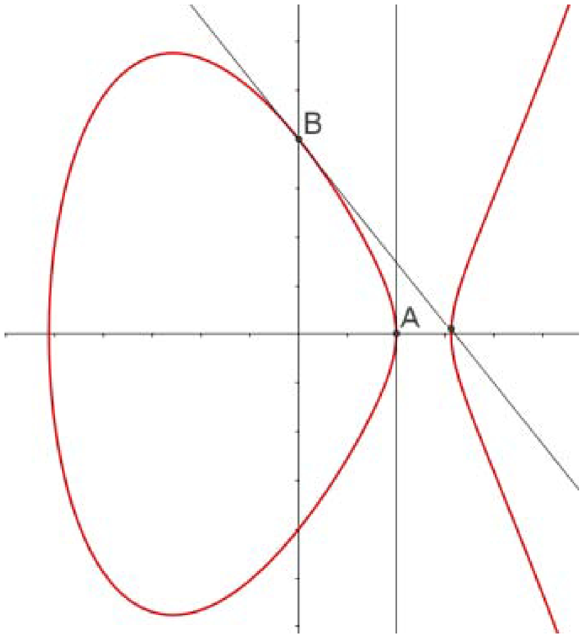
Bulletin

Mai 2013 – Mai 2013

N° **122**



VSMP — SSPMP — SSIMF

Verein Schweizerischer Mathematik– und Physiklehrkräfte
Société Suisse des Professeurs de Mathématique et de Physique
Società Svizzera degli Insegnanti di Matematica e Fisica

In dieser Nummer – *Dans ce numéro*

Kurse

Internet-Adressen – *Adresses Internet*
http://www.vsmp.ch — http://www.sspmp.ch — http://www.ssimf.ch

Page de titre
Investigations sur les courbes elliptiques (cf. page 19).

Chère collègue, Cher collègue,

Cet automne, la Société suisse des professeurs de l'enseignement secondaire sous l'impulsion des Sociétés suisses des profs de math/physique et de biologie/chimie organisent conjointement un grand con-grès sur le thème

«Science – Cuisine»

Celui-ci se tiendra à Sion du 23 au 26 octobre 2013.

Il tiendra lieu de cours de perfectionnement pour les branches mathématiques, physique, biologie et chimie.

Vous avez peut-être déjà reçu des flyers y relatifs, qui commencent à circuler dans vos écoles ou dans vos boîtes à lettres.

Ceux d'entre nous qui ont vécu le congrès de la SSPMP en 1999 sur le thème Musique-Physique et Mathématique (MUPHYMA) à Locarno s'en souviennent avec plaisir.

Nous espérons le même succès pour «Science – Cuisine». C'est pourquoi nous vous l'annonçons très tôt pour que vous puissiez déjà réserver les dates dans vos agendas.

La présentation globale du congrès est accessible ici:
www.vsmp.ch/science-cuisine

L'inscription se fera ensuite au CPS comme de coutume.

Pour le comité d'organisation:
Jean-Daniel Monod, président
Gordana Gerber, membre et coprésidente CRP

Liebe Kolleginnen,
Liebe Kollegen

Im Herbst dieses Jahres organisieren der Fachverein Biologie & Chemie und wir als VSMP gemeinsam einen Kongress zum Thema

«Science – Cuisine»

Dieser findet vom 23. bis 26. Oktober in Sion statt.

Diejenigen von Euch, welche beim VSMP-Kongress 1999 über Musik, Physik und Mathematik in Locarno dabei waren, denken heute noch gerne daran zurück. Und wir sind zuversichtlich, dass auch der diesjährige Kongress im Sinne einer Weiterbildungsveranstaltung ein starkes Erlebnis werden und uns allen lange in Erinnerung bleiben wird. Am besten trägt Ihr die Daten schon einmal in Eure Agenda ein.

Ein Kongress-Flyer ist diesem Bulletin beigelegt; Ihr findet ihn auch auf der Website des VSMP:
www.vsmp.ch/science-cuisine

Unter dieser Adresse findet Ihr auch noch viele weitere Hinweise zum geplanten Kongress (Programm, etc.).

Die Anmeldung (online) wird via 'link' über die Website der WBZ erfolgen.

Fürs Organisationskomitee:
Jean-Daniel Monod, Präsident
Hansjürg Stocker, Mitglied & Präsident des VSMP

Cara collega, caro collega

il prossimo autunno verrà organizzato congiuntamente dalla Società svizzera degli insegnanti di matematica e fisica e dalla Società svizzera degli insegnanti di biologia e chimica un congresso dal titolo

«Science – Cuisine»

Esso avrà luogo a Sion dal 23 al 26 ottobre.

È certamente ancora vivo, tra coloro vi hanno partecipato, il ricordo del congresso MuFiMa (Musica-Fisica-Matematica) tenutosi a Locarno nel 1999; siamo certi che anche il congresso previsto per ottobre, concepito come un'occasione di aggiornamento ed approfondimento, rappresenterà un'esperienza indimenticabile per tutti i partecipanti. Consigliamo quindi di riservare già fin d'ora le date summenzionate.

Troverete un opuscolo dedicato al congresso in allegato al presente Bollettino. Esso è inoltre consultabile all'indirizzo
www.vsmp.ch/science-cuisine

L'iscrizione dovrà essere effettuata online a partire dal sito CPS/WBZ.

Per il Comitato d'Organizzazione:
Jean-Daniel Monod, Presidente
Hansjürg Stocker, Membro e Presidente SSIMF

Deutschschweizerische Mathematikkommission (DMK) des
Vereins Schweizerischer Mathematik- und Physiklehrkräfte

Schwyz, im März 2013

Umfrage zum Lehrmittelkatalog der DMK

Geschätzte Mathematiklehrerkollegin!
Geschätzter Mathematiklehrerkollege!

Wir bedanken uns für das grosse Echo auf unsere Umfrage betreff Lehrmittelkatalog der DMK. Die eingegangenen Antworten werden nun von uns analysiert. Unser Ziel ist es, die daraus gewonnenen Erkenntnisse in kommende Buchprojekte einfliessen zu lassen. Besten Dank speziell auch für die teilweise ausführlichen Kommentare und differenzierten Bemerkungen.
Die persönlichen Gespräche, welche ich mit engagierten Lehrpersonen führen durfte, welche mich als Reaktion auf den Fragebogen kontaktiert haben, waren sehr interessant und zeigen mir, dass es sehr viele Lehrpersonen in der Schweiz gibt, für die der Beruf nicht mit dem Pausenläuten aufhört.
An dieser Stelle also auch ein genereller Dank an alle Mathematiklehrpersonen, die mit ihrer täglichen Arbeit wichtige Grundsteine legen und die Freude an der Mathematik weitergeben.

Mit freundlichen Grüssen

D. Grawehr

Daniela Grawehr
Präsidentin DMK

Verteilen von Objekten auf Schubladen

Pietro Gilardi, MNG Rämibühl

Zusammenfassung

n Objekte werden auf m Schubladen zufällig verteilt. Wie gross ist die Wahrscheinlichkeit, dass in jeder Schublade mindestens ein Objekt liegt?
Das Problem wird zuerst rekursiv gelöst. Aus der rekursiven Formel wird dann eine explizite Formel hergeleitet.

1 Einführung

In der Schule wird folgendes Problem behandelt:
n Objekte werden auf m Schubladen zufällig verteilt. Jemand öffnet eine Schublade. Wie gross ist die Wahrscheinlichkeit, dass die Schublade nicht leer ist?
Sei X die Anzahl Objekte in der Schublade. Es gilt:

$$p(X \geq 1) = 1 - p(X = 0) = 1 - \left(\frac{m-1}{m}\right)^n$$

Da die Schublade zufällig gewählt ist, könnte man denken, dass diese Zahl auch die Wahrscheinlichkeit ist, dass keine Schublade leer ist. Der Fall $n = m = 3$ wiederlegt dies:
Die Wahrscheinlichkeit, dass keine Schublade leer ist, ist $3!\left(\frac{1}{3}\right)^3 = \frac{6}{27}$.
Die obige Formel liefert hingegen die Wahrscheinlichkeit $\frac{19}{27}$.
Die Formel für die Wahrscheinlichkeit, dass keine Schublade leer ist, ist im allgemeinen Fall komplizierter und wird unten hergeleitet.

2 Rekursive Formel

Man betrachte folgende Bezeichnungen:

- A_n^m : Jede der m Schubladen enthält mindestens eines der n Objekte, $m \geq 2$, $n \geq 1$.
- B_k^m: Die erste der m Schubladen enthält k Objekte.
- $p(m,n) = p(A_n^m)$ (Wahrscheinlichkeit von A_n^m)

Für $m = 2$ gilt:

$$p(2,n) = 1 - \left(\frac{1}{2}\right)^{n-1} = 1 - 2\left(\frac{1}{2}\right)^{n}$$

Für $m \geq 3$ kann einer der folgendenden $(n-1)$ Fälle eintreten:
Die erste Schublade enthält k Objekte und die restlichen $(n-k)$ Objekte werden auf die restlichen $(m-1)$ Schubladen verteilt, $1 \leq k \leq n-1$. Es gilt:

$$p(m,n) = \sum_{k=1}^{n-1} p(B_k^m) \cdot p(m-1, n-k)$$

Die Wahrscheinlichkeit von B_k^m ist leicht zu bestimmen. Es gilt:

$$p(B_k^m) = \binom{n}{k}\left(\frac{1}{m}\right)^{k}\left(\frac{m-1}{m}\right)^{n-k}$$

Somit sieht die Rekursionsgleichung wie folgt aus:

$$p(m+1,n) = \sum_{k=1}^{n-1} \binom{n}{k}\left(\frac{1}{m+1}\right)^{k}\left(\frac{m}{m+1}\right)^{n-k} p(m, n-k)$$

3 Explizite Formel

Die rekursive Berechnung von $p(m,n)$ ist selbst für ein CAS-Programm wie MAPLE aufwendig. Um die explizite Formel für $p(m,n)$ zu bestimmen werden zuerst $p(3,n)$, $p(4,n)$ und $p(5,n)$ explizit bestimmt. Es gilt:

$$p(3,n) = \sum_{k=1}^{n-1} \binom{n}{k}\left(\frac{1}{3}\right)^{k}\left(\frac{2}{3}\right)^{n-k} p(2, n-k)$$

Für $p(2, n-k)$ wird der hergeleitet Ausdruck eingesetzt:

$$p(3,n) = \sum_{k=1}^{n-1} \binom{n}{k}\left(\frac{1}{3}\right)^{k}\left(\frac{2}{3}\right)^{n-k}\left(1 - 2\left(\frac{1}{2}\right)^{n-k}\right)$$

Wenn die Klammern aufgelöst werden, bekommt man:

$$p(3,n) = \sum_{k=1}^{n-1} \binom{n}{k} \left(\frac{1}{3}\right)^k \left(\frac{2}{3}\right)^{n-k} - 2 \cdot \sum_{k=1}^{n-1} \binom{n}{k} \left(\frac{1}{3}\right)^k \left(\frac{2}{3}\right)^{n-k} \left(\frac{1}{2}\right)^{n-k}$$

$$\Updownarrow$$

$$p(3,n) = \sum_{k=1}^{n-1} \binom{n}{k} \left(\frac{1}{3}\right)^k \left(\frac{2}{3}\right)^{n-k} - 2 \cdot \sum_{k=1}^{n-1} \binom{n}{k} \left(\frac{1}{3}\right)^k \left(\frac{1}{3}\right)^{n-k}$$

Das Summenzeichen lässt sich eliminieren, indem man folgende Formel benutzt:

$$\sum_{k=1}^{n-1} \binom{n}{k} x^k y^{n-k} = (x+y)^n - x^n - y^n$$

Es gilt:

$$p(3,n) = 1 - \left(\frac{1}{3}\right)^n - \left(\frac{2}{3}\right)^n - 2 \cdot \left(\left(\frac{2}{3}\right)^n - \left(\frac{1}{3}\right)^n - \left(\frac{1}{3}\right)^n\right)$$

$$\Updownarrow$$

$$p(3,n) = 3 \cdot \left(\frac{1}{3}\right)^n - 3 \cdot \left(\frac{2}{3}\right)^n + 1 = 3 \cdot \left(\frac{1}{3}\right)^n - 3 \cdot \left(\frac{2}{3}\right)^n + \left(\frac{3}{3}\right)^n$$

Analoge Berechnungen führen zu:

$$p(4,n) = -4 \cdot \left(\frac{1}{4}\right)^n + 6 \cdot \left(\frac{2}{4}\right)^n - 4 \cdot \left(\frac{3}{4}\right)^n + \left(\frac{4}{4}\right)^n$$

$$p(5,n) = 5 \cdot \left(\frac{1}{5}\right)^n - 10 \cdot \left(\frac{2}{5}\right)^n + 10 \cdot \left(\frac{3}{5}\right)^n - 5 \left(\frac{4}{5}\right)^n + \left(\frac{5}{5}\right)^n$$

Es liegt die Vermutung nahe:

$$p(m,n) = (-1)^m \sum_{k=1}^{m} (-1)^k \binom{m}{k} \left(\frac{k}{m}\right)^n$$

4 Beweis

Die explizite Formel wird mit vollständiger Induktion bewiesen.

- Für $m = 2$ ist der Fall klar.

- Induktionsschritt

$$p(m+1,n) = \sum_{k=1}^{n-1} \binom{n}{k} \left(\frac{1}{m+1}\right)^k \left(\frac{m}{m+1}\right)^{n-k} p(m,n-k)$$

$$\Updownarrow$$

$$p(m+1,n) = \sum_{k=1}^{n-1} \binom{n}{k} \left(\frac{1}{m+1}\right)^k \left(\frac{m}{m+1}\right)^{n-k} (-1)^m \sum_{i=1}^{m} (-1)^i \binom{m}{i} \Bigg($$

$$\Updownarrow$$

$$p(m+1,n) = (-1)^m \sum_{k=1}^{n-1} \sum_{i=1}^{m} (-1)^i \binom{m}{i} \binom{n}{k} \left(\frac{1}{m+1}\right)^k \left(\frac{i}{m+1}\right)^{n-k}$$

$$\Updownarrow$$

$$p(m+1,n) = (-1)^m \sum_{i=1}^{m} (-1)^i \binom{m}{i} \sum_{k=1}^{n-1} \binom{n}{k} \left(\frac{1}{m+1}\right)^k \left(\frac{i}{m+1}\right)^{n-k}$$

$$\Updownarrow$$

$$p(m+1,n) = (-1)^m \sum_{i=1}^{m} (-1)^i \binom{m}{i} \left(\left(\frac{1+i}{m+1}\right)^n - \left(\frac{1}{m+1}\right)^n - \Bigg(\frac{i}{m+}\right.$$

Der Koeffizient von $\left(\frac{i}{m+1}\right)^n$ wird mit a_i bezeichnet. Man muss zeigen:

$$a_i = (-1)^{m+1}(-1)^i \binom{m+1}{i} \qquad 1 \leq i \leq m+1$$

Der Term $\left(\frac{1}{m+1}\right)^n$ kommt in jedem Summand mit $i > 1$ einmal und im Summand mit $i = 1$ zweimal vor. Es gilt also

$$a_1 = (-1)^m \left(m - \sum_{i=1}^{m} (-1)^i \binom{m}{i} \right)$$

Da

$$\sum_{i=0}^{m} (-1)^i \binom{m}{i} = 1 + \sum_{i=1}^{m} (-1)^i \binom{m}{i} = 0$$

ist

$$\sum_{i=1}^{m} (-1)^i \binom{m}{i} = -1$$

Also:

$$a_1 = (-1)^m (1+m) = (-1)^{m+1}(-m-1) = (-1)^{m+1}(-1)^1(m+1)$$

$$\Updownarrow$$

$$a_1 = (-1)^{m+1}(-1)^1\binom{m+1}{1}$$

Der Term $\left(\dfrac{i}{m+1}\right)^n$, $1 < i \leq m$ kommt zweimal vor. Es gilt:

$$a_i = (-1)^m \left((-1)^{i-1}\binom{m}{i-1} - (-1)^i\binom{m}{i}\right)$$

$$\Updownarrow$$

$$a_i = (-1)^{m+1} \left((-1)^{i}\binom{m}{i-1} + (-1)^i\binom{m}{i}\right)$$

$$\Updownarrow$$

$$a_i = (-1)^{m+1}(-1)^i\binom{m+1}{i}$$

Der Term $\left(\dfrac{m+1}{m+1}\right)^n$ kommt genau einmal vor. Es gilt:

$$a_{m+1} = (-1)^m(-1)^m\binom{m}{m}(= 1)$$

Somit gilt:

$$p(m+1,n) = (-1)^{m+1}\sum_{k=1}^{m+1}(-1)^k\binom{m+1}{k}\left(\frac{k}{m+1}\right)^n$$

und die Formel ist bewiesen.

Aha! Mathematatik! – Teil IV.

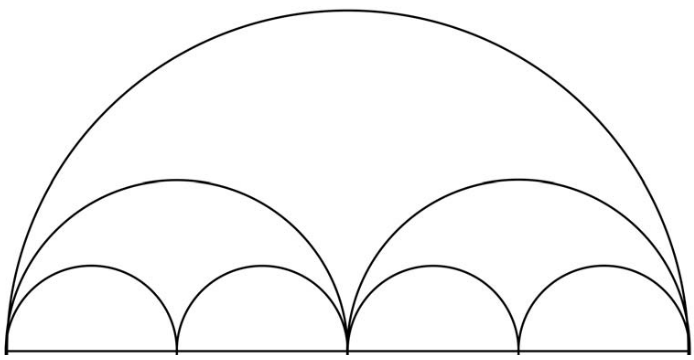
Klein-Archimedes berechnet π.

Urs Stammbach

Archimedes minor, heute Klein-Archimedes genannt, hatte viel Gutes von seinem grossen Namensvetter gehört. Besonders die Art und Weise, wie Archimedes die Zahl π approximativ bestimmte, hatte ihn nachhaltig beeindruckt; es ist ja tatsächlich staunenswert, dass mehr als 2000 Jahre später der Archimedische Wert von $3\frac{1}{7}$ immer noch benützt wird. Ganz klar, Klein-Archimedes wollte in dieser Sparte eine ähnlich grosse Tat vollbringen. Er wusste natürlich, dass die Verhältniszahl zwischen Umfang U und Durchmesser d eines Kreises unabhängig von der Grösse des Kreises ist: $U = \pi \cdot d$. Das hatte ja ebenfalls sein Vorbild Archimedes gezeigt. Aber dessen nachfolgende Überlegungen, diese Verhältniszahl mit Hilfe von ein- und umbeschriebenen regelmässigen Vielecken zu berechnen schien ihm denn doch etwas kompliziert. Klein-Archimedes schwebte Einfacheres vor. Entspannt im Bade liegend machte er sich die folgenden Überlegungen. Man hatte heute morgen in der Mathematikstunde eine interessante Übungsaufgabe gelöst, die möglicherweise seinen Zwecken diente. Wie war das genau:

Man betrachtet einen Halbkreis, Durchmesser d; die Länge des Halbkreises ist $\frac{1}{2} \cdot \pi \cdot d$. Man halbiere d und zeichne über jeder Hälfte wiederum einen Halbkreis. Jeder dieser Halbkreise hat die Länge $\frac{1}{2} \cdot \pi \cdot \frac{d}{2}$. Es folgt:

Die Summe der Längen der beiden kleinen Halbkreise ist gleich der Länge des grossen Halbkreises.



So lautete in der heutigen Mathematikstunde das Resultat der Übungsaufgabe. Klein-Archimedes überlegte sich: Wenn man dieses Verfahren wiederholt, indem man über jedem Viertel des Durchmessers des ursprünglichen Halbkreises je wieder einen Halbkreis zeichnet, so ist nach obigem die Summe der Längen der *vier* kleinen Halbkreise gleich der Länge des ursprünglichen grossen Halbkreises.

Und nun kann man dieses Verfahren sukkzessive in der gleichen Art wiederholen! Bei diesem unendlich wiederholten Prozess strebt dann offenbar jeder Punkt der aus Halbkreisen zusammengesetzten Kurve gegen einen Punkt des Durchmessers. Die Limeskurve fällt also mit dem Durchmesser des ursprünglichen Halbkreises zusammen. Die Summe der Längen der einzelnen Halbkreise ändert sich bei den einzelnen Schritten nicht, sie bleibt immer $\frac{1}{2} \cdot \pi \cdot d$. Die Länge der Limeskurve ist deshalb ebenfalls $\frac{1}{2} \cdot \pi \cdot d$. Aber andererseits ist die Limeskurve gerade der Durchmesser des ursprünglichen Halbkreises, und dessen Länge ist d.

Es ergibt sich so offenbar die Gleichung

$$\frac{1}{2} \cdot \pi \cdot d = d \ .$$

Also folgt $\pi = 2$.

Klein-Archimedes verzichtete darauf, *Heureka!* zu rufen; er fand, das sei nicht mehr ganz zeitgemäss. Trotzdem stieg er schleunigst aus der Badewanne und machte sich daran, seine Überlegungen aufzuschreiben. So ganz wohl war ihm bei der Sache allerdings nicht, denn so stark konnte sich doch sein älterer Namensvetter nicht geirrt haben! Da musste er selber bei seinen Überlegungen einen Fehler gemacht haben; den galt es zu finden! Aber wo lag er? Intensiv brütete er über seinen Papieren, und wenn ihn Kameraden stören wollten, lag ihm das *Noli turbare circulos meos* zuvorderst auf der Zunge, auch wenn *seine* Kreise nur Halbkreise waren!

Er brauchte Hilfe! Er fand sie bei seinem älteren Bruder, der eben begonnen hatte, Mathematik zu studieren. Hier lernte er dann: Die Länge einer gekrümmten Kurve ist mathematisch mit Hilfe von Streckenzügen definiert, die Punkte der Kurve durch Strecken, also durch *Geraden*stücke verbindet. In einem mathematisch korrekten Vorgehen muss eine Folge derartiger Streckenzüge herangezogen werden, bei der das Maximum der Länge der einzelnen Strecken gegen Null strebt. Die Länge der Kurve ist dann definiert als Grenzwert der Summe der Längen der einzelnen Strecken. So ging damals auch der grosse Archimedes vor; er approximierte die Kreislinie durch den Umfang von ein- und umbeschriebenen regelmässigen Vielecken. Dieses Vorgehen war mathematisch korrekt. Klein-Archimedes hingegen hat in mathematisch unerlaubter Weise den Streckenzug durch eine aus einzelnen Halbkreisen bestehende Kurve ersetzt. Im Grenzübergang hat er mit einer derartigen Kurve den Kreisdurchmesser approximiert und so dessen Länge "bestimmt". Das war sein Fehler! – Wenn Klein-Archimedes ebenso berühmt werden will wie sein grosser Namensvetter, so wird er wohl noch andere, bedeutendere Leistungen zu vollbringen haben.

Zu Archimedes, sowohl zu seiner Biographie wie auch zu den hier angedeuteten Legenden, vergleiche man die Internetseiten:

http://de.wikipedia.org/wiki/Archimedes
http://www-history.mcs.st-andrews.ac.uk/Biographies/Archimedes.html

Walser, Hans. Fibonacci, Zahlen und Figuren, 98 Seiten, EUR 14.50, Edition am Gutenbergplatz Leipzig EAGLE, 2012, EAGLE 060, ISBN 978-3-937219-60-8

Leonardo di Pisa, genannt Fibonacci, ist Kaufmannssohn, Rechenmeister, Hofmathematiker von Friedrich Barbarossa und so eine wichtige Persönlichkeit für die Mathematikgeschichte. Auf Reisen im Magreb, Spanien und der Provence erlebte er eine technologische Überlegenheit arabischer Kaufleute, die an Stelle von römischen Zahlen und einem Rechenbrett mit Kenntnissen der orientalischen Mathematik vertraut waren, das Dezimalsystem und die indisch-arabische Notation benutzten. Fibonacci eignete sich dieses Wissen an und setzte sich zum Ziel, seine neu erworbenen Kenntnisse in seiner Heimat zu vermitteln. Bemerkenswert ist das aus dieser didaktischen Absicht motivierte Rechenbuch, *Liber Abaci*, der bedeutendste mittelalterliche mathematische Text aus Europa. In einer der Aufgaben wird ein frühes Modell der Populationsentwicklung formuliert. In einem Gehege befindet sich ein Paar junge Kaninchen, ein Männchen und ein Weibchen. In einem Monat werden sie erwachsen. Jedes Paar von erwachsenen Kaninchen wirft jeden Monat ein Paar Junge, ein Männchen und ein Weibchen. Angenommen, kein Kaninchen stirbt. Wie viele Kaninchen gibt es im Gehege nach 12 Monaten? Fibonaccis Kaninchen haben wenigstens im mathematischen Universum Unsterblichkeit erlangt in Gestalt der Fibonaccifolge mit der bekannten rekursiven Definition $a_1 := a_2 := 1$ und $a_{n+1} := a_n + a_{n-1}$ für $n > 2$.

Übrigens, die von Fibonacci angestebte Erneuerung der Rechenpraxis beanspruchte in ganz Europa rund 400 Jahre, bis die Vorteile, die Fibonacci rasch erkannte, sich allgemein durchsetzten.

Heute ist aber die Fibonaccifolge noch immer Prototyp für eine lineare Rekursion. Wie viel Potenzial in diesem Thema steckt, zeigt die Existenz einer Zeitschrift, des *Fibonacci Quarterly,* das sich, wie der Text von Hans Walser, mit den zahlreichen Aspekten des Themas und seinen vielfältigen Verzweigungen befasst. Der vorliegende Text wendet sich an Studierende, Schülerinnen und Schüler, Lehrpersonen und interessierte Laien.

Hans Walser bearbeitet den Stoff, wie einen Diamanten, elementarer Substanz, die durch die Kunst des Schleifers die Fähigkeit zum Funkeln und zur Lichtbrechung erst entfalten kann. Zwei Eigenschaften des Textes sind augenfällig: die schlichte und präzise Sprache und die spielerische Leichtigkeit, mit der Themen vernetzt, abgewandelt oder ästhetisch ansprechend und eindrücklich dargestellt werden. Aus Zahlentheorie und Algebra wird unvermittelt Geometrie, wird wieder Algebra oder Analysis oder Kombinatorik. Ist diese Ambivalenz und stete Wechsel das Geheimnis des Funkelns dieses Diamanten?

Der Text beginnt mit der klassischen Fibonaccifolge und verschiedenen Visualisierungen. Die erste geometrische Verwandlung handelt vom Ansetzen von Quadraten auf Polygonseiten. Bald trifft Fibonacci auf Pythagoras und Querbezüge zum Goldenen Schnitt. Im Abschnitt *Ausdünnen und Verdichten* werden Teilfolgen der Fibonaccifolge studiert oder die Fibonaccifolgen werden interpoliert, sodass wir die reellwertigen oder komplexwertigen Verwandten kennen lernen. Fibonaccifolgen in Restklassenringen $\mathbb{Z}/n\mathbb{Z}$ werden periodisch. Bezüge zu verwandten linearen Rekursionen, die periodisches Verhalten zeigen, runden das Thema ab.

Ein ausführliches Zitat aus Moritz Cantors *Vorlesungen über die Geschichte der Mathematik* (1900) ist als biografische und historische Notiz zu Fiboancci angefügt.

Das Thema entpuppt sich in Walsers Aufbereitung als ein reichhaltiger Mikrokosmos, geeignet auch für Begabtenförderung, anregend für Unterrichtsprojekte oder Maturaarbeiten. Der Autor geht mit herausfordernden Fragen auf die Leser zu und regt deren eigene Gedanken an, bietet dann aber auch Hilfestellungen und seine eigenen Lösungen an.

Dieses kleine Buch hat mir beim Lesen grosse Freude bereitet.

H.R. Schneebeli, Wettingen

Bettinaglio, Marco und Kirchgraber, Urs: Perspektive verstehen. Ein anschaulicher Zugang zur Mathematik perspektivischer Bilder mit Anwendungen. Zürich: Orell Füssli 2011. ISBN 978-3-280-04069-0. 144 Seiten. Broschiert. 21.0 × 29.7 cm. 1. Auflage. November 2011. CHF 39.80, € 29.80.

Das vorliegende Buch, als Begleit- und Anregungsbuch für Lehrpersonen gedacht, hilft mit, die im Unterricht vernachlässigte Raumgeometrie zu fördern.

Die Zentralperspektive (ars perspectiva) wird konsequent nach dem Grundsatz „zeichnen, was man sieht“ eingeführt; eine ansprechende Art, Raumgeometrie ohne explizite Bezugnahme auf die etwas verstaubt wirkende Darstellende Geometrie zu betreiben.

Die Entwicklung der Zentralperspektive zwischen 1350 und 1450 erscheint aus unserer zeitlichen Distanz von mehreren Jahrhunderten zwar als Quantensprung, war aber damals im Einzelnen mühsam und kleinschrittig. Dies wird am Beispiel von Paolo Uccello illustriert.

Im Sinne einer didaktischen Fokussierung werden hauptsächlich quaderförmige Objekte dargestellt. Dies wird oft illustriert mit architektonischen Entwürfen und Bauten. Auf Formeln wird weitgehend verzichtet. Es werden aber Abbildungsgleichungen der projektiven Geometrie exemplarisch vorgestellt und diskutiert.

Erfreulich ist die Bezugnahme auf die Lochkamera und die Einführung zugehöriger technischer Begriffe wie etwa der Brennweite.

Das Buch hat hohen ästhetischen Anspruch. Es ist weitgehend zweispaltig mit einer Text- und einer Illustrationsspalte. Die Situationsdarstellung „Objekt / Bildebene / Beobachter“ geschieht im Schrägbild.

Zeichnungsunterlagen und Lösungen sind kapitelweise auf dem Netz gratis als pdf abrufbar.

Kritikpunkte: Die Darstellung der Kugel, ein Sorgenkind in vielen Lehrmittelillustrationen und Geometriebüchern, wird nicht besprochen. Bei Problemen der Entzerrung perspektivischer Bilder wäre im Sinne eines aktuellen Praxisbezuges der Hinweis auf Bedeutung die Fotogrammetrie im Ingenieurwesen und in der Kartografie angebracht.

Ich wünsche diesem schönen Buch eine weite Verbreitung an den Schulen.

Basel, 4. Januar 2013
Hans Walser

DPK

Zähmen der Unendlichkeit

Martin Lieberherr, Andreas Vaterlaus, Clemens Wagner, ETH Zürich
limartin@ethz.ch, clemens.wagner@phys.ethz.ch, vaterlaus@phys.ethz.ch

Einführung

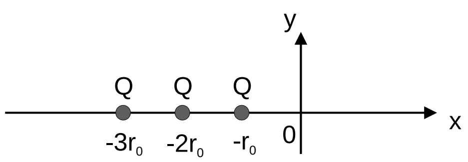
Einige Eltern vermuten bei ihrem Nachwuchs ein unendliches Potential und schicken ihn sogleich aufs Gymnasium. Die Mittelschulen wenden dann eine Technik namens „Renormierung" an, welche zeigt, dass dieses Potential meist eine Frage des Blickwinkels ist. Von einem analogen, elektrostatischen Problem soll hier die Rede sein.

Wir stiessen auf das Problem, als wir Aufgaben im Rahmen des produktiven Übens entwarfen. Die Idee des produktiven Übens stammt aus der Mathematik, wo man versucht, das drillmässige Lösen von unabhängigen Aufgaben zu ersetzen durch verknüpfte Aufgaben, die eine Gesetzmässigkeit beinhalten (1). Die Schülerinnen und Schüler sollen nach der Gesetzmässigkeit suchen und dabei gar nicht mehr realisieren, dass die Aufgabe eigentlich einen anderen Zweck verfolgt. Ein weiterer Vorteil ist, dass Resultate, die nicht der Gesetzmässigkeit entsprechen, identifiziert werden können. Die Schülerinnen und Schüler beginnen automatisch ihre Resultate zu reflektieren (2).

Wir versuchten, das Prinzip „produktives Üben" auf Physikaufgaben, insbesondere aus der Elektrostatik, zu übertragen. Die Idee war, auf der x-Achse in regelmässigen Abständen Punktladungen zu platzieren und die elektrische Feldstärke oder das elektrische Potential im Nullpunkt zu bestimmen. Der interessante Fall ist der, bei dem die Anzahl Ladungen nach unendlich geht. Da die elektrische Feldstärke quadratisch mit der Distanz abnimmt ($E \propto 1/r^2$), ist klar, dass die Summe der Feldstärken am Nullpunkt konvergiert. Betrachtet man jedoch das elektrische Potential, welches umgekehrt proportional mit der Distanz abfällt ($\varphi \propto 1/r$) dann divergiert diese Reihe. Dies scheint ein Widerspruch zu sein, denn wir wissen, dass die Feldstärke der negative Gradient des Potentials ist. Wie berechnet man die Feldstärke, wenn das Potential unendlich ist? Wir wollen nun zeigen, wie man diesen vermeintlichen Widerspruch auflöst, indem man den Nullpunkt des Potentials geeignet wählt.

Problem

Die Aufgabe baut man auf, indem man zuerst eine Ladung bei $-r_0$ platziert und das elektrische Feld im Nullpunkt bestimmen lässt. In der nächsten Teilaufgabe setzt man eine weitere Ladung bei $-2r_0$ und lässt wiederum das elektrische Feld im Nullpunkt berechnen. Anschliessend lässt man die Aufgabe für n Ladungen an den Punkten $-r_0$, $-2r_0$, ..., $-(n-1)r_0$, $-nr_0$ bestimmen (siehe **Figur 1**).



Figur 1: Problem der Ladungskette. Die Punktladungen haben alle denselben Wert Q und sind an den Positionen $x = -r_0$, $-2r_0$, $-3r_0$ usw. Es soll das elektrische Potential und die elektrische Feldstärke im Nullpunkt des Koordinatensystems berechnet werden.

Zuletzt lässt man, wie oben erwähnt, die Anzahl n der Ladungen gegen unendlich gehen. Für die elektrische Feldstärke erhält man (3)

$$E = \frac{1}{4\pi\varepsilon_0}\left(\frac{Q}{r_0^{\,2}} + \frac{Q}{(2r_0)^2} + \frac{Q}{(3r_0)^2} + \cdots\right) = \frac{1}{4\pi\varepsilon_0}\frac{Q}{r_0^2}\left(\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots\right) = \frac{1}{4\pi\varepsilon_0}\frac{Q}{r_0^2}\frac{\pi^2}{6}$$

Die unendliche Reihe für die Feldstärke konvergiert. Analog hätte die Reihe für das elektrische Potential im Nullpunkt folgendes Aussehen

$$\varphi(0) = \frac{1}{4\pi\varepsilon_0}\left(\frac{Q}{r_0} + \frac{Q}{2r_0} + \frac{Q}{3r_0} + \cdots\right) = \frac{1}{4\pi\varepsilon_0}\frac{Q}{r_0}\left(\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots\right)$$

Die Summe stellt die harmonische Reihe dar, die bekanntlich divergiert. Wie ist es möglich, dass das Potential divergiert, die elektrische Feldstärke jedoch endlich ist? Physikalisch muss es einen Ausweg geben, denn wo eine Feldstärke ist, ist auch ein Potential.

Lösung

Das elektrische Potential ist nur bis auf eine additive Konstante bestimmt. Um sie zu geeignet auszusuchen, benutzen wir die bekannte Beziehung (4)

$$\lim_{n\to\infty}\left(1 + \frac{1}{2} + \frac{1}{3} + .. + \frac{1}{n} - \ln(n)\right) = \gamma\,.$$

Die Zahl γ = 0.57721.. heisst Euler-Mascheroni Konstante. Der Trick besteht nun darin, von der n-ten Partialsumme den Wert $\ln(n)$ zu subtrahieren. Wir schreiben das elektrische Potential neu

$$\phi_n(0) = \frac{1}{4\pi\varepsilon_0}\frac{Q}{r_0}\left(\sum_{i=1}^{n}\frac{1}{i} - \ln(n)\right).$$

Offensichtlich können wir nun das Potential für $n \to \infty$ bestimmen

$$\varphi(0) = \frac{1}{4\pi\varepsilon_0}\frac{Q}{r_0}\lim_{n\to\infty}\left(\sum_{i=1}^{n}\frac{1}{i} - \ln(n)\right) = \frac{1}{4\pi\varepsilon_0}\frac{Q}{r_0}\gamma.$$

Das scheinbare Problem ist also gelöst, denn bei passender Normierung bleibt das elektrische Potential endlich.

Kontrolle

Nun möchten wir noch zeigen, dass man tatsächlich über die Ableitung des Potentials die elektrische Feldstärke erhält. Dazu müssen wir das Potential auch in der Umgebung des Nullpunktes (bei x) kennen. Mit der Abkürzung $z = x/r_0$ wechseln wir auf dimensionslose Zahlen.

$$\varphi_n(x) = \frac{1}{4\pi\varepsilon_0}\left(\frac{Q}{r_0 + x} + \frac{Q}{2r_0 + x} + \cdots + \frac{Q}{nr_0 + x}\right), \quad x > -r_0$$
$$= \frac{1}{4\pi\varepsilon_0}\frac{Q}{r_0}\left(\frac{1}{1+z} + \frac{1}{2+z} + \cdots + \frac{1}{n+z}\right), \quad z = \frac{x}{r_0} > -1$$

Auch diese Reihe divergiert für alle festen z für $n \to \infty$. Die Partialsumme lässt sich durch die so genannte Digamma-Funktion ψ^0 ausdrücken. Die Digamma-Funktion hat folgende Eigenschaften (5)

$$\psi^0(z) = \frac{\frac{d\,\Gamma(z)}{dz}}{\Gamma(z)} \qquad \psi^0(z) = \ln(z) - \frac{1}{2z} - \ldots \quad (z \to \infty)$$

$$\psi^0(1) = -\gamma \qquad \psi^1(z) = \frac{d\psi^0(z)}{dz}$$

$$\psi^0(n+1+z) = \frac{1}{n+z} + \frac{1}{n-1+z} + \frac{1}{n-2+z} + \ldots + \frac{1}{1+z} + \psi^0(1+z)$$

Dass sie auftritt und mit der bekannteren Gammafunktion $\Gamma(z)$ verwandt ist, verwundert nicht, denn sie ist bei allen negativen, ganzen Zahlen (bei den Positionen der Ladungen) nicht definiert. Mit Hilfe der Digamma-Funktion lässt sich die n-te Partialsumme folgendermassen schreiben:

$$\phi_n(z) = \frac{1}{4\pi\varepsilon_0}\frac{Q}{r_0}\left(\psi^0(n+z+1) - \psi^0(z+1)\right),$$

Für grosse n nähert sich das Potential asymptotisch dem Ausdruck

$$\varphi_n(z) = \frac{1}{4\pi\varepsilon_0}\frac{Q}{r_0}\left(\ln(n) - \psi^0(z+1)\right),$$

Subtrahierten wir also wie vorher $\ln(n)$ von $\varphi_n(z)$ und lassen dann, für ein festes z, n gegen unendlich gehen, so erhält man

$$\phi(z) = -\frac{1}{4\pi\varepsilon_0}\frac{Q}{r_0}\psi^0(z+1).$$

Nun können wir unser Resultat für den Nullpunkt überprüfen. Für das elektrische Potential am Nullpunkt erhält man

$$\phi(0) = -\frac{1}{4\pi\varepsilon_0}\frac{Q}{r_0}\psi^0(1) = \frac{1}{4\pi\varepsilon_0}\frac{Q}{r_0}\gamma\,,$$

Die elektrische Feldstärke ist der negative Gradient des Potentials

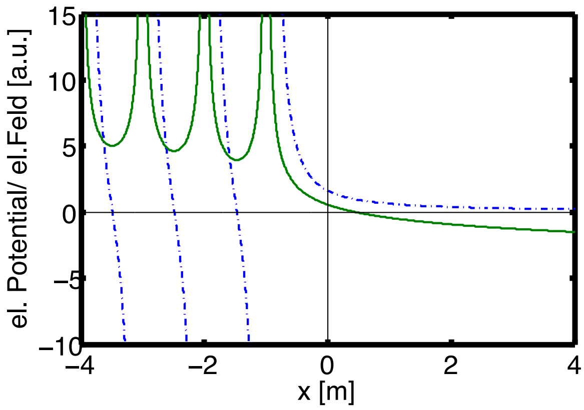
$$E(x) = -\frac{d\phi(x)}{dx} = \frac{1}{4\pi\varepsilon_0}\frac{Q}{r_0}\psi^1(z+1)\frac{dz}{dx}\,.$$

Mit $\psi^1(1) = \frac{\pi^2}{6}$ (5) erhält man für die elektrische Feldstärke

$$E(0) = \frac{1}{4\pi\varepsilon_0} \frac{Q}{r_0^2} \frac{\pi^2}{6}$$

in Übereinstimmung mit dem obigen Resultat.

Der Verlauf des elektrischen Potentials und des elektrischen Feldes lässt sich numerisch einfach bestimmen (Figur 2).



Figur 2: Das elektrische Potential (ausgezogene Linie) und die Feldstärke (gestrichelte Linie) einer langen Ladungskette auf dem negativen Ast der *x*-Achse. Zur numerischen Berechnung wurden 500 Ladungen benutzt und die Distanz zwischen den Ladungen betrug r_0 = 1 m. Die Vorfaktoren des elektrischen Potentials und der elektrischen Feldstärke wurden 1 gesetzt, so dass das Potential und die Feldstärke die vertikale Achse ungefähr bei γ und bei $\pi^2/6$ kreuzen.

Diskussion

Wir haben uns die Aufgabe gestellt, das elektrische Potential im Nullpunkt einer unendlich langen Kette von äquidistanten, identischen Punktladungen auf dem negativen Ast der *x*-Achse zu bestimmen. Die Lösung führt über die harmonische Reihe, die bekanntlich divergiert. Zähmen kann man das Potential indem man die asymptotische Entwicklung der Reihe studiert und den geeigneten Term ln(n) von der Summe subtrahiert; indem man also die Freiheit ausnützt, dass ein elektrisches Potential nur bis auf eine additive Konstante bestimmt ist.

Referenzen

1. Leuders T. Intelligent üben und Mathematik erleben. In: Leuders T, Hefendehl-Hebeker L, Weigand H-G, editors. Mathemagische Momente. Berlin: Cornelson; 2009. p. 130 -43.
2. Leuders T, Holzäpfel L. Kognitive Aktivierung im Mathematikunterricht. Unterrichtswissenschaft. 2011;39:213 - 30.
3. Bronstein I, Semedjajew K, Musiol G, Mühlig H. Taschenbuch der Mathematik. Frankfurt am Main: Verlag Harri Deutsch; 2008.
4. DMK-DPK-DCK. Formeln-Tabellen-Begriffe. Zürich: Orell Füssli Verlag; 2009.
5. Weisstein EW. Polygamma Function. Available from: http://mathworld.wolfram.com/PolygammaFunction.html

Investigations sur les courbes elliptiques en classe de 12e

Marie-Pierre Falissard, professeure de mathématiques à Pully-Lausanne (collège Champittet)

Le travail décrit ici a été proposé aux élèves préparant le Baccalauréat International[1] dans le cadre de leur "portfolio" (équivalent du Travail de maturité). L'intérêt, d'un point de vue pédagogique, était de combiner des notions intéressantes d'algèbre et d'analyse, impliquant à la fois du calcul numérique et une investigation s'appuyant sur des outils graphiques (tels que Geogebra). Les notions du programme mises en œuvre étaient les suivantes :

- équation du second degré ; polynômes, propriétés de leurs racines ;

- dérivation ; droite tangente en un point ; droites du plan ; propriétés de courbes ;

- notion de groupe (abordée dans une partie optionnelle du cours, "*Ensembles, relations et groupes*", choisie par les élèves concernés).

Il s'agit d'étudier les propriétés remarquables de certaines courbes à équation cubique, propriétés qui sont par ailleurs utilisées couramment en sécurité informatique. Le terme consacré de *courbe elliptique* peut prêter à confusion, puisque ces courbes n'ont pas de rapport avec l'ellipse.

Une courbe cubique donnée ($y^2 = x^3 - 5x + 4$) est étudiée en deux phases.

Dans une première partie, on étudie quelques propriétés de la courbe et on s'attache à valider une conjecture sur les abscisses x_1, x_2 et x_3 des points d'intersection de la courbe avec une droite quelconque : on se rend compte que l'une des abscisses se déduit aisément des deux autres.

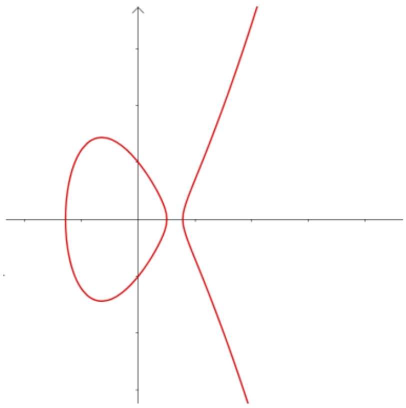
Le but de la seconde partie est d'étudier une relation de groupe définie sur les points de la courbe. Elle exploite les résultats de la première partie, puisque cette relation découle de l'intersection de droites avec la courbe précédemment étudiée.

La principale originalité du sujet était cette étude d'une loi de groupe définie sur les points d'une courbe elliptique. Il s'agit là d'un sujet presque "concret", puisque la *cryptographie sur courbe elliptique* (comparable au système RSA mais plus performante) gagne de plus en plus d'importance en sécurité informatique.

On étudie donc la courbe $\mathscr{C}$ formée par les points M (x, y) du plan pour lesquels est vérifiée la relation :

$$y^2 = x^3 - 5x + 4$$

1. Etude de la courbe



Dans une première partie, on s'intéresse à la courbe et à ses intersections avec certaines droites.

L'élève peut tracer la courbe avec Geogebra à partir des fonctions $f(x) = \sqrt{x^3 - 5x + 4}$ et $g(x) = -\sqrt{x^3 - 5x + 4}$.

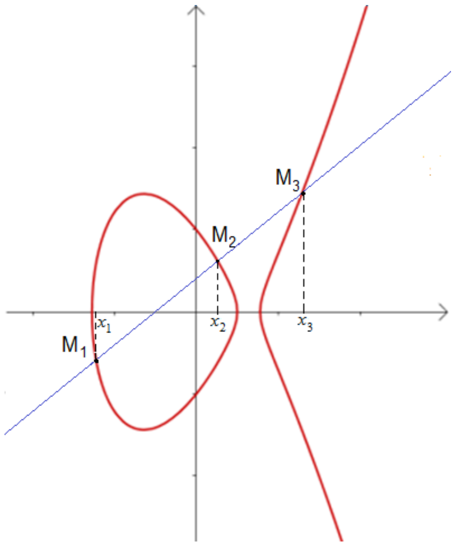
Il remarque que la courbe est en deux parties : une partie fermée, l'autre ouverte. Il en trouve les points remarquables (1, 0), (0, 2), (0, −2).

Il recherche, d'abord graphiquement, puis par le calcul, les abscisses des points d'intersection de $\mathscr{C}$ avec l'axe des abscisses, et trouve aisément les solutions : 1, $\frac{\sqrt{17}-1}{2}$, $\frac{-\sqrt{17}-1}{2}$.

[1] Diplôme de fin d'études secondaires, préparé dans des écoles à vocation internationale, reconnu dans plusieurs pays (principalement anglo-saxons) et ouvrant l'accès à l'université. Actuellement, 35 établissements offrent ce programme en Suisse.

Il s'agit ensuite de s'intéresser graphiquement à l'intersection de $\mathscr{C}$ avec des droites D_a d'équation $y = x + a$. Il y a en général trois points d'intersection, et on cherche à élaborer une conjecture relativement aux abscisses de ces points. Plusieurs essais graphiques (avec différentes valeurs de a) permettent de trouver la relation qui existe entre ces abscisses : leur somme donne toujours 1.

Si maintenant l'on s'intéresse à l'intersection de $\mathscr{C}$ avec d'autres familles de droites, comme les droites D'_a d'équation $y = 2x + a$, on peut de même conjecturer, toujours graphiquement, une relation entre les abscisses des trois points d'intersection : leur somme donne toujours 4.



L'élève peut alors formuler une conjecture plus générale sur les abscisses x_1, x_2 et x_3 des points d'intersection de $\mathscr{C}$ avec une droite d'équation générale $y = px + q$.

La conjecture est que leur somme $x_1 + x_2 + x_3$ donne p^2.

On souhaiterait démontrer cette conjecture dans le cas général. On effectue pour cela un petit détour par la théorie des polynômes, tout en évitant les notions hors programme (telles que les « fonctions symétriques élémentaires des racines du polynôme »). La démonstration ne présente en réalité pas de difficulté pourvu que l'élève soit mis sur la voie.

On étudie d'abord le coefficient a_{n-1} d'un polynôme $P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ dont on suppose qu'il admet n racines. Une démonstration par récurrence doit fournir la valeur a_{n-1} en fonction des racines de $P(x)$.

La propriété :

« si $P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ admet n racines, alors a_{n-1} vaut l'opposé de la somme des racines »

est facilement vérifiée pour $n = 1$ et $n = 2$.

On suppose (hypothèse de récurrence) qu'elle est vraie jusqu'à l'ordre $n - 1$.

$P(x)$ ayant n racines peut s'écrire $P(x) = (x - x_n)\,(x - x_{n-1})\ldots\,(x - x_1)$,

ce qui peut s'écrire aussi : $(x - x_n)\,(x^{n-1} - S_{n-1}\,x^{n-2} + \ldots)$ où S_{n-1} est la somme des racines $x_1 + \ldots + x_{n-1}$ (d'après l'hypothèse de récurrence).

Le développement du produit donnera $x^n - x_n\,x^{n-1} - S_{n-1}\,x^{n-1} + \ldots$

Le coefficient du facteur x^{n-1} sera donc $(- x_n \; - S_{n-1})$, ce qui vérifie l'hypothèse de récurrence à l'ordre n.

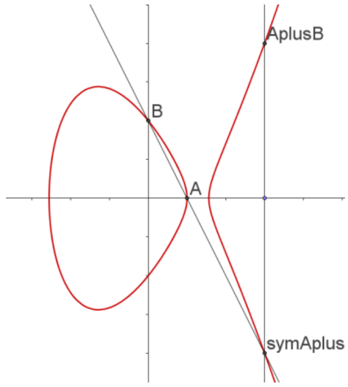
On peut expliquer à l'élève, pour sa culture personnelle, que ces coefficients S_i sont appelés « fonctions symétriques élémentaires des racines du polynôme », et qu'il est établi (mais les démonstrations sont hors programme) que le coefficient a_{n-2} de $P(x)$ vaudra la somme de tous les doubles produits des racines, a_{n-3} l'opposé de la somme de tous les triples produits des racines, etc., jusqu'à a_0 qui vaudra $(-1)^n\, x_1 \ldots x_{n-1}\, x_n$.

A présent, si l'on remplace y par $px + q$ dans l'équation $y^2 = x^3 - 5x + 4$, et que l'on développe le polynôme du 3^e degré résultant, le terme en x^2 aura un coefficient $-p^2$, coefficient qui sera aussi l'opposé de la somme des racines.

La somme des abscisses x_1, x_2 et x_3 des points d'intersection de $\mathscr{C}$ avec une droite d'équation $y = px + q$ est donc bien $\boldsymbol{p^2}$.

L'intérêt de ce résultat est qu'il permet de calculer facilement x_3 quand x_1 et x_2 sont connus (voir seconde partie), ainsi que $y_3 = px_3 + q$. Deux points d'intersection M_1 et M_2 de la courbe et de la droite étant connus, le troisième M_3 s'en déduit facilement. A partir d'une droite (M_1M_2), on peut ainsi construire une correspondance $(M_1,M_2) \rightarrow M_3$.

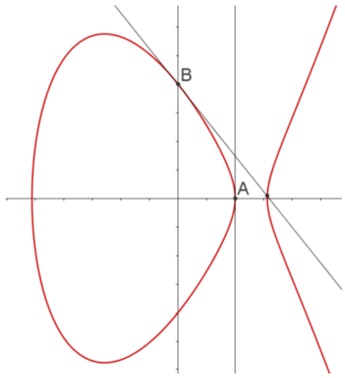
2. Etude d'une loi de groupe définie sur les points de la courbe



Le but de cette partie est d'étudier une relation de groupe, notée par un opérateur $\oplus$, et définie ainsi (loi de groupe sur les points d'une courbe elliptique) :

> Etant donnés deux points quelconques A et B de la courbe $\mathscr{C}$, on note A $\oplus$ B ("AplusB" sur le schéma Geogebra) le point qui est le symétrique par rapport à l'axe des abscisses du point d'intersection de $\mathscr{C}$ avec la droite (AB), quand un tel point existe ("symAplusB" dans Geogebra).

Le cas général A $\oplus$ B est représenté sur la figure ci-contre.



Il faut considérer le cas où les deux points sont confondus. Si A = B, la "droite" (AB) devient la tangente au point A. Cette tangente a généralement une intersection avec $\mathscr{C}$ (exemple du point B sur le schéma ci-contre) sauf si elle est verticale (exemple du point A ci-contre).

L'élève doit enfin repérer les cas où A $\oplus$ B n'est pas défini.

Ces cas se produisent quand les deux points sont sur une même droite verticale, ou quand les deux points sont confondus et ont une ordonnée nulle (tangente verticale).

Quand A $\oplus$ B n'existe pas, on décide de noter A $\oplus$ B = O. Le point O est interprété géométriquement comme « point à l'infini sur l'axe des y ».

L'élève est invité à constater qu'il est alors possible de donner un sens à A $\oplus$ O et O $\oplus$ A. L'intersection de la droite verticale (AO) avec $\mathscr{C}$ sera le symétrique de A par rapport à l'axe des x. Donc A $\oplus$ O redonne A, de même O $\oplus$ A.

Si l'on appelle A' le symétrique de A par rapport à l'axe des x, on a A $\oplus$ A'= A' $\oplus$ A = O. Chaque point de $\mathscr{C}$ a donc un "opposé" dans la loi de groupe, qui est simplement son symétrique par rapport à l'axe des x.

De même, si P est un des trois points d'intersection de $\mathscr{C}$ avec l'axe des abscisses (les trois points vus en première partie), alors P $\oplus$ P a un sens : c'est le point à l'infini O. En ce cas, le point P a pour opposé lui-même.

On a donc bien défini une loi de composition interne sur tous les points de la courbe, en s'aidant d'un « point à l'infini ») fictif qui sert d'élément neutre.

On peut chercher, en utilisant la première partie, à trouver un procédé pour calculer l'abscisse du point $M_1 \oplus M_2$, les deux points M_1 et M_2 étant donnés.

Il faut d'abord calculer l'équation $y = px + q$ de la droite (M_1M_2). Une fois son coefficient directeur p connu, on sait que le point $M_1 \oplus M_2$ aura pour abscisse $x = p^2 - x_1 - x_2$. Son ordonnée sera $-y = -px - q$ puisque c'est le point symétrique de l'intersection de $\mathscr{C}$ avec la droite qui nous intéresse.

On peut utiliser le résultat suivant pour étudier quelques exemples numériques :

> l'équation d'une droite passant par deux points $M_1(x_1, y_1)$ et $M_2(x_2, y_2)$ est :
>
> $$y = \frac{y_1 - y_2}{x_1 - x_2} x + \frac{x_1 y_2 - y_1 x_2}{x_1 - x_2}.$$

Si par exemple l'on cherche A ⊕ B, avec A(1, 0) et B(0, 2) :

- la droite (AB) a pour équation $y = -2x + 2$;
- le point A ⊕ B aura pour abscisse $p^2 - x_1 - x_2 = 4 - 1 = 3$, et pour ordonnée $-(-2\times 3 + 2) = 4$;
- on a donc A ⊕ B = D (3 ; 4).

Si par exemple l'on cherche le point B ⊕ B avec B(0, 2), il faut s'intéresser à la tangente à la courbe au point B :

- en dérivant $f(x) = \sqrt{x^3 - 5x + 4}$, on trouve que $f'(0) = -\dfrac{5}{4}$;
- l'équation de la tangente est donc $y = -\dfrac{5}{4}x + 2$;
- le point B ⊕ B aura pour abscisse $p^2 - x_1 - x_2 = \dfrac{25}{16} - 0 - 0 = \dfrac{25}{16}$, et pour ordonnée $-\dfrac{3}{64}$;
- donc B ⊕ B = (1,5625 ; −0,046875), ce qu'on peut vérifier avec Geogebra (avec la précision adéquate).

Plusieurs propriétés de groupe ayant été établies dans les questions précédentes, on s'intéresse à présent à l'associativité.

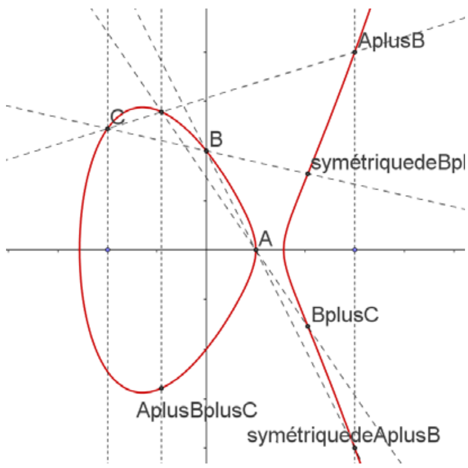
On peut inviter l'élève à la vérifier sur des exemples, en utilisant les points A et B précédents.

Par exemple, pour vérifier que A ⊕ (A ⊕ B) = (A ⊕ A) ⊕ B :

- A ⊕ (A ⊕ B) = A ⊕ D avec A(1, 0) et D (3 ; 4) ; l'équation de la droite (AD) est $y = 2x - 2$; le point A ⊕ D aura donc pour abscisse $p^2 - x_1 - x_2 = 4 - 1 - 3 = 0$ et pour ordonnée 2 : c'est le point B ;

- d'autre part, (A ⊕ A) ⊕ B = O ⊕ B = B.

L'élève est invité alors à vérifier graphiquement, grâce à Geogebra qui permet de déplacer dynamiquement les points sur la courbe, l'associativité de la loi : A ⊕ (B ⊕ C) = (A ⊕ B) ⊕ C, avec A, B et C trois points quelconques de $\mathscr{C}$.



Le schéma correspond ici aux points A(1, 0), B(0, 2) et C(−2,√6)).

Il n'est évidemment pas question de donner une démonstration de cette associativité dans le cas général : cela entraînerait beaucoup trop de calculs, et cela se démontre d'ailleurs autrement.

On propose seulement à l'élève de vérifier analytiquement que les points A ⊕ (B ⊕ C) et (A ⊕ B) ⊕ C sont les mêmes dans le cas suivant : A(1, 0), B(0, 2) et C(−1, −√8).

Le calcul donnera :

- A ⊕ B = (3, 4) et (A ⊕ B) ⊕ C = $\left(\sqrt{2} - \dfrac{1}{2}; 3\dfrac{\sqrt{2}}{4} - \dfrac{3}{2}\right)$ (soit le point (0.9142137 ; 0.43933911)).
- B ⊕ C = $\left(13 + 8\sqrt{2}; -60 - 42\sqrt{2}\right)$ et A ⊕ (B ⊕ C) = $\left(\sqrt{2} - \dfrac{1}{2}; 3\dfrac{\sqrt{2}}{4} - \dfrac{3}{2}\right)$.

On a donc pu vérifier sur plusieurs exemples les propriétés de groupe de l'opérateur ⊕ (loi de composition interne, élément neutre, symétriques, associativité), la commutativité étant évidente.

Dans cette étude, on a vu sur un exemple précis les propriétés qui sont au fondement de la *cryptographie sur courbe elliptique*. On peut par la suite expliquer aux élèves que ce procédé cryptographique repose sur la difficulté à retrouver un nombre *n* étant donné un point M de la courbe et le « produit » *n*M lié à la loi de groupe ainsi définie (problème du logarithme discret sur courbe elliptique, les opérations s'effectuant modulo un nombre premier).

Le Défi Turing

Didier Müller, Lycée cantonal de Porrentruy

En cours d'informatique ou en maths appliquées, on voit souvent que certains élèves sont bien plus rapides que d'autres pour faire les exercices de programmation. Que faire alors de ces élèves ? Leur donner des exercices supplémentaires est une solution parmi d'autres. Mais où trouver des exercices assez courts, et quand même intéressants ? C'est en cherchant une réponse à cette question qu'est né le « Défi Turing ».

Qu'est-ce que le Défi Turing ?

Le Défi Turing est directement inspiré du **Project Euler** (http://projecteuler.net), qui a deux inconvénients : il est en anglais et seuls les premiers problèmes sont abordables par des lycéens. On peut voir le Défi Turing comme une version française pour débutants en informatique.
Le défi Turing a commencé le 31 décembre 2012 (dernier jour de l'année du centenaire d'Alan Turing). **C'est une série de problèmes mathématiques et informatiques**. Bien que les mathématiques permettront parfois de trouver des méthodes élégantes et efficaces, l'utilisation d'un ordinateur et des compétences en programmation seront nécessaires pour résoudre la plupart des problèmes.
Ce défi est destiné aux programmeurs débutants, donc principalement aux lycéens, mais toutes les personnes intéressées par les énigmes mathématiques sont les bienvenues. L'idée est de créer une base de données d'exercices de programmation stimulants. Des **classements** (un classement général, un par pays et un par classe) seront disponibles afin de créer une saine émulation entre les participants.

Classes virtuelles

Une classe est un groupe de membres. Un enseignant peut par exemple regrouper ses élèves dans une classe virtuelle. Un classement **spécifique** sera généré, ce qui pourra créer une émulation dans la classe (les élèves aiment bien les concours).

Quelle est la difficulté des problèmes ?

La difficulté est variable. Le nombre de personnes qui ont trouvé la réponse donne une idée de la difficulté. En moyenne, un programme de 10 à 30 lignes suffira pour répondre à la question (cela dépend évidemment du langage utilisé).
Si le programme est écrit de façon optimale, la réponse tombera en **moins d'une minute**. Cela dit, la réponse pourra aussi être trouvée après plusieurs heures de calculs... Si tel est le cas, on pourra se demander comment améliorer le programme.
Un nouveau problème est mis en ligne chaque dimanche, à 0h00.

Exemples de problèmes

Chaque nouveau terme de la suite de Fibonacci est généré en ajoutant les deux termes précédents. En commençant avec 1 et 1, les 10 premiers termes sont les suivants :

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ...

En prenant en compte les termes de la suite de Fibonacci dont les valeurs ne dépassent pas 4 millions, trouver la somme des termes impairs.

Un cryptarithme est un casse-tête numérique et logique qui consiste en une équation mathématique où les lettres représentent des chiffres à trouver.

Résoudre le cryptarithme ci-dessous (donner comme réponse le produit obtenu) :

THREE x NINE = TROIS x NEUF

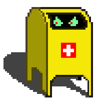
Contraintes:
THREE et NEUF sont des multiples de 9 ;
TROIS et NINE sont des multiples de 3.

Comment participer ?

Il est possible de voir les problèmes sans s'inscrire, mais pour proposer une réponse et apparaître dans les classements, il faut impérativement s'inscrire (c'est gratuit). L'adresse :

http://turing.nymphomath.ch

Il est aussi possible de participer en **proposant des problèmes** ! Envoyez l'énoncé, la source du problème et la réponse (avec le programme qui l'a trouvée) à l'adresse :



turing@nymphomath.ch

Pour être accepté, un problème doit répondre aux critères suivants :

1. l'énoncé doit être clair, sans équivoque, et dans un français irréprochable ;
2. le niveau de maths nécessaire pour résoudre le problème ne doit pas dépasser le niveau du lycée ;
3. le programme pour le résoudre ne doit pas être trop long (disons moins de 50 lignes pour fixer les idées) ;
4. la réponse doit pouvoir se trouver en moins d'une minute de calculs ;
5. la réponse doit être un (grand) nombre entier, éventuellement négatif.

24. Schweizerischer Tag über Mathematik und Unterricht

Die Schweizerische Mathematische Gesellschaft SMG, die Deutschschweizerische Mathematik-Kommission DMK und die ETH Zürich laden Sie herzlich zu dieser Weiterbildungsveranstaltung ein.

Kursdaten

Ort:	Kantonsschule Chur (Plessur), Chur
Datum:	Mittwoch, 11. September, 2013
Organisation:	Meike Akveld (ETH), Caspar Bamert (KS Chur), Norbert Hungerbühler (ETH), Josef Züger (KS Chur)

Programm

09:45 Uhr	**Check-in:** Kaffee, Orangensaft und Gipfeli; Verkauf von Bons für's Mittagessen (20 CHF)
ab 10:15 Uhr	3 Plenumsvorträge
16:00 Uhr	**Offizielles Ende der Veranstaltung**

Programm und Anmeldungen: ***http://www.math.ch/TMU2013/***

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Kolloquium über Mathematik, Informatik und Unterricht
Programm HS 2013

Die Vorträge finden jeweils an einem Donnerstag um 17:15 Uhr
im Hörsaal HG G 3 des Hauptgebäudes der ETH Zürich statt.

Abgeschlossen werden die Veranstaltungen mit einem **Apéro im HG G 69** (D-MATH Common Room).

Donnerstag, 24. Oktober 2013
An diesem Tag fällt das Kolloquium aufgrund des gleichzeitig stattfindenden Kongresses Science-Cuisine **(23. - 26. Oktober in Sitten) aus.** Weitere Informationen finden Sie auf der Seite de.VSMP **www.vsmp.ch**

Donnerstag, 7. November 2013
Herr Martin Mattmüller, Universität Basel
Die schwere Geburt der Stochastik: Jacob Bernoullis Ars Conjectandi (Basel 1713)

Abstrakt folgt!

Donnerstag, 21. November 2013
Dr. Ana Cannas da Silva, ETH Zürich, Department Mathematik
Wallpaper stamps


Shell 1 and shell 2

We can have exactly 17 different wallpapers in terms of types of symmetry patterns and no more. This was established at the end of the 19th century by the Russian mathematician and mineralogist Yevgraf Fyodorov.

Much more recently Murray Macbeath, Bill Thurston and John H. Conway discovered and publicised a new geometric perspective, together with a felicitous notation, which is more inviting and informative than the classical crystallographic perspective.

The modern perspective relies on the notion of (2-dim) orbifold - a kind of surface with singular points - and a corresponding Euler characteristic. We will discuss how these surfaces can be seen as exotic stamps for printing patterns.

Donnerstag, 5. Dezember 2013
Prof. Dr. Gregor Dolinar, Faculty of Electical Engineering, University of Ljubljana, Slovenia
How far is your daily weight from the normal one?

If we want to know how far we need to walk to the best coffee bar in town, or if the number that we are dictating is recognized by our mobile phone, or if the distribution of our daily weight is the normal one, then we can find the answers to these questions with a help of various kinds of distances.

In our talk we will first recall the definition of the general concept of a distance, that is the concept of a metric space. Then examples of different distances, such as Manhattan distance, L^2 distance, Kolmogorov-Smirnov distance, and there applications in voice and image recognition, statistics, etc. will be presented.

Herzlich laden ein: N. Hungerbühler, J. Hromkovič, Meike Akveld, H. Klemenz

---

Weitere Informationen: http://www.math.ethz.ch/didaktik/weiterbildung/kolloquium

http://math.ch/mathematics@school/

PH Zürich

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Vom Kindergarten bis zur Hochschule – Mathematik im Unterricht heute

Zentrale Aspekte des Mathematiklernens gelten vom Kindergarten bis zur Hochschule. In dieser neuen Vortragsreihe der Fachbereiche Mathematik der PH Zürich und der ETH Zürich soll vorgestellt werden, was für den Mathematikunterricht aller Stufen wesentlich ist – theoretisch fundiert und praktisch illustriert. Diese Veranstaltung richtet sich an Lehrpersonen aller Stufen sowie an Mathematikunterricht Interessierte.

Donnerstag, 5. September 2013 in Zürich

17:15 bis 18:45 Uhr Vortrag mit anschliessendem Apéro (Eintritt frei)

Beat Jaggi (PH Bern)

Aktiv-entdeckendes Lernen mit spannenden Aufgabenformaten

In Aufgabenformaten wie Rechendreiecken, Zahlenmauern oder Zahlenwaben steckt ein grosses Potential sowohl für aktives Entdecken wie auch für natürliche Differenzierung.

Im Vortrag wird gezeigt, wie dieses Potential in der Primarschule, in der Sekundarschule, aber auch im Gymnasium genutzt werden kann. Fast alle wichtigen mathematischen Gebiete (Algebra, Geometrie, Gleichungssysteme, Funktionen, Vektoren, Matrizen, etc.) kommen vor!

Differenzierung ist auf einfache Art und Weise zu erzielen und in mehrere Richtungen möglich. Für das Lösen der grundlegenden Aufgabenstellungen gibt es unterschiedliche Methoden, die aber alle auf wichtigen und tragfähigen mathematischen Konzepten basieren.

Dr. Beat Jaggi ist Mathematiklehrer am Gymnasium Alpenstrasse in Biel und Dozent für Fachdidaktik der Sekundarstufe II an der Pädagogischen Hochschule in Bern.

Herzlich laden ein

Norbert Hungerbühler (ETH Zürich) und
René Schelldorfer (PH Zürich)

Veranstaltungsort

ETH Zürich
Maschinenlabor (neben Hauptgebäude)
Eingang Ecke Tannen- und Clausiusstrasse
Hörsaal E 12

Tram Linie 6 oder 10 ab HB bis «Polyterasse»,
Linie 9 ab Bellevue bis «ETH/Unispital»,
Polybahn ab Central

DPK Deutschschweizerische Physikkommission des VSMP

ETH Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

14. Schweizerischer Tag für

Physik und Unterricht

Mittwoch, 13. November 2013, 13:00 - 17:30 an der ETH Zürich,
Campus Hönggerberg

Themen: Quantenphysik in Wissenschaft Technologie und Lehre .

13:00 - 13:30	Begrüssungskaffee ETH Hönggerberg, HPF G6 (siehe Angaben zum Treffpunkt)
13:30 - 13:35	***Begrüssung***
13:35 - 15:00	***Eine Einführung in QSIT(Quantum Science and Technology, www.qsit.ethz.ch/)*** Vortrag von: Prof. K. Ensslin, ETH Zürich.
15:00 - 15:30	***Pause***
15:30 - 16:15	***Unterricht lernwirksam gestalten. Der Aufbau intelligenten Wissens mit kognitiv aktivierenden Lernformen*** Vortrag von: Dr. R. Schumacher, ETH Zürich (www.educ.ethz.ch/mint).
16:30 - 17:15	***Vom Doppelspalt zum Quantencomputer. Eine Unterrichtseinheit des MINT-Lernzentrums.*** Vortrag von: Dr. J. Lipscher, ETH Zürich.
17:15 – 17:30	***Abschluss***

Treffpunkt (vorerst provisorisch)

Ort:	ETH Hönggerberg (Erreichbarkeit: www.ethz.ch/about/location/hoengg)
Gebäude:	HPF
Stockwerk:	G
Raum:	6 (Seminarraum)

Mailen, faxen oder schicken Sie die Anmeldung bitte spätestens bis zum 04. November 2013 an: (für eine frühzeitige, ev. auch provisorische Anmeldung sind wir sehr dankbar!)

Andreas Vaterlaus, ETH Hönggerberg HPF G4.1 , 8093 Zürich.

FAX 044 633 1623

Email: vaterlaus@phys.ethz.ch

Kosten: keine

Angaben:

Name und Vorname: ……………………………………………………………………………………………….

Schule: ………………………….. Email: …………………………………….

Ja - Oui - Sì ☐

Ich möchte Mitglied des Vereins Schweizerischer Mathematik und Physiklehrkräfte (VSMP) sowie des Vereins Schweizerischer Gymnasiallehrerinnen und lehrer (VSG) werden.

J'aimerais devenir membre de la Société Suisse des Professeurs de Mathématique et de Physique (SSPMP) et de la société suisse des professeurs de l'enseignement secondaire (SSPES).

Desidero diventare membro della Società Svizzera degli Insegnanti di Matematica e Fisica (SSIMF) e della Società Svizzera degli Insegnanti delle Scuole Secondarie (SSISS).

Beitrag/ Montant/Quota: Fr. 120.- (VSG - SSPES - SSISS) + Fr. 40.- (SSIMF - SSPMP - VSMP)

Frau/Mme/Sig.ra ☐ Herr/M./Sig. ☐ Prof. ☐ Dr. ☐

Name/Nom/Cognome: ....

Vorname/Prenom/Nome: ....

Adresse/Indirizzo (privat/privato): ....

Plz-Ort/NP-Ville/CAP -Luogo: ....

(Land/Pays/Paese): ....

Email: .... (Tel): ....

(Geburtsdatum/Date de naissance/Data di nascita): ....

Sprache/Langue/Lingua: D ☐ F ☐ I. ☐

Schule/école/scuola: .... Kanton/canton/cantone: ....

Kategorie/Catégorie/Categoria: activ/actif/attivo ☐ passive/passif/passivo ☐
Student/in, étudiant(e), studente/ssa. ☐

Einsenden an/envoyer à/inviare a:
VSG - SSPES - SSISS, Sekretariat (Frau Doris Lazzeri), 3000 Bern
oder per Internet: www.vsg-sspes.ch

Impressum

Herausgeber – *Éditeur*
VSMP / SSPMP / SSIMF

Korrespondenz – *Correspondance*
Franz Meier franz.e.meier@bluewin.ch
Alpenquai 44 Tel. 079 79 89 770
6005 Luzern

Layout – *Mise en page*
Stéphane Davet davet.stephane@lyca.eduvs.ch
Av. Plantaud 28B Tél. 024 471 21 83
1870 Monthey

Inserateverwaltung – *Publicité*
Stefan Walser stefan.walser@alumni.ethz.ch
Weinbergstrasse 3 Tel. 055 410 62 36
8807 Freienbach

Bestimmungen für Inserate und Beilagen
– *Tarifs pour les annonces et les annexes*

Inserate:

Ganzseitige	Fr. 500.–
Halbseitige	Fr. 300.–

Beilagen:

bis 20 g	Fr. 500.–
über 20 g	Nach Vereinbarung

Adressänderung – *Changement d'adresse*
VSMP Mitglieder – Membres de la SSPMP :
VSG – SSPES – SSISS
Sekretariat (Frau Doris Lazzeri)
3000 Bern
Tel. 056 443 14 54 / Fax 056 443 06 04
E-Mail: information@vsg-sspes.ch

Abonnenten, die nicht Mitglieder des VSG sind:
Franz Meier franz.e.meier@bluewin.ch
Alpenquai 44 Tel. 079 79 89 770
6005 Luzern

Auflage – *Tirage*
900. Erscheint dreimal jährlich.

Präsident VSMP – SSPMP – SSIMF
Hansjürg Stocker hjstocker@bluewin.ch
Friedheimstrasse 11 Tel. 044 780 19 37
8820 Wädenswil

Deutschschweizerische Mathematikkommission
Daniela Grawehr grawehr@kfanet.ch
Schützenstrasse 36 Tel. 041 810 49 88
6430 Schwyz

Deutschschweizerische Physikkommission
Christian Stulz christian.stulz@gymburgdorf.ch
Marienstrasse 21 Tel. 031 534 66 74
3005 Bern

Commission Romande de Mathématique
José Luis Zuleta joseluis.zuletaestrugo@epfl.ch
Avenue de Rumine 42 Tél. 021 624 25 46
1005 Lausanne

Commission Romande de Physique
Gordana Gerber gordana.gerber@gymalp.ch
Chemin du Petit-Clos 15 Tél. 032 342 42 94
1815 Clarens-Montreux

Commissione di Matematica della Svizzera Italiana
Arno Gropengiesser groppi@bluewin.ch
Via Vincenzo d'Alberti 13
6600 Locarno Tél. 091 751 14 47

Redaktionsschluss (Erscheinungsdatum)
– *Délais de rédaction (de parution)*

Nr. 123	31.07.2013 (20.09.2013)
Nr. 124	30.11.2013 (20.01.2014)
Nr. 125	31.03.2014 (20.05.2014)

Druck und Versand – *Imprimerie*
Niedermann Druck AG
Rorschacherstrasse 290
9016 St. Gallen

Internet-Adressen – Adresses Internet

http://www.vsmp.ch — http://www.sspmp.ch — http://www.ssimf.ch