } \mathsf{a} \text{ or } \mathsf{b}\end{array}\middle|\,\text{zero accumulated } \mathsf{a}\text{'s}\right) \\ &= q \cdot \frac{1}{26} + 0 \cdot \frac{1}{26} + p \cdot \frac{24}{26}, \end{aligned}$$

that is,

$$p = \frac{1}{26} \cdot q + \frac{24}{26} \cdot p.$$

Similarly, we obtain

$$\begin{aligned} q &= \frac{1}{26} \cdot r + \frac{24}{26} \cdot p, \\ r &= \frac{1}{26} + \frac{24}{26} \cdot p. \end{aligned}$$

Solving this linear system yields $p = \frac{1}{704}$. Going back to ($\star$), the answer is thus 703.

9. Matrix-valued function in one variable

Leslie Molag MSc., Katholieke Universiteit Leuven

Let $f:\mathbb{R}\longrightarrow\mathbb{R}^{3\times 3}$ be a C^∞ function such that $f(0)=\mathbb{I}$ and $\det f(x)$ is constant.

(a) Prove that $f'(0)^3=0$ when f is a linear function, i.e. when $f(x)=\mathbb{I}+xf'(0)$.

(b) Show that it is not guaranteed that $f'(0)^3=0$.

(c) Is $f'(0)^3=0$ guaranteed under the additional requirement that $f''(0)=0$?

Solution.

(a) Since the determinant is invariant under basis transformations we may assume without loss of generality that $f'(0)$ is in Jordan normal form. Then it is clear that $\det f(x)$ can only be constant if all eigenvalues of $f'(0)$ are 0, which is equivalent to $f'(0)^3=0$.

(b) One-parameter families of determinant 1 matrices remind us of rotations. Indeed, if we define

$$f(x)=\begin{pmatrix}\cos(x) & -\sin(x) & 0\\ \sin(x) & \cos(x) & 0\\ 0 & 0 & 1\end{pmatrix},$$

then $f(0)=\mathbb{I}$ and $\det f(x)=1$ but $f'(0)^3\neq 0$. Another notable example, among others, is

$$f(x)=\begin{pmatrix}\lambda(x) & 0 & 0\\ 0 & \lambda(x)^{-1} & 0\\ 0 & 0 & 1\end{pmatrix}$$

where $\lambda(0)=1, \lambda'(0)\neq 0$ and $\lambda(x)$ is never 0, for example $\lambda(x)=1+x+x^2$.

(c) No. Before giving the counter example, let me show you the ideas behind it. If indeed $f''(0)=0$ then Taylor's theorem, applied to each component, would yield $f(x)=\mathbb{I}+f'(0)x+\mathcal{O}\left(x^3\right)$ as $x\to 0$. Let us denote $y=x^{-1}$, then we have

$$y^3=\det\left(yf(x)\right)=\det\left(y\mathbb{I}+f'(0)+\mathcal{O}\left(y^{-2}\right)\right),\qquad y\to\infty.$$

The reason to write it like this is that it is close to $y^3=\det\left(y\mathbb{I}+f'(0)\right)$, which is equivalent to the characteristic polynomial of $-f'(0)$ being equal to y^3. This would then imply immediately that $f'(0)^3=0$, since any matrix satisfies its own characteristic polynomial equation (in fact, problem (a) can be proved this way). The determinant is a sum of products of three components of $y\mathbb{I}+f'(0)+\mathcal{O}\left(y^{-2}\right)$. The $\mathcal{O}\left(y^{-2}\right)$ part of such a component can only be significant if the component is matched with two diagonal components. This implies that

$$y^3=\det\left(y\mathbb{I}+f'(0)+\mathcal{O}\left(y^{-2}\right)\right)=\det\left(y\mathbb{I}+f'(0)\right)+3\cdot y\cdot y\cdot\mathcal{O}\left(y^{-2}\right)+\mathcal{O}\left(y^{-1}\right),\quad y\to\infty.$$

Hence $\det(y\mathbb{I} + f'(0)) = y^3 + \mathcal{O}(1)$ as $y \to \infty$. Since the left-hand side is a polynomial we must conclude that $\det(y\mathbb{I} + f'(0)) = y^3 + \det f'(0)$. If the conditions of f somehow imply that $\det f'(0) = 0$ then the conclusion would be that $f'(0)^3 = 0$ always. As already announced, there will be a counter example to this statement. Let us begin by considering the simplest case $f'(0)^3 = \mathbb{I}$. What kind of non-trivial matrices satisfy such an identity? Well, we could try matrices that cyclically permute the basis vectors, i.e. we try

$$f'(0) = \sigma = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

A convenient way to make f satisfy both $f(0) = \mathbb{I}$ and $f'(0) = \sigma$, but in a not too trivial way, is to consider an exponential like $e^{x\sigma} = \mathbb{I} + x\sigma + \frac{1}{2}x^2\sigma^2 + \frac{1}{6}x^3\mathbb{I} + \ldots$, which by coincidence has the correct determinant. To see why, let us denote $\omega = e^{2\pi i/3}$. Since σ is diagonalizable with eigenvalues $1, \omega, \omega^2$ we know that $e^{x\sigma}$ is diagonalizable with eigenvalues $e^x, e^{\omega x}, e^{\omega^2 x}$. Then it follows that

$$\det e^{x\sigma} = e^x e^{\omega x} e^{\omega^2 x} = e^{(1+\omega+\omega^2)x} = 1,$$

where we have used that $1 + \omega + \omega^2 = 0$. Thus we have found yet another counter example for (b). However, since we want $f''(0) = 0$ we should alter this a little. Our guess is that the definition

$$f(x) = e^{x\sigma - \frac{1}{2}x^2\sigma^2}$$

works. Indeed, then $f''(0) = 0$ and since σ and σ^2 can be simultaneously diagonalized we also have

$$\det f(x) = e^{x - \frac{1}{2}x^2} e^{\omega x - \frac{1}{2}\omega^2 x^2} e^{\omega^2 x - \frac{1}{2}\omega x^2} = e^{(1+\omega+\omega^2)(x - \frac{1}{2}x^2)} = 1,$$

Thus, with this definition, $f(0) = \mathbb{I}$, $\det f(x)$ is constant and $f''(0) = 0$, but $f'(0)^3 = \sigma^3 = \mathbb{I} \neq 0$.

UNIVERSITEIT
GENT

VU VRIJE UNIVERSITEIT AMSTERDAM

Faculty of Science

667.000 werkza
Aantal zelfdodingen niet verder gestegen
10% meer containervervoer vanuit China
Aantal Nederlanders met een dubbele nationaliteit gestegen tot
9% meer omzet detailhandel
Verdubbeli
Feestdagen goed voor
Omzet industrie lager door prijsdaling
Kantines en catering doen weer goede zaken
Fors meer investeringen vooral in woningen
Koopwoningen ruim 3% duurder dan vorig jaar
Hoge opleiding: gezonder en tevreden
Recordomzetgroei voor IT-dienstverleners
Immigratie en emigratie naar recordhoogte
Minder jongeren verhuizen naar universiteitssteden
Laagste aantal faillissementen in bijna 7 jaar
Omzet hotels stijgt al 2 jaar op rij
R&D uitgave 12.235.000.000
Inflatie daalt naar 0,8%
Bevolking werkz
159.300 bedrijven opgericht
Koopkracht gestegen na 4 jaar daling
Milieubelastingen brengen bijna 24 miljard euro op
Broeikasgassen in 2014 bijna 5% lag
Binnenvaart vervoert minder door lage waterstanden
Gebruik levensl
Koopwoni
Reco

Werken aan de
basis van belangrijke
beslissingen

Het CBS maakt gebruik van big data zoals satellietdata en social media.
Wil jij een bijdrage leveren aan deze nieuwe innovaties?
Kijk voor stagemogelijkheden en vacatures op www.werkenbijhetcbs.nl.

cbs

10. Rational points

Prof. dr. Frans Oort, Universiteit Utrecht

Consider a prime number $p \equiv 3 \pmod 4$. Show:

$$\#\{(x,y) \in (\mathbb{F}_p)^2 \mid 1 = x^2 + y^2 + x^2y^2\} = p + 1;$$

we write $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Solution.
A solution $(x,y) \in (\mathbb{F}_p)^2$ satisfies

$$y^2 = \frac{1-x^2}{1+x^2}.$$

Note that there is no $e \in \mathbb{F}_p$ with $e^2 = -1$. For $x \in \{0,1,-1\}$ there are exactly four solutions:

$$(0,+1), \quad (0,-1), \quad (+1,0), \quad (-1,0).$$

Claim. For a fixed $a \notin \{0,1,-1\}$ there are exactly two solutions with (a,y) or $(1/a,y)$.
Proof. If (a,y_1) is a solution, then $y_1 \neq 0$ and $(a,-y_1)$ is another solution; moreover we have

$$\frac{1-x^2}{1+x^2} = -\frac{1-(1/x)^2}{1+(1/x)^2};$$

we see that in this case there are no solutions $(1/a,y_2)$; because if so, we would have $(y_1/y_2)^2 = -1$; this proves the claim.
Counting all solutions for all $a \in \mathbb{F}_p$ we obtain in total $4 + ((p-3)/2) \times 2 =$ p+1.

11. How about this question?

Prof. dr. Lex Schrijver, Universiteit van Amsterdam

Let L be a linear subspace of $(\mathbb{Z}/2\mathbb{Z})^n$. Call an element x of L *maximal* if the support of x is not contained in the support of any other element of L. Prove that the number of maximal elements of L is odd.

Solution. Let $e_1, \dots, e_n$ be a (standard) basis for $\mathbb{F}_2^n$. For a vector $v = e_{i_1} + ... + e_{i_k}$ denote $\text{supp}(v) = \{e_{i_1}, ..., e_{i_k}\}$ and $\text{supp}(0) = \emptyset$. Consider a subset S of $L \times L$ of ordered pairs (u, v) such that $\text{supp}(u) \cap \text{supp}(v) = \emptyset$. We note and prove a few facts.
(1) For u, the set

$$L_u = \{v \in L : \text{supp}(u) \cap \text{supp}(v) = \emptyset\}$$

is a vector subspace of L. Indeed, since

$$\text{supp}(v + w) \subset \text{supp}(v) \cup \text{supp}(w),$$

we have the following implication

$$\text{supp}(u) \cap \text{supp}(v) = \emptyset, \text{supp}(u) \cap \text{supp}(w) = \emptyset \Rightarrow \text{supp}(u) \cap \text{supp}(v + w) = \emptyset,$$

i.e. this set is closed for addition and clearly is closed with respect to multiplication by elements of $\mathbb{F}_2$ (these are only 0 and 1).
(2) If $u \in L$ is maximal element, then $L_u = \langle 0 \rangle$. Suppose there is a nonzero vector $v \in L_u$. Then for $u + v \in L$ holds $\text{supp}(u) \subsetneq \text{supp}(u + v)$, so u cannot be maximal.
(3) Let $u \in L$ be an element that is not maximal. There is an element $w \in L$ with $\text{supp}(u) \subsetneq \text{supp}(w)$ and then for a non-zero element $w - u$ in L holds $\text{supp}(u) \cap \text{supp}(w - u) = \emptyset$. So, vector space L_u is non-trivial and has even number of elements (it is equal to some $2^a \geq 2$).
(4) Number of elements of S is odd. Indeed, a relation defining S is symmetric, therefore there is an even number of pairs of distinct elements and there is only one pair (u, u) in S, precisely for $u = 0$.
(5) We can count a number of elements of S in the following way. For each $u \in L$, a number of vectors v with $\text{supp}(u) \cap \text{supp}(v) = \emptyset$ is exactly $\#L_u$. Then

$$\#S = \sum_{u \in L} \#L_u.$$

(6) Let the number of maximal elements be k. In the previous sum on the right hand side we have exactly k odd terms. As the sum is odd (we know that $\#S$ is odd), so k is odd, what we wanted to prove. □

Radboud University

Mathematics

Title/degree: Master of Science (MSc)
Duration: 2 years (120 EC), full-time
Start month: September
Language of instruction: English
Croho code: 66980

Gaining a solid, theoretical understanding of the field of mathematics and in-depth knowledge in an area of interest.

Discover the very heart of mathematics. Whether you want to immerse yourself in pure mathematics or want to discover its application in other disciplines, the Master's programme in Mathematics at Radboud University offers you several possibilities. Our Mathematics programme is known and respected for its quality and theoretical approach to mathematics with applications to selected fields. To get a feeling for the possible focus area's at Radboud University, please have a look at the overview of Master's theses.

change perspective

Why study Mathematics at Radboud University?

- Teaching takes place in a stimulating, collegial setting with small groups. This ensures that at Radboud University you'll get plenty of one-on-one time with your thesis supervisor.
- You partake in the Mastermath programme, meaning you can follow the best mathematics courses, regardless of the university in the Netherlands that offers them. It gives you the opportunity to interact with fellow mathematics students from all over the country.
- As a Mathematics Master's student of certain specialisations you get to work closely with the mathematicians and physicists of the Institute for Mathematics, Astrophysics and Particle Physics, as well as the computer scientists at the Institute for Computing and Information Sciences.
- More than 85% of our graduates find a job or a gain a PhD position within a few months of graduating.

www.ru.nl/wiskunde

KONINKLIJKE
HOLLANDSCHE MAATSCHAPPIJ
DER WETENSCHAPPEN

12. Restrict the extension

Prof. dr. Robert Tijdeman, Universiteit Leiden

Let $(v_n)_{n=0}^{\infty}$ be a sequence in $\mathbb{Z}^2$ with $v_0 = (1,0), v_1 = (0,1)$ and for $n = 1, 2, ...$

$$v_{n+1} = v_n + 2v_{n-1} \text{ or } v_{n+1} = v_n - 2v_{n-1}.$$

(a) Prove that for $n = 2, 3, \ldots$ the set

$$V_n := \left\{ \sum_{i=0}^{n-1} \varepsilon_i v_i \quad \text{with } \varepsilon_i \in \{0,1\} \text{ for } i = 0, 1, \ldots n-1 \right\}$$

consists of 2^n distinct points.

(b) Prove that the diameter of the convex hull of V_n for $n \geq 6$ is at least $(\sqrt{2})^n (> 1.414^n)$.

(c) Prove that the signs can be chosen in such a way that the diameter of the convex hull of V_n for $n = 2, 3, \ldots$ is at most 1.67×1.601^n.

P.S. The convex hull W of V is the smallest set such that if $v, w \in V$, then the connecting line segment belongs to W.

Solution.

(a) We start with some observations. Write $v_n = (p_n, q_n) \in \mathbb{Z}^2$ for $n = 0, 1, \ldots$.

Lemma 1. *We have* $p_{n+1}q_n - p_n q_{n+1} = \pm 2^n$ *and* $\gcd(p_n, q_n) = 1$ *for* $n = 1, 2, \ldots$.

Proof. We have $p_1 q_0 - p_0 q_1 = -1 = -2^0$ and $\gcd(p_1, q_1) = 1$.
If the minus sign holds, we have $p_{n+1}q_n - p_n q_{n+1} =$
$(p_n - 2p_{n-1})q_n - p_n(q_n - 2q_{n-1}) = 2(p_n q_{n-1} - p_{n-1}q_n)$ and the plus sign case is similar.
The first statement follows by induction on n.
Since $\gcd(p_n, q_n)$ divides $p_{n-1}q_n - p_n q_{n-1}$, it has to be a power of 2.
However, by construction the sequence of q_n's consists of odd integers for positive n.
Thus $\gcd(p_n, q_n) = 1$ for all n. □

A *lattice* $\Lambda \subset \mathbb{Z}^2$ is a set $\mathbb{Z}(a,b) + \mathbb{Z}(c,d)$ where $a, b, c, d \in \mathbb{Z}$ are such that (a,b) and (c,d) are linearly independent over $\mathbb{Z}^2$. A set $A \subset \mathbb{Z}^2$ is a *tile* for the lattice Λ if every $(x,y) \in \mathbb{Z}^2$ can be written uniquely as $(p,q) + r(a,b) + s(c,d)$ with $(p,q) \in A$ and $r, s \in \mathbb{Z}$.

Lemma 2. V_{n+1} *forms a tile for the lattice*

$$\Lambda_{n+1} := \mathbb{Z}(p_n + 2p_{n-1}, q_n + 2q_{n-1}) + \mathbb{Z}(p_n - 2p_{n-1}, q_n - 2q_{n-1})$$

for $n = 1, 2, \ldots$.

Proof. By induction on n. We have $V_2 = \{(0,0),(0,1),(1,0),(1,1)\}$ and this forms a tile for the lattice

$$\Lambda_2 = \mathbb{Z}(2,1) + \mathbb{Z}(2,-1) = \mathbb{Z}(2,1) + \mathbb{Z}(0,2).$$

Suppose the statement is true for n. Then V_{n+1}, the set of all the sums of subsets of $\{(p_0,q_0),(p_1,q_1),\dots,(p_n,q_n)\}$, forms a tile for

$$\Lambda_{n+1} = \mathbb{Z}(p_n + 2p_{n-1}, q_n + 2q_{n-1}) + \mathbb{Z}(p_n - 2p_{n-1}, q_n - 2q_{n-1}).$$

Let $p_{n+1} = p_n - 2p_{n-1}$, $q_{n+1} = q_n - 2q_{n-1}$, the other case is similar. Then, in self-evident notation,

$$\begin{aligned}\mathbb{Z}^2 &= \mathbb{Z}(p_n + 2p_{n-1}, q_n + 2q_{n-1}) + \mathbb{Z}(p_n - 2p_{n-1}, q_n - 2q_{n-1}) + V_{n+1}\\ &= \mathbb{Z}(2p_n - p_{n+1}, 2q_n - q_{n+1}) + \mathbb{Z}(p_{n+1}, q_{n+1}) + V_{n+1}\\ &= \mathbb{Z}(p_{n+1} - 2p_n, q_{n+1} - 2q_n) + \mathbb{Z}(2p_{n+1}, 2q_{n+1}) + \{(0,0),(p_{n+1},q_{n+1})\} + V_{n+1}\\ &= \mathbb{Z}(p_{n+1} - 2p_n, q_{n+1} - 2q_n) + \mathbb{Z}(p_{n+1} + 2p_n, q_{n+1} + 2q_n) + V_{n+2} = \Lambda_{n+2} + V_{n+2}.\end{aligned}$$

The statement of the lemma follows. □

By Lemma 1 the lattice determinant of Λ_{n+1} equals the absolute value of

$$\begin{vmatrix} p_n + 2p_{n-1} & q_n + 2q_{n-1} \\ p_n - 2p_{n-1} & q_n - 2q_{n-1} \end{vmatrix} =$$

$$4\begin{vmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{vmatrix} = 2^{n+1}.$$

On the other hand, the number of elements equals 2^{n+1}. Therefore all combinations of V_{n+1} are distinct.

(b) Attach to every point (p,q) the square

$$\{(x,y) : p - \frac{1}{2} \le x < p + \frac{1}{2}, q - \frac{1}{2} \le y < q + \frac{1}{2}\}.$$

Suppose the diameter of 2^n points in $\mathbb{Z}^2$ is $2R$. Then all 2^n corresponding unit squares are in a disc of radius $R + \frac{1}{2}\sqrt{2}$. Hence, comparing the areas,

$$2^n \le \pi(R + \frac{1}{2}\sqrt{2})^2 < \pi R^2 + 4.5R + 2 < 4R^2$$

for $R \ge 6$. Therefore the diameter $2R$ satisfies $2R > 2^{n/2} = (\sqrt{2})^n$.

(c) From now on we fix the sequence $(v_n)_{n=1}^{\infty}$. For $n = 2,3,\dots$ we choose $v_n = v_{n-1} - 2v_{n-2}$ if $p_{n-2}p_{n-1} + q_{n-2}q_{n-1} \ge 0$ and $v_n = v_{n-1} + 2v_{n-2}$ otherwise.

Lemma 3. *We have* $|v_n| \le 1.601^n$ *for* $n = 0,1,\dots$.

Proof. By induction on n. For $n = 0,1$ we have $|v_n| = 1$, for $n = 2$ we have $|v_2| = \sqrt{5} < (1.601)^2$.

Suppose the induction hypothesis holds for all values smaller than n. In particular, $|(v_{n-2}| \le 1.601^{n-2}, |v_{n-1}| < 1.601^{n-1}$.

Let α denote the angle between $-v_{n-2}$ and v_{n-1} if $p_{n-2}p_{n-1}+q_{n-2}q_{n-1} \geq 0$ and between v_{n-2} and v_{n-1} otherwise. Then $\cos\alpha \leq 0$ and, by plane geometry,

$$\begin{aligned} &|(p_n, q_n)|^2 = \\ &|(p_{n-1}, q_{n-1}|^2 + 4|(p_{n-2}, q_{n-2}|^2 + 4|(p_{n-1}, q_{n-1})| \cdot |(p_{n-2}, q_{n-2})| \cdot \cos\alpha \\ &\leq |(p_{n-1}, q_{n-1}|^2 + 4|(p_{n-2}, q_{n-2}|^2 \\ &\leq 1.601^{2n-2} + 4 \cdot 1.601^{2n-4} < 1.601^{2n}. \end{aligned}$$

□

Theorem 1. *The sequence $(v_n)_{n=1}^{\infty}$ can be chosen such that the diameter d of the resulting set V_n is at most $1.67 \cdot 1.601^n$ for all n.*

Proof. The diameter of V_n is determined by two endpoints which both are distinct subsums of $v_0, v_1, \ldots, v_{n-1}$. Hence the diameter d satisfies $d = |\pm v_{i_1} \pm v_{i_2} \cdots \pm v_{i_t}|$ with $0 \leq i_1 < i_2 < \cdots < i_t < n$.
By the previous lemma we obtain

$$d \leq |v_{i_1}| + |v_{i_2}| \cdots + |v_{i_t}| \leq \sum_{k=0}^{n-1} |v_k| \leq \sum_{k=0}^{n-1} 1.601^k < \frac{1.601^n}{.601}.$$

Hence $d < 1.67 \cdot 1.601^n$. □

Exercises made by:
Harry Smit MSc.
Ir. Harold de Boer
Prof. dr. Hendrik Lenstra
Prof. dr. Gunther Cornelissen
Prof. dr. Jaap Top
Eduardo Ruíz Duarte MSc.
Stijn Cambie MSc.
Dr. Daniel Valesin
Leslie Molag MSc.
Prof. dr. Frans Oort
Prof. dr. Lex Schrijver
Prof. dr. Robert Tijdeman

KWG

GQT

transtrend

13532057

332807 178208206 1511191 84356460617 299 20301227 1810358
313962 aaaccc 49344361 35563 2311820137 299 332807 6856967
996473518293 614712075356824928256 608399 989 14839 2806
45433063754 20301227 93497093 acc 49344361 35563 52131695

332807 178208206 1511191 9310186 299 20301227 2678207712468409
21529682515 bbc 1439568097 3337 231287 1633 299 332807 4045337
aa 116692587470 3337 86735 aaaac 7064094873146 56560603 1358
3337 86735 1633 67252 1238666 332807 33022 4573545608786 1633

332807 178208206 1511191 0123456789 299 332807 9394 608399
989 1282836161204411 299 332807 2945436432455 20819117 1032971504246 3337
1696781075 14839 2191657476063 3337 14839 11973866 3337 27522212277367368
14839 1154958430385193 1528111 14839 19505 332807 4443145 33

2 26298542

CRACK THE CODE

HINT:

aaaccc = 1000