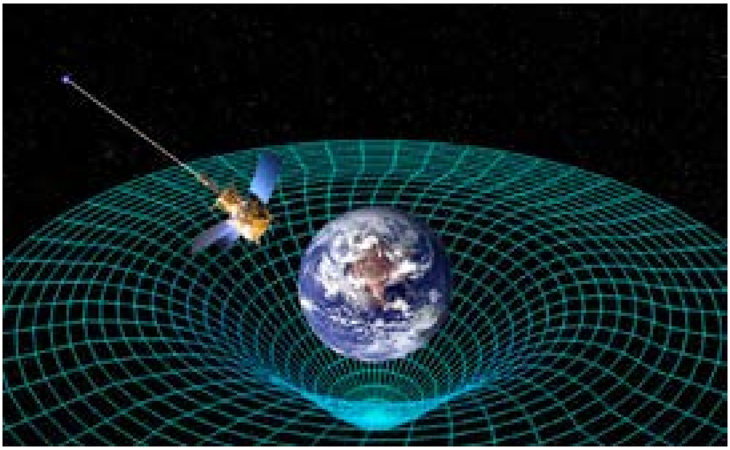
perio*diek

recurring at regular intervals volume 2016 number 2

6 - Slow Down with Gravity

Many thing go too fast these days. This also applies to the research on the origin of gravity. Discover the newest findings in the research on gravity and see why we indeed should slow down with gravity.



16 - Plasmonics

Get along with Arsalan to go through the hot research topic of Plasmonics. Read now why this new field of research show a high potential.

28 - Cryptography

Have you ever wondered about the security of your e-mails, transactions, secure mesages and so on? Find out how these things are being protected and why they are secure.

Erratum

In the previous version, Periodiek 2016-1, on page 18 the figure captions are interchanged. On the left is Anton Philips and on the right is Hendrik Antoon Lorentz.

In this Periodiek

From the editor in chief

The end is near, by the time you are reading this magazine you are probably enjoying your holidays as much as I am. Whether you are enjoying your holidays in Prague, as most of the editors seem to have chosen for, or somewhere else, take your time, enjoy the sun and your free time. You are going to need it for the next academic year. To help you relax we have this awesome Perio*diek, where professor Bergshoeff tells you why you should slow down with gravity. A great motto for these holidays.

Slow down, take a step back and review the past year. For the Perio*diek the past year has been a year of change. We changed the language to English and the style into full colour. I can say that both of these changes make the Perio*diek a better magazine, now and in coming years. I hope that you enjoy reading it as much as we enjoyed making it. Have fun reading!

— Douwe Visser

Editors Derk Rouwhorst, Douwe Visser, Klaas Hakvoort, Nick Lutjes, Thomas Meijknecht, Martine Schroor.

Authors Eric Bergshoeff, Nick Lutjes, Martine Schroor, Marieke Mudde, Jos Borger, Max Kronberg, Arsalan Torke Ghashghaee.

Advertisers Talent & Pro (p. 11), KxA (p.15), Philips (p.23), Schut (p. 32).

Advertise? Contact us at bestuur@fmf.nl.

Print run 1100 pieces

Press Gildeprint

ISSN 1875-4546

The Periodiek is a magazine from the Fysisch-Mathematische Faculteitsvereniging and appears five times per year. Previously printed Periodiek's can be found at perio.fmf.nl. The board of editors can be reached by perio@fmf.nl.

In the news

TU Delft's capsule concept

The capsule train designed by a team of students at TU Delft, to travel at speeds of more than 900km/h through reduced-pressure tubes, has taken second place in an international competition launched by SpaceX. The concept capsule was also awarded the prize for the most innovative design in the Hyperloop competition.

The system consists of a number of passenger capsules, which are designed to travel through tubes in a partial vacuum, with the lack of pressure allowing them to reach very high speeds. The Delft team were one of 124 who presented their designs to a jury of researchers and experts from Tesla Motors and SpaceX in the first stage of the competition. They will now join 20 other teams in progressing through to the next stage, in which they will build a half-scale version of their capsule and test it on a track in California in the summer.

The Engineer

NWO Spinoza Prizes for Lodi Nauta and Bart van Wees

2016 is a good Spinoza year for the University of Groningen. Two laureates have been added to its list of honour in one go: Lodi Nauta, Professor of the History of Philosophy, and Bart van Wees, Professor of Applied Physics. The winning academics both receive 2.5 million euro for research. In total the University of Groningen now has seven winners of the Spinoza prize.

Lodi Nauta is the first philosopher to receive the Spinoza Prize. 'I consider this to be not merely the recognition of my own work, but also of the importance of philosophy and its history.' Bart van Wees still needs to have a good think about how he will spend the money: 'I could use it for my current research, but I will certainly use some of it to explore new territory too.'

The NWO Spinoza Prize is the highest distinction in Dutch academia. The award was introduced by NWO, the Netherlands Organisation for Scientific Research, a national organization that funds and stimulates academic research in the Netherlands. A maximum of four prizes are awarded annually. The winning academics receive 2.5 million euro for research, and are given complete freedom to choose their research subject and involve other, mostly young, researchers. Thus, the prize is partially recognition for accomplished researchers and partially stimulus to conduct further research.

University of Groningen

Crystallize

Games are usually more fun when you play with other people, but if you're playing an educational game, interacting with other players may help you learn more, according to Cornell University research.

Researchers at the University of Cornell have made a game called crystallize, where you are to learn a new language through interacting with npc's and other players. You do this by collecting words and phrases and sharing them. When you learn new words you have to go home and study them via a quiz system. Then once you have mastered these words you can use them to answer questions in the game and thus earning money.

Currently the only language you can learn via this game is Japanese. But this no problem considering that this is the language to learn for the next GBE. You can apply for the GBE at gbe.fmf.nl. The words in the game currently do not have audio, also the words can be shown in Roman leters (Romaji) or Japanese signs (Kanji). The game can be downloaded form http://crystallize-online.com. Note that the central servers currently do not seem to work, therefore in order to make the game work, you have to set local server to "true".

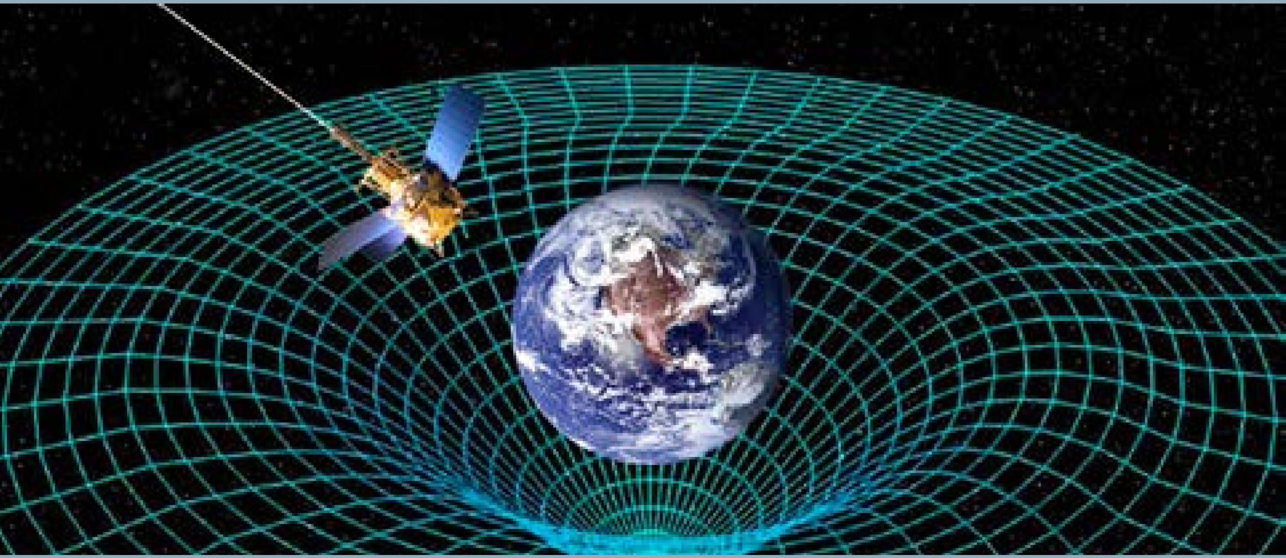
Cornell University

NASA wants to purify more urine into drinking water in Space Station

Space Agency NASA increases the production of purified urine in the International Space Station. The purifier makes drinking water from the urine of the crew. The ISS has the purifier since a few years. Urine consists mainly out of water, which is taken out by the machine. The new device, to be installed in 2018, is designed such that 94 percent of all urine is reused in the ISS as water. The purification of the urine in the space station supplies approximately six thousand liters of water per year. Those liters therefore do not have to be transferred from Earth to the space station which provides a considerable cost saving.

Reuse of urine also helps if people ever want to go far into space, for example to Mars. It tastes just like ordinary water, the only problem is between the ears of the crew, they have to get used to the idea that they drink purified urine.

Nu



AUTHOR: ERIC BERGSHOEFF

Slow Down with Gravity!

Many things go too fast these days. This was the theme of Douwe Bob's song at the recent Eurovision Song Contest in Stockholm. We should slow down a bit! The same applies to the way we get educated in gravity.

Usually, a course on Einstein's General Relativity only mentions the old Newton's theory in the margin. The reason for this is that Newton's theory is only valid when applied using velocities that are small with respect to the speed of light and that many phenomena, such as the bending of light by the Sun or the operation of the GPS system, can be explained by General Relativity only. Nevertheless, there is a recent new appreciation for an improved version of Newton gravity, called Newton-Cartan gravity. This is due to the fact that in modern research, gravity is not only used to describe the gravitational force, but it is also applied as a novel tool to get new insights into the non-perturbative properties of a variety of physical systems. Many of these applications are in the non-relativistic domain.

When, in November 1915, Einstein presented his new description of the gravitational force, now known as General Relativity, he had improved the old description by Newton in two ways. First of all, he gave a description of gravity that was consistent with the Special Relativity Theory (SRT) he had formulated ten years earlier by imposing that any two inertial frames of reference are connected by a Lorentz transformation. Second, he constructed his equations consistent with the principle of equivalence that states that gravity is a pseudo-force experienced by an observer in a non-inertial frame. In Einstein's description of gravity the curvature of spacetime plays a crucial role. To construct his equations Einstein needed to use the mathematics of Riemannian geometry, which was only developed around the middle of the 19th century, by Riemann. The monumental achievement by Einstein in 1915 marked the end of a large period of uncertainties and struggle. The history that led to this remarkable result started much earlier.

Newton was the first one to give a mathematical description of the gravitational force by a simple formula which stated that two bodies attract each other with a strength that is proportional to the gravitational mass of each body and inversely proportional to the square of the distance between these two bodies. Newton's formula has a few remarkable features. First of all, Newton used the notion of absolute time, i.e., the 8 o'clock news applies to the whole Universe. Second, the action of the gravitational force is instantaneous. If, by a thought experiment, somebody removes the Sun, the Earth would immediately disappear with a straight line, into space. Finally, the way Newton's formula is usually presented is only valid in an Earth-based frame. It was never formulated in a frame-independent way.

Newton's formula worked for centuries to everybody's satisfaction. Things started to change when in 1873 Maxwell introduced his unifying laws of electricity and magnetism. The remarkable thing that Maxwell achieved is that by adding an extra term to the known laws of electricity and magnetism he obtained a new set of equations that allowed a wave solution whose speed he could calculate using the constants of nature occurring in the equations. Once it was verified that this speed was precisely the speed of light, it was quickly realized that light is in fact an electromagnetic wave. Given the fact that light is a wave, it was a big surprise that a few years later Michelson and Morley measured that the speed of light was always the same, independently of whether this light was approaching or retarding.

Élie Cartan (1869 – 1951)

The work of Maxwell and the Michelson-Morley experiment was of crucial importance in what follows when Einstein enters the scene in 1905. Einstein knew about the so-called Principle of Relativity, introduced by Galileo Galilei in 1632 in his famous Dialogo. This principle states that the laws of physics do not depend on whether you are in rest or move with constant velocity. Imagine you are sitting in an airplane from Schiphol to New York. If you can't look out of your window, the motors do not give any sound and there is no turbulence, you cannot find out whether you are flying over the ocean or whether you are still parked at Schiphol airport. This makes sense. But now comes Einstein! For the same reason, he argued that you cannot change the speed of light, depending on whether this light is approaching or retarding, because changing the speed of light is only possible if you change the constants of nature that occur in Maxwell's equations, but this is forbidden by the Principle of Relativity! For Einstein this was obvious, since he believed strongly in the Principle of Relativity. The price he had to pay is that he had to manipulate the classic notions of space and time in order to keep the velocity of light, which is space divided by time, the same. This was the starting point of the construction of his Special Relativity in 1905.

One consequence of Special Relativity is that no information can travel faster than the speed of light. Since this is incompatible with the instantaneous action of Newton's gravitational force, Einstein realized he had to do something to make gravity consistent with Special Relativity. In the years to follow, Einstein succeeded in doing this by inventing a 2-step procedure for gravity. Suppose there is no Sun and no Earth, then, according to Einstein, our space is flat. To visualize flat space, it is best to compare it with a sheet under tension. Putting the Sun into space will cause the space around the Sun to get curved, like putting a heavy ball on the sheet causes a hole in the sheet. Compare the Earth with a little marble. On a flat sheet the marble follows a straight line but approaching the hole

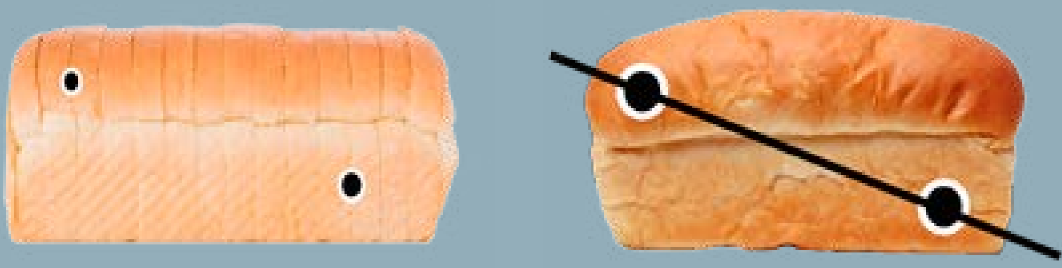


FIGURE 1 The sliced bread (left) represents Newton-Cartan geometry while the un-sliced bread (right) stands for Riemannian geometry. The currants right are in the same slice of bread.

caused by the Sun it falls into it and starts circling around the Sun. The nice thing about this 2-step procedure is that Einstein built in a delay effect: the curvature of space propagates not instantaneously but with the speed of light. Putting the Sun into space is like throwing a stone into the water: the stone causes ripples in the surface of the water that propagate with a finite speed. Similarly, the Sun causes ripples in spacetime that propagate with the speed of light. These ripples of spacetime are the gravitational waves that have been detected earlier this year by the LIGO experiment.

Not only had Einstein in this way made his General Relativity consistent with Special Relativity, by 1915 he had also succeeded in formulating his equations in a frame-independent way. It was only 8 years later, in 1923, that Élie Cartan realized that by using geometry you can also formulate Newton's law in an arbitrary reference frame. This improved theory is now known as Newton-Cartan gravity. One difference with General Relativity is that instead of Riemannian geometry you need a so-called Newton-Cartan geometry. The difference between Newton-Cartan and Riemannian geometry is best illustrated by comparing a sliced Dutch currant bread (Newton-Cartan geometry) with an un-sliced one (Riemannian geometry), see Fig.1. At the left each slice of bread represents the Universe at a given time. Note that the un-sliced bread at the right can be sliced in many different ways: vertically but also diagonally. Consider two currants in the bread, one at the top-left and one at the bottom-right, each of them stands for a particular event in spacetime. Looking to Newton-Cartan geometry we see that the two currants are in a different slice of bread and therefore happen at a different (absolute) time. In the case of the un-sliced bread there are many ways of slicing the bread such that the two currents are in a different slice of bread. But there is also one way of slicing the bread diagonally such that the two currants are in the same slice of bread and therefore happen at the same time. In other words, in General Relativity time is relative!

In the years that followed, there was not much interest in Newton-Cartan gravity for a good reason: to describe gravity General Relativity is better than Newton's theory! Things started to change in the 1990's when 't Hooft [1] and Susskind [2], basing themselves upon their research on Black Holes in General Relativity, introduced the so-called Holographic Principle, which states that all information about a gravitational theory in a given volume is contained in a Quantum Field Theory (QFT) that is defined on the boundary surface surrounding that volume (Fig. 2). The fascinating thing about this Holographic Principle is that it relates two theories to each other that at first sight are completely different. On the one hand there is a gravitational theory and on the other hand we have a QFT that is defined in a different dimension and that seemingly has no relation with gravity. Nevertheless, the Holographic Principle states that out of (the collective behavior of) the quantum degrees of freedom of the QFT should emerge the spacetime and geometry of Einstein's General Relativity. An attractive feature of the Holographic Principle is that, looking into the details, it relates General Relativity to strongly coupled QFT, which is a corner of QFT we do not know much about but which is needed to investigate non-perturbative phenomena such as the confinement of quarks or the quark gluon plasma.

Soon it was realized that the Holographic Principle can be extended to a non-relativistic holography by taking background geometries in General Relativity that have non-relativistic isometries. Holography relates such gravity theories to non-relativistic QFT's that can be used to gain new insights into a wide range of non-relativistic non-perturbative phenomena such as cold atoms, quantum-critical points in condensed matter, strange metals and high-temperature superconductivity [3]. It is in the context of this non-relativistic holography that recently NC geometry has emerged as a background geometry of the non-relativistic QFT.

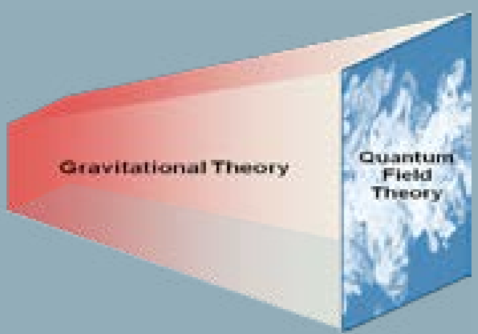


FIGURE 2 The Holographic Principle
The holographic principle states that all information about a gravitational theory in a given volume (left) is contained in a QFT that is defined on the boundary surface surrounding that volume (right).

Independent of the holographic approach, the QFT's of the type that arise at the boundary can also be applied as the lowest-order terms of Effective Field Theories (EFT's). In the Condensed Matter community it was realized that frame-independence is not only relevant to gravity but also to these EFT's [4]. Later came the insight that this frame-independence can be obtained by coupling the non-relativistic EFT to a NC background. It is well-known how to couple a relativistic EFT to General Relativity. In contrast, the details of how to couple an EFT to a NC gravitational background were only worked out in 2014.

The developments described above have promoted NC gravity and NC geometry as a novel tool to obtain new insights into the non-perturbative properties of a variety of non-relativistic models. Douwe Bob ended a bit disappointedly at the 11th place in the final of the Eurovision Song Contest. I am convinced that NC gravity and NC geometry will rank higher in the research agenda of the coming years! •

References

[1] G. 't Hooft, Dimensional Reduction in Quantum Gravity, Salamfestscrift 0284-296, World Scientific (1993), ISBN- 978-981-02-1421-0.

[2] L. Susskind, The World as a Hologram, J. Math. Phys. 36, 6377 (1995)

[3] For a modern review with many references, see Y. Liu, K. Schalm, Y.-W. Sun and J. Zaanen, Holographic Duality in Condensed Matter Physics, Cambridge University Press (2015), ISBN: 9781107080089.

[4] One of the advocators of NC geometry in this context is Son, see, e.g., D. T. Son, Newton-Cartan Geometry and the Quantum Hall Effect, arXiv:1306.0638.

AUTHOR: NICK LUTJES

From Internal Relations & the Secretary

It's amazing how quickly the board year passed. One week you're installed, the next half a year has passed and another week later you suddenly have your successor ready to take over. In the last seconds before I hand over the reins I'll take this opportunity to tell something about me.

For those who haven't met me yet, I'm Nick Lutjes. Born in Assen, raised in Ruinen and now studying and living in Groningen. If it was only for moving I wouldn't have seen a lot of the world. Luckily, I love to travel and to see the world. Something I did a lot over the past year.

It started out with going to Copenhagen on a sudden whim, during the final weeks of the summer holiday of last year. I saw some more of the Netherlands by visiting national meetings of Physics and Mathematics + Computing Science. More of Germany during an international meeting and a visit with the Huygens committee. A bit of Greece when my parents invited me on a trip there for their 25th wedding anniversary.

Last but not least of course Russia and Estonia which we visited with the KBE. Next year, Japan is up for a visit with the GBE, as one of its organizers I can really recommend it. See gbe.fmf.nl for more information.

Next to travelling, I'm also quite fond of documenting my travels with my camera. Maybe I'll try my hand on underwater photography someday, when I've finished my diving course, which I started in the year before my board year, but never got around to finishing. When there's no travelling to be done, whether it's above or underwater, I like to game a bit. A fun game I just discovered, this weekend, is crystallize. For more details on the game see "In the News."

It's a strange function, commissioner of internal relations. The one week you're being drowned in the responsibilities you have, the next week there's basically nothing to be done. Just recently, I was going through all the posters of the activities we had. There have been a lot of activities, all in all, over 120! My function is managing the calendar and helping the committees who make everything possible. The bordcie was a nice addition this year. Even though we already have well over 30 committees the bordcie still had a place, with at least 30 people showing up for the board games evenings. Not only that, but they also introduced Dungeons and Dragons to the FMF, which was quite well received.

Through a weird twist during the year, I got an additional function. The downside being the extra work it entailed, the upside being that I've got 2 successors now! That was it for now. I'm ready to hand over the reins, to both my successors. I wish you both and of course the other board candidates a great board year! •

AUTHOR: **MARTINE SCHROOR**

Student Abroad

Master thesis in Melbourne - Australia

When I set foot on Australia approximately five years ago during the study trip of the FMF, Cookaburra '11, I realised that I wanted to leave the Netherlands and move there or at least return once more for an extended period. Fortunately this happened on October 30th 2015.

My supervisor at the RuG, prof. Pallante, was very keen to help me when she heard that I wanted to go to Australia. Luckily she had some connections over there and eventually this resulted in me going to the University of Melbourne for six months.

Since the academic year runs from approximately March till November,over there, my time of arrival was not the best and I had to organize a place to live from the hostel I stayed at. All the colleges and cheap places were filled up of course. I ended up in the central business district, at the main street of Melbourne across Flinders Street Station with a beautiful view on St. Paul's cathedral.

"I ended up in the central business district"

Before my first day at the University of Melbourne (UoM) even started, I had a meeting with one of the students of the physics student society. On the internet I had found that there were actually two study associations for physics students. One for all students and one for postgraduates only. I got excited when I saw that there would some sort of FMF down there too, so I contacted them and one of the students wanted to meet and show me around on the campus which was great!

Unfortunately, or maybe: 'luckily' as there is more time for studies and less distraction, the societies are not the same as we are used to in the Netherlands. They organize much less activities and they do not have a room like the FMF where you can hang out.

The next day I started and got a desk in an office where a few PhD students were located already. The number of students increased to seven eventually. We often had very interesting conversations, usually about physics. There were also offices with experimental physics PhD's and a big room, referred to as 'the barn', due to the big number of students, full of master and some bachelor students. Each master student gets appointed a desk for their studies, not just for the research project. At least this was the case for the research group I was in. This group is the Centre of Excellence of Particle Physics at the Terascale (CoEPP). The centre consists of 4 universities, so called 'nodes', one in Sydney, one in Adelaide and two in Melbourne. Every week there was a Skype meeting between all the nodes, during which new papers or problems that researchers encountered were discussed. Each node specializes in a different part of particle physics. For example the theorists of the University of Melbourne node worked a lot on Dark Matter, so you can guess what my master project is about. The experimentalists focused on supersymmetry. However, in Adelaide they focus more on quantum chromodynamics, at least the theoretical group. The experimental side of CoEPP has collaborations with CERN and BELLE II amongst others.

"You can probably imagine I still miss tea time"

Every week there were lunch talks as well, where a staff member or PhD talks about their research. It is very interesting and inspiring to hear what everybody is working on! As I did not take courses in experimental physics, it is nice to hear more on how a detector actually works and how it can be improved for example. When the 750 GeV diphoton excess was officially announced by ATLAS and CMS, several lunch talks were dedicated to this. But of course the rumours had spread before already.

Apart from that, there was a colloquium on a weekly basis; these were not necessarily on particle physics, but also on applied physics and astronomy/astrophysics. The latter are also offered at the University of Melbourne.

Each Thursday morning was tea time, maybe some British influences here! Anyway, there was tea, good coffee, although you could get good coffee on any time on the day there as the group had a Nespresso machine, and very fancy snacks varying from sweet to savoury. You can probably imagine I still miss tea time.

After a week or so I finally met the man who made it happen, prof. Volkas. He agreed to let me visit and I am very grateful for that.

We had a few meetings during which he gave me some research options to pick from and I decided to work with one of his PhD students on dark quantum chromodynamics. The idea is that we try to explain what dark matter is made of. For this we use quantum chromodynamics, the theory of the strong interactions.

I just finished reading on the topic when I heard that I had to present a poster on my research during the annual workshop of CoEPP. At this workshop all nodes meet in a hotel for five days. Each student in CoEPP is supposed to present a poster which resulted this year in roughly 75 posters. The conference room almost had new wallpaper, even the windows could not escape being covered.

The conference of this year took place in Torquay, close to Melbourne. Prior to the workshop there was a mandatory summer school. We learned a lot of the basics to be able to understand the talks later given that week.

We did not do solely serious stuff. One day we went for surfing lessons with approximately 40 colleagues on a nearby beach. Funny thing was that several people were afraid of the temperature of the water, which they reckoned would be 'too low'. But the ocean was at least 25 degrees Celsius, so I did not understand where the fuzz was about. Compare this to the temperature of the North Sea.

FIGURE 1 Koala in tree at French Island.

Anyway, I was not the only one looking ridiculous, most of the Australians were not able to surf either.

The time around New Year's Eve, I spend some days with a few of my colleagues in a cottage outside Melbourne to celebrate New Year. We went to the beach every day, for a swim and fish & chips. This seems to be a very Australian thing to do. Initially, I was sceptic as I expected lots of sand in my food, but it is not as windy as we are used to in the Netherlands. The food had crunch from the fried batter only, as it is supposed to. Apart from hanging out on the beach and barbecuing at the cottage, we did nothing, which was nice for a change.

As there were lots of bushfires at that time, we had to check our phones regularly in case we had to evacuate. Fortunately, we were at the right side of the woods that burned down, but it is very sad to see and it feels unreal. Maybe because we hardly ever encounter this phenomenon in the Netherlands. The forests in Australia actually need the fires every now and then to be able to reproduce.

During my stay in Melbourne, I have of course seen much more than just the office. I spend quite some time in the royal botanical gardens or parks close to my place. Sometimes to work, as for some parts of the research I only needed pen and paper. I have experienced three heat waves, but I actually quite liked that, though 45 degrees or over is tough... At least it is very sunny and not cold! By heat wave I mean one in Australian terms, i.e., five days above 35 of which three or more days over 40 degrees. So on the really hot days I did not go to the beach as it is incredibly hot. Now that I have visited Australia, I understand how scorching the Sun can be and that you can actually get a sun burn even at spots covered by clothes.

All in all it was a very exciting experience where I not only learned a lot about physics, but also about different cultures and nature. I can really recommend studying abroad •

{kxa} De dataspecialisten

Software Innovations

KxA software innovations is gevestigd in de provincie Groningen. Het is een uniek bedrijf dat innovatieve, gekke, grote, kleine, duurzame, sociale, maar natuurlijk ook normale maatwerk software-opdrachten uitvoert. De overeenkomst tussen al deze projecten is dat het gaat om data in alle soorten en maten, bijvoorbeeld:

- Het Nederlandse verkeer in 400 miljard metingen toegankelijk opslaan
- In een stal het gedrag van koeien monitoren
- Software ontwikkelen voor de gigantische SKA radiotelescoop

van BIG BANG tot

- Hulpverleners in de zorg ondersteunen met VCA

Werken bij KxA

Bij ons vind je allerlei achtergronden (natuurkunde, informatica, AI, etc). Iedereen deelt het enthousiasme voor softwaretechniek en wat je daar allemaal mee kunt doen.

We hebben regelmatig afstudeeropdrachten, stageplekken én vacatures. Je krijgt hierbij een opleidingstraject om je helemaal in ons vakgebied te bekwamen. Het vervoer naar Visvliet kan geregeld worden.

Ben jij geïnteresseerd in het werken bij een High Tech bedrijf? Kijk dan eens op **www.kxa.nl**, of neem contact met ons op via mulder@kxa.nl

AUTHOR: **ARSALAN TORKE GHASHGHAEE**

Plasmonics

Plasmonics, in principle a very clever way to achieve optical information exchange on a nano-level (bypassing the diffraction limit) without requiring revolutionary physics. Also, it's not that hard to understand, the basics of it anyway. And the potential applications: promising, to say the least.

Plasmonics is the science dealing with plasmons. A plasmon is a collective oscillation of electrons. There may be a chance you're still fuzzy about this and can't picture it, let's elaborate on this by means of visuals. You'll need to provide the visuals in your mind. Take a metal sphere and shrink it down to a radius of about 10nm. This tiny sphere, being of metal, is chock full of free electrons. The electrons are not bound to an atom and can therefore move freely among metal atoms. This is called a free electron gas, or FEG. In ordinary circumstances, the FEG is distributed homogeneously, leaving the tiny sphere devoid of any polarity. In other words, your sphere is electrically neutral. Apply an electric field to the sphere and the electrons will be attracted to the positive side of the field. Thus, the FEG forms a lump on one side of the sphere, a negatively charged lump. The sphere is now slightly negative on one side and consequently slightly positive on the other. It has poles [figure1]! Now then, if you would switch the polarity of the electric field, the FEG would lump up on the other side of the sphere. With every switch of the field, the electrons making up the FEG will move to the other side of the sphere. So if you have an oscillating electric field, the FEG would oscillate. A collective oscillation of a bunch of electrons, A plasmon!

Before moving on an appetizer is given. Simply as a cheap means to keep the reader hooked for that moment when she or he understands how the applications can be achieved. The prospects are computer chips utilizing optical information exchange, improved solar cells, cancer treatment and invisibility.

Let's talk parameters. Would every sphere suffice? No. Every metal? Not really. The interest here lies in the spheres being small, as in the 10nm radius mentioned above. Why? Practicality. When exploiting the effects of plasmons on nano-scales, nano-scale materials are necessary. The most practical oscillating electric fields are electromagnetic fields, such as light. It's not only practical because it oscillates but also because of how its average wavelengths fit in with the use of tiny metal spheres. Those will be called Metal Nanoparticles, or MNPs. To obtain a unified oscillation of the free electrons in an MNP, the applied electric field must be homogeneous across the entire MNP. Otherwise on one side of the MNP the field could point one way, and on the other side another way. With light having wavelengths on the order of hundreds of nanometers, applying that to an MNP with a radius of 10-20nm ensures that one MNP can be placed inside one 'wave' of light. Thus ensuring that the electric field is homogeneous along the entire MNP [figure 2]. Also of importance is the medium in which the MNPs are placed. This has to be a dielectric, like an insulator, say, glass or air.

Crucially, the right combination of parameters can lead to a resonance of the FEG. This resonance is called a Localized Surface Plasmon, where localized refers to the fact that the plasmon is isolated to the MNP and surface refers to the fact that oscillations occur at the surface of the MNP. The reason for the latter is that electrons, which are trying to cross from one end of the MNP to the other, have to travel through the bulk of metal atoms in the MNP and are thus slowed due to collisions.

One key features that is exploited in nanophotonics is called local field enhancement, or LFE. This refers to the strong magnification of light intensity in the near vicinity of the surface of the MNP. In laymen's terms, things get kinda bright. This LFE effect has led to plasmons being utilized to improve solar cell effectiveness [1]. Because more light means more output, no? In fact, though the real-world improvement in solar cells isn't astonishing, there is an area of science that has found a distinct benefit in this feature. Raman-spectroscopy, a technique used to identify molecules based on their vibrational fingerprint [2], can be enhanced greatly by utilizing plasmonics. This improved method is called Surface Enhanced Raman Spectroscopy, or SERS [3].

Perhaps a more fascinating use can be found in the way the distinctive features of plasmonics are employed in cancer treatment. Attaching nano-sized particles to certain biological substances and then inject this combination into the bloodstream is nothing particularly new. Such methods can be used to detect the movement of particular substances in the human body. Now, imagine a nano-sized spheres made of a dielectric material and cover this with a layer of metal. Injecting a substance consisting of such spheres into the bloodstream such that they attach themselves to cancer cells and shining harmless infrared radiation on them heats them up. The LSPs heat up so much that they kill off the cancer cells they're attached to [4,5].

When it comes to awesomeness, though, nothing can really beat computer chips. Chips as we know them use electricity for information transfer. The thing is, with its ridiculously high frequencies, light can be a

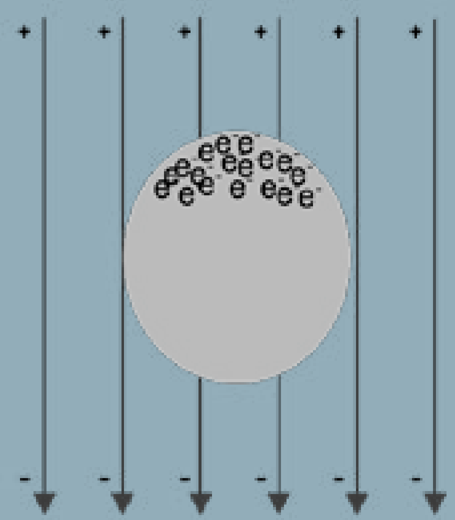


FIGURE 1 source: http://nanocomposix.com/pages/plasmonics

much more effective bearer of information than electricity [6]. The problem is the diffraction limit.

Put a single MNP in an oscillating electric field and it will become polarized. In other words, it'll turn into a dipole. Because of this the MNP will emit its own electric field, a dipole field. Now imagine putting another MNP some distance off this first one, and set it up such that only the first MNP feels the effects of the incident electric field that is shone on it. This first MNP behaves like a dipole and starts emitting its own electric field. The neighbouring MNP will subsequently be affected by this dipole field, and in turn starts behaving like a dipole as well. The idea isn't so much that a dipole game is played, it's that the neighbouring MNP now 'knows' that there is an incident signal without directly having experienced it. Put a third MNP in line and it will feel the effects of the dipole field of the first MNP and the second MNP. Continuing like this an arbitrarily long chain can be made of MNPs with the initial optical signal being transferred along the chain. Important to note is how the dipole field of the third MNP will also again influence the first and second MNP. Really the whole setup involves a big web of interacting MNPs [figure 3]. With every flip of the field however the polarity will flip as well. So now the MNPs behave like oscillating dipoles and it is immediately noticeable how the frequency of the incident electric field can be utilized in information transfer in such a scenario.

Fire up the machines and let's make those plasmon computer chips! Not so fast, there are downsides of course. A significant one is the strength of the signal along the chain. Sending a signal from one place to another almost always involves the signal experiencing losses. In this scenario the electric field strength diminishes as the signal progresses through the chain since the strength of the dipole fields of the MNPs diminishes with distance. As such, every next MNP in the chain sees a reduction in magnitude of the electric field as compared to the initial MNP. Realistically then, signals can only travel for very short distances. To exploit this possible use of plasmons more research needs to be done. For now, mass market applications are unfortunately some way off.

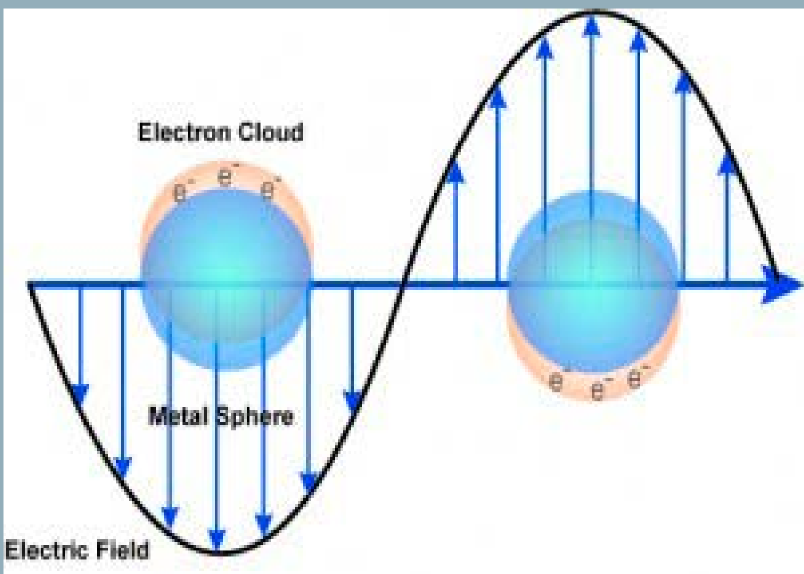


FIGURE 2 source: http://nanocomposix.com/pages/plasmonics

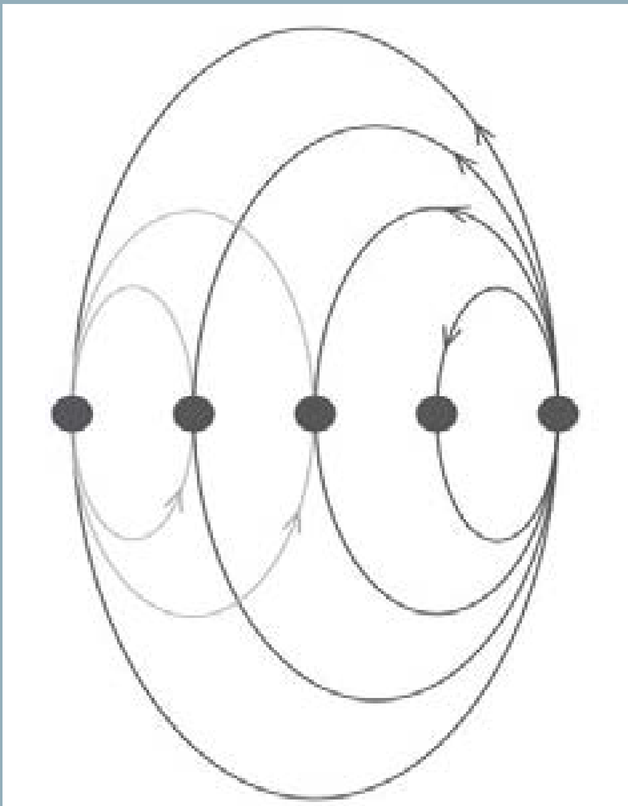


FIGURE 3

In fact, though the concept of plasmonics was unconsciously used centuries ago by craftsmen making stained glass [7,8] (yes, plasmonics are responsible for those colours), the beginning of the previous century proved the starting point for the underlying theory to start to be constructed [9,10]. Then through the decades some research here and there shed more light on the issue before improved manufacturing in the late century allowed proper experiments on nano scales to be performed. Since then the hype reached somewhat of a fever pitch and the subject of plasmonics was very much a hot topic. In 2016 though, things look decidedly less sexy for the field as the proposed applications are taking longer than expected. Then again, that's the downside of a hype. It usually ends going downhill. Still though, SERS!

Oh yes, about that invisibility. Turns out, it's a tad convoluted, not less awesome [6,11] •

References

[1] S. Kim et al. Plasmon enhanced performance of organic solar cells using electrode-posited ag nanoparticles. Appl. Phys. Lett., 93(7):073307, 2008.

[2] K. Scott, Raman spectroscopy, University of St. Andrews, https://www.st-andrews.ac.uk/seeinglife/science/research/Raman/Raman.html, accessed July-2016.

[3] P. L. Stiles et al. Surface-enhanced raman spectroscopy. Annu. Rev. Anal. Chem., 1:601{626, 2008.

[4] C. Loo et al. Nanoshell-enabled photonics-based imaging and therapy of cancer. Tech-nol. Cancer Res. Treat., 3(1):33{40, 2004.

[5] X. Qian et al. In vivo tumor targeting and spectroscopic detection with surface-enhanced raman nanoparticle tags. Nat. Biotechnol., 26(1):83{90, 2008.

[6] H. A. Atwater. The promise of plasmonics. Sci. Am., 296:56, 2007.

[7] M. I. Stockman. Nanoplasmonics: The physics behind the applications. Phys. Today, 64:39{44, 2011.

[8] S. A. Maier and H. A. Atwater. Plasmonics: Localization and guiding of electromagnetic energy in metal/dielectric structures. J. Appl. Phys., 98:011101, 2005.

[9] G. Mie. Beiträge zur optik trüber medien, speziell kolloidaler metallösungen. Ann. Phys., 330(3):377{445, 1908.

[10] A. Sommerfeld, Über die fortpflanzung elektrodynamischer wellen längs eines drahtes, Ann. Phys., 303(2):233{290, 1899.

[11] A. Myers, Cloak and swagger: Engineers use plasmonics to create an invisible photodetector, Stanford University, http://news.stanford.edu/news/2012/may/plasmonics-invisible-photodetector-052212.html, 2012, accessed July-2016.

[12] A. Torke Ghashghaee, On the effects of disorder on signal transmission through a chain of localized surface plasmons, Master's thesis, University of Groningen, 2015.

AUTHOR: **MARIEKE MUDDE**

Iedereen aan de wiskunde krijgen

Wiskundigen schrijven zelden voor een breed publiek. Ze zien het niet als hun taak, mensen vinden het niet leuk om over wiskunde te lezen en het is lastig om eenvoudig en aantrekkelijk over wiskunde te schrijven. Dit artikel onthult zes tips om succesvol populairwetenschappelijk te schrijven over wiskunde.

Vorige maand verscheen in het nieuws dat een Italiaanse economiehoogleraar uit een vliegtuig werd gehaald omdat hij volgens de vrouw naast hem verdachte aantekeningen maakte. Ze zag onbegrijpelijke symbolen en kromme lijnen. De vrouw meldde dit aan de bemanning, die vervolgens de hoogleraar uit het vliegtuig haalde. De hoogleraar liet daarop zijn aantekeningen zien. De bemanning schaamde zich diep toen bleek dat hij alleen maar wiskundige formules opschreef voor een presentatie tijdens een conferentie.

"Ze zag onbegrijpelijke symbolen en kromme lijnen."

Dit voorbeeld laat goed zien dat veel mensen weinig kennis van wiskunde hebben. Ze herkennen symbolen en lijnen niet als wiskunde. Niet alleen weten mensen weinig van wiskunde, ze zien het nut en de schoonheid van wiskunde ook niet in. Ik merk dit in mijn eigen leven ook. Als ik aan mensen vertel dat ik wiskunde gestudeerd heb, kijken mensen mij verbaasd aan. Ze stellen vragen als: 'Wat kan je nou met wiskunde?' en 'Vind je wiskunde echt leuk?' Daaraan voegen ze meestal toe dat ze op de middelbare school altijd een hekel hadden aan wiskunde.

Weinig populairwetenschappelijke boeken over wiskunde

Veel mensen vinden wiskunde moeilijk of saai en daardoor lezen weinig mensen populairwetenschappelijke boeken over wiskunde. Dit in tegenstelling tot andere vakgebieden. Populairwetenschappelijke boeken over biologie en psychologie zijn razend populair.

Het slechte imago van wiskunde is niet de enige reden waarom er weinig populairwetenschappelijke boeken over wiskunde geschreven worden. Het is ook de schuld van de wiskundigen zelf. Wiskundigen zien het niet als hun taak om over wiskunde te schrijven voor een breed publiek. De Britse wiskundige Godfrey Harold Hardy verwoordde het ooit zo: 'De taak van een wiskundige is om iets te doen, om een nieuwe stelling te bewijzen, om iets toe te voegen aan de wiskunde, en niet om te praten over wat hij of een andere wiskundige heeft gedaan.'

Daarnaast is het ook heel ingewikkeld om aantrekkelijk over wiskunde te schrijven. Wiskunde is abstract en bestaat uit ingewikkelde symbolen en formules. Het is moeilijk om de vertaalslag te maken naar het grote publiek.

Het is zonde dat wiskundigen het schrijven over wiskunde niet als hun taak zien en dat het zo lastig is om over wiskunde te schrijven. Hierdoor ziet maar een klein gedeelte van de bevolking de schoonheid en het nut van wiskunde in. Het is belangrijk dat meer mensen kennis van wiskunde krijgen, omdat wiskunde overal in het dagelijks leven terugkomt. Zo zit wiskunde in de natuur, maar ook in het spelen van spelletjes als Candy Crush en Pacman.

Drie soorten publiek

Om aantrekkelijk over wiskunde te schrijven, is het eerst belangrijk om je publiek te kennen. Volgens wiskundige Steven Strogatz zijn er drie soorten mensen.

De getraumatiseerden zijn ooit vernederd door de wiskunde. Dit kan al gebeurd zijn op de basisschool bij het leren van tafels, of later op de middelbare school bij kansberekening. Voor deze mensen is wiskunde een trieste herinnering, een blijvende deuk in hun ego.

Daarnaast heb je de verbijsterden. Deze groep mensen heeft geen traumatische ervaring met wiskunde opgelopen in hun jeugd. Ze vonden wiskunde gewoon zinloos. Ze konden sommen oplossen, maar wisten eigenlijk niet wat ze aan het doen waren.

Tot slot zijn er nog de natuurtalenten. Zij hebben een wiskundeknobbel. Ze snappen wat ze doen en het geeft ze voldoening als ze een som succesvol weten op te lossen. In zeldzame gevallen gaan ze wiskunde studeren. Velen komen in een gerelateerd werkveld terecht zoals boekhouding of techniek. Helaas gebruikt een groot aantal wiskundetalenten in hun werk nooit wiskunde. Echter, ze zullen hun hele leven nog aantrekking tot wiskunde voelen. Dit zijn de mensen die populairwetenschappelijke boeken over wiskunde lezen.

Om succesvol over wiskunde te schrijven voor een breed publiek, moet je niet alleen de natuurtalenten, maar ook de getraumatiseerden en de verbijsterden bereiken. Hieronder volgen zes tips om hierin te slagen.

Tip 1: Laat zien dat wiskunde belangrijk is

Zoals eerder genoemd, zien de verbijsterden het nut van wiskunde niet in. Dit geldt ook voor de getraumatiseerden. Laat daarom zien wat je met wiskunde kan. Een goed voorbeeld hiervan is het redden van mensenlevens door gebruik te maken van wiskunde. Wiskundige Rob van der Mei vertelde tijdens het evenement Bessensap over zijn onderzoek om ambulances beter over de regio te verspreiden. Hij heeft een model ontwikkeld dat aan ambulances doorgeeft waar ze heen moeten rijden, ook als er geen ongeluk in hun buurt is. Dit verkort de aanrijtijden aanzienlijk. Rob van der Mei zei: 'Dit is een schoolvoorbeeld van wat je met wiskunde kan.'

Tip 2: Geef de lezer een aha-erlebnis

Laat de lezer het licht zien. Hierdoor zal hij van wiskunde gaan houden. Als voorbeeld gebruikt Strogatz het kwadraat. Geen enkele docent vertelt dat het woord kwadraat van het Latijnse quadratus komt, wat vierkant betekent. Door dit wel te vertellen, wordt het begrip kwadraat ineens veel duidelijker. Twee kwadraat betekent twee keer twee en de uitkomst hiervan kan in de vorm van een vierkant gelegd worden, met twee voorwerpen in de lengte en twee in de breedte. Je moet de lezer dus een succeservaring geven. Vooral voor de getraumatiseerden werkt dit goed: eindelijk snappen ze iets.

Tip 3: Verbind wiskunde aan interessante onderwerpen

Wiskunde wordt aantrekkelijker als je het koppelt aan onderwerpen waar mensen iets mee hebben. Voorbeelden hiervan zijn sport, muziek, films en liefde. Door wiskunde te koppelen aan deze onderwerpen, wordt de niet-wiskundige lezer uitgenodigd. Zij voelen zich dan ook welkom. Wiskundige Hannah Fry doet dit in haar boek Liefde volgens de wiskunde erg goed. Door in haar boek wiskunde te verbinden aan liefde, wordt het boek bereikbaar voor iedereen.

Tip 4: Zie de lezer als een vriend

Wiskundigen zijn gewend om hun stukken in een vaste volgorde op te schrijven. Ze vermelden de aannames, noemen de stelling en tot slot bewijzen ze de stelling. Ze denken niet na over wat de lezer wil weten. Om succesvol over wiskunde te schrijven voor een breed publiek, moet je dit wel doen. Door de lezer te zien als een vriend zonder wiskundekennis, zul je automatisch met de juiste toon schrijven. Ook zul je hierdoor automatisch jargon vermijden.

Tip 5: Gebruik zo min mogelijk formules en symbolen

Formules schrikken met name de getraumatiseerde lezer af. Gebruik in plaats daarvan tabellen, infographics en afbeeldingen. Vermijd ook het gebruik van symbolen. De lezer kan de symbolen niet lezen en daardoor het symbool ook niet in hun hoofd horen. Hierdoor zullen ze afhaken. Rob van der Mei deed dit in zijn praatje erg goed. Hij gebruikte geen enkele formule en verduidelijkte zijn oplossing om ambulances dynamisch over de regio te verspreiden door gebruik te maken van een animatie. De animatie liet het verplaatsen van ambulances in de provincie Flevoland zien. Hierdoor begreep de luisteraar direct wat Van der Mei bedoelde.

Tip 6: Nummer figuren niet

Het nummeren van figuren komt over als een tekstboek, dit is onaantrekkelijk voor met name de getraumatiseerden. Plaats figuren ook niet boven of onder een tekst, maar precies op de plek waar je over de figuren praat. Hierdoor hoeft de lezer niet meer te zoeken naar de juiste figuur, wat het leesgemak vergroot.

Deze tips zullen er hopelijk voor zorgen dat wiskundigen meer over wiskunde gaan schrijven voor een breed publiek. Dan zullen in de toekomst steeds minder mensen aan wiskundigen vragen waarom zij wiskunde gestudeerd hebben en wat daar leuk aan is. Steeds meer mensen zullen de schoonheid van wiskunde in gaan zien en wiskundigen bewonderen omdat zij zich bezig houden met dit mooie en interessante vak •

Top 3 populairwetenschappelijke wiskundeboeken

[1] Liefde volgens de wiskunde - Hannah Fry
[2] Getallen ontraatseld - Alex Bellos
[3] Ik was altijd heel slecht in wiskunde - Jeanine Daems en Ionica Smeets

Previous Brainwork

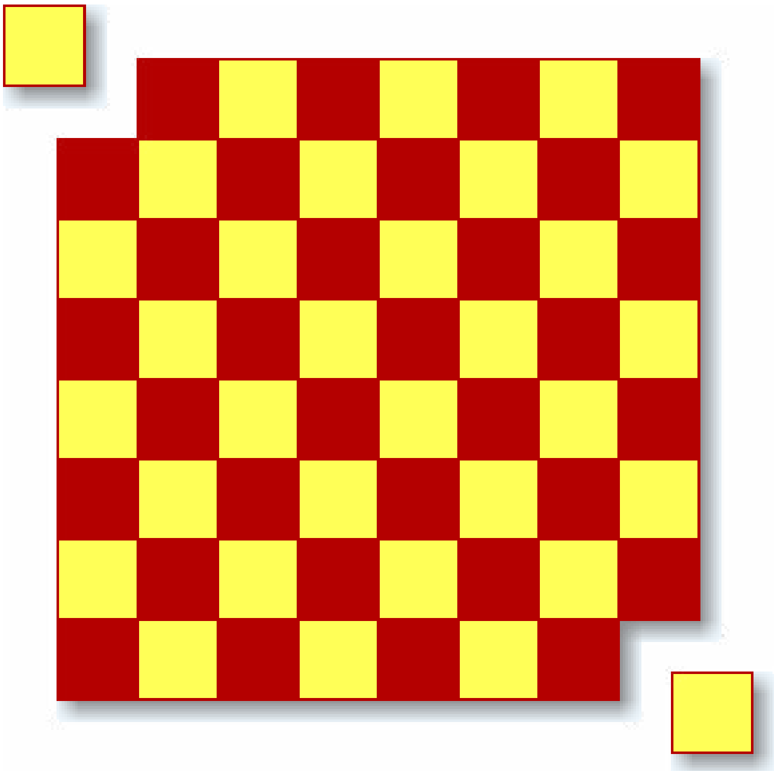
A Cryptic Rebus

Due to some problems with the shipping of the previous Perio*diek, many of you did not have a chance to hand in your solutions for the previous brainwork. Therefore, we have decided that the deadline for "A cryptic rebus" has been postponed to the 21th of October 2016. You can send your solutions to perio@fmf.nl. Among the right solutions we will select the winner of the book "Cakes, Custard and Category Theory, Easy Recipes for Understanding Complex Maths" by lottery •

New Brainwork

A filled chessboard

When we were working on this magazine in the FMF members room there was a chessboard laying on the table. As we were thinking for a puzzle for the "Brainwork", we considered filling the entire board with dominoes. Considering that a chessboard is 8 by 8 this was not such a difficult job indeed. Therefore we have come up with a twist. Suppose that we cut off two squares at diagonally opposite corners of the board. Can we now fill the entire board with 31 dominoes?



Is it possible to place the 31 dominoes on the board so that all the remaining 62 squares are covered? If so, show how it can be done. If not, prove it impossible. The solutions can be handed in before the 21th of October 2016 at perio@fmf.nl. Among the right solutions we will select the winner of a chessboard by lottery •

AUTHOR: **JOS BORGER**

Where did all the (anti-)matter go?

Two years ago I had to write my bachelor thesis, as I did the track Theoretical Physics naturally I e-mailed prof. Timmermans to inform about the possiblities. Luckily, he still had a few spots left and we soon made an appointment.

One of the subjects he suggested was based on a paper by J.G. Cramer and W.J. Braithwaite out off 1977 titled: "Distinguishing between Stars and Galaxies Composed of Matter and Antimatter Using Photon Helicity Detection." This paper treats one of the biggest open questions in physics, namely: "Where did all the (anti-)matter go?" and it connects this big fundamental question to an experiment that could potentially falsificate our current point of view on this problem. I like to think about these fundamental questions but I realized that I, as a mere bachelor student, could not really contribute to the solving of such a problem. So naturally once I was offered the possibility to think about such matters I immediately took the opportunity.

In 1928, Paul Dirac derived what is now known as the Dirac equation, a relativistic wave equation describing massive spin-1/2 particles such as electrons. This was the first example of a theory that accounted for special relativity in the context of quantum mechanics. This equation allowed for negative energy solutions and so predicted the existence of an anti-electron now know as the positron. This particle was later observed experimentally which opened the way to other anti-particles. Antimatter particles are very similar to their regular particle counterparts, their mass and lifetime is the same, their charge however is the opposite of its regular particle. If we let the operator C change the sign of the charge of a particle and the operator P the sign of the spatial coordinates of the particle, letting the operator CP work on a regular particle would give us its anti-particle. You can think of this as looking at the anti-particle as a kind of mirror-image, and just like the symmetry of a mirror we talk about CP-symmetry. This symmetry would mean that nature treats particles and antiparticles on equal footing. When an anti-particle and its particle meet they annihilate, which means that they disappear and their energy is converted into photons or other particle anti-particles pairs. Now this leaves us with a problem, matter and anti-matter are created in equal amounts but when we look around we only see one of the two. Namely if matter and antimatter would be distributed around the cosmos in equal proportions we would expect there to be areas where the two meet. This would mean that annihilation would happen in these areas and we could observe radiation (the energy converted in photons) coming from these areas. We do not observe this radiation so we conclude that our cosmos consists solely of matter. We can solve this problem in two not mutually exclusive ways:

1) We assume nature treats matter and antimatter differently, in other words we say that the CP-symmetry is violated. In this particular case this would have to mean that slightly more anti-particles disappear then regular particles when annihilated. This could solve our problem because although during the Big Bang equal amounts of matter and antimatter were created, upon annihilation slightly more antimatter disappeared and thus some matter remained, composing all massive things we see today. This CP-violation has been experimentally observed, however the observed violation was very small for purposes of explaining our problem, i.e., it could account for some matter still existing, but not all that we see.

2) We assume that the matter and antimatter is spatially separated. This would be an explanation why there are no interaction areas where annihilation would happen. If we assume this we of course want to explain why these parts are spatially separated but this is currently not of my concern. Since the laws of gravity are assumed to be the same for matter and antimatter, if there is a reasonable amount of anti-matter, we expect formation of stars and galaxies to happen for anti-matter just like for regular matter.

From the lack of observed annihilation radiation, we conclude that there are no interaction areas in our near vicinity. And although CP-violation has been observed, in our current model of the Big Bang it can not account for all our galaxies consisting of one type of matter. The second proposed solution predicts the existence of whole anti-matter galaxies. The lack of interaction areas lets us conclude that there are none of these galaxies in our near vicinity but what if they exist but just far away? To be able to say anything about this we need a way to distinguish between an anti-matter galaxy and a regular galaxy without the need for a interaction area. We need a way to be able to distinguish between the two by just looking at them. I looked at a way this can be done following a 1977 article by Cramer and Braithwaite. This method uses the predicted difference in polarization between emitted photons of stars and anti-stars.

Fermions can be left or right handed, unfortunately the exact meaning of this statement is a little bit too much for this article so I will just state it here. At high energies this left or right handedness corresponds to the helicity of a fermion. Helicity is the projection of the angular momentum of a particle on its momentum, which is something that can be measured! A peculiar property of the weak force is that it treats the left and right fermions differently.

In order to predict a difference between stars and antistars we need to know that kind of processes take place inside of them. Although there are a lot of complicated processes happening inside stars it all comes down to protons getting turned into neutrons. This happens via β+-decay and electron capture. This β+ process gives rise to positrons with almost only right-handed helicity and electron neutrinos that are left-handed. In an antistar we would see “anti β+-decay”, a process that will turn a proton into a neutron, an electron and an anti electron neutrino. This process would only produce left-handed electrons and right-handed antineutrino’s. This means there would be a difference between stars and anti-stars. The nuclear processes in the star produce right-handed positrons and left-handed neutrinos while the antistar produces left-handed electrons and right-handed neutrino’s.

Positrons formed by the β+-decay do not live very long in the dense environment that is the nucleus of a star. These positrons will annihilate via the electron-positron annihilation process. Now I am interested if this handedness of the positrons is handed over to the created photons in the form of a preferred polarization. It took me quite some time to calculate this especially because I did not follow the master course Quantum Field Theory yet but in the end I got the calculation right and showed that this preferred handedness is indeed handed over in the form of a preferred polarization of the created photons.

The polarisation of photons is measurable and one might naively think that this can be done to distinguish between stars and anti-stars. However, we have to realise that these nuclear processes happen in the core of the star/anti-star. Since the core of a star is very dense we expect the electron/positron to annihilate very quickly, the photon emitted with a preferred polarization then has to travel from the core of the star to its surface. Since this is a very dense environment the photon will only travel a small distance before it runs into a hydrogen/anti-hydrogen atom and is absorbed and later on re-emitted in a random direction. This means that it will take the photon a considerable amount of time to travel from the core of the star to its surface. It is estimated that it takes the photon around 170.000 years [2] to reach the surface of the Sun. This means the photon has a lot of interactions before it is finally radiated out in space. These interactions are of electromagnetic nature and will therefore not conserve the preferred handedness. 170.000 years of interactions mean that even if the produced radiation had a preferred handedness, this preference will fade out by the time the photon reaches the surface and hence we cannot observe it here on Earth.

In my main article [1] the authors Cramer and Braithwaite think of an ingenious way to overcome this problem, they propose to look at supernovea. It is thought that this phenomenon happens when the fusion processes in the star have terminated with a large quantity of ^{56}Ni at the peak of the energy binding curve so that the star is out of fuel. This ^{56}Ni decays by electron capture to ^{56}Co, which decays by electron capture and positron decay to ^{56}Fe. A large fraction of the energy is released in the form of this decay sequence and since the star explodes the produced photons do not have to traverse the whole outer shell, keeping its preferred helicity.

Then the authors make an estimation of what kind of experiment is needed to measure this effect. It is estimated that a polarization meter of 1m in diameter, mounted in space, that counts for a year starting 2 weeks after the supernova would register $3 \cdot 10^5$ events, and this should be enough to give a determinationof the sign of the helicity. Effects on the helicity might also be induced on the way from the star to Earth, think of a gas cloud absorbing and re-emitting the photons. Since these effects are dependent on the place of the star/anti-star with respect to Earth one needs to observe a lot of events (determinations of sign of helicity) out of different directions to be able to statistically rule these effect out.

It is estimated that around 2 supernovae happen in our Milky Way every 100 years. Outside of our galaxy they are often hard to detect. This would make itextremely hard to direct your polarisation meter in the right direction on time.

Concluding: although nuclear processes and secondary sources produce light with a different preferred polarization for stars and anti-stars, this effect will be faded out by the time the light reaches the surface of the star or anti-star. Looking at supernovae gives us the possibility to actually observe this effect. However, the cost of the experimental set-up needed to detect the effect versus the rate at which supernovae happen make this an unrealistic enterprise.

Maybe one day neutrino's can be detected more effectively and since the weak force processes also produce neutrino's with preferred helicity these can also be used to distinguish between stars and anti-stars. Since neutrino's hardly interact they will move straight out of the stars/anti-stars and the effect will not fade out, unfortunately this lack of interaction also makes it hard to detect them here •

References

[1] J.G. Cramer, W.J. Braithwaite (1977) Distinguishing between Stars and Galaxies Composed of Matter and Antimatter Using Photon Helicity Detection. Phys. Rev. Let. Volume 39, Nr.17.

[2] R. Mitalas, K.R. Sills (1992) "On the photon diffusion time scale for the sun". The Astrophysical Journal Vol 401, Nr.2.

AUTHOR: **MAX KRONBERG**

Cryptography

A Brief Introduction

Nowadays, live without cryptography is unthinkable. Every time you open a browserto visit a website, information is exchanged between you and the server. Often this is some vulnerable information, e.g your bank account. Most servers offer the possibility to send information over a secure channel. For the user the usage of a secure channel is indicated by a green lock in the address line of the browser. Clicking on this icongives you more detailed information about the way the communication is secured. Forexample https://www.google.nl uses ECDH encryption and https://www.amazon.nl uses RSA encryption. What this means we want to describe in this article.

Let us first consider the different possibilities of a secure communication. For the first scenario, assume Alice wants to send Bob a secret message. Alice can put the message in a box and add a lock to that box. To read the message, Bob needs a key to the lock. So Alice and Bob have to meet and Alice has to hand over a copy of the key to Bob.

Since the first scenario needs a meeting between Alice and Bob, they could exchange the secret information personally instead. Thus this is not a very practical solution. A possibility to avoid a personal meeting of the two, Alice can still send Bob a locked box. Now Bob adds an additional lock to the box and keeps the key. He sends the doubly locked box back to Alice, who can now remove her lock. She now sends the box that is only locked by the lock of Bob back to Bob, who can open the box and receive the message.

The second scenario does not need a personal meeting of Alice and Bob, but the message has to be send three times until Bob is able to read it. Again, this does not seem very practical. To reduce the amount of traffic, Bob can send Alice an empty box with an open lock that can be closed without the key. Now Alice can place the message in the box and close the lock. The locked box is send to Bob, who is able to open the box with his key and read the message.

In the following section we describe two of these scenarios in a theoretical way.

Definition *A tuple* $(\mathcal{P}, \mathcal{C}, k, k', \text{enc}_k, \text{dec}_{k'})$, *where* $\mathcal{P}$ *is a set consisting of all plaintexts,* $\mathcal{C}$ *is a set consisting of all ciphertext,* k, k' *are keys,* $\text{enc}_k : \mathcal{P} \to \mathcal{C}$ *is a function depending on the key* k *and* $\text{dec}_{k'} : \mathcal{C} \to \mathcal{P}$ *is a function such that* $\text{dec}_{k'} \circ \text{enc}_k = 1$ *is called* ***cryptographic scheme.***

Theoretical Background on Cryptography

We have to distinguish between two central concepts related to the description in the introduction. A cryptographic scheme with $k = k'$ we call *symmetric*. In this case the key should be a shared secret between Alice and Bob. A scheme where $k \neq k'$ is called *asymmetric*. If the key k that is used in the encryption is made public, such a scheme is called *public key scheme*. On a first sight, it seems to be a bad idea to make information about a key public but we will see examples where this is convenient and has no practical impact on the security of the scheme.

The simplest example for a symmetric scheme you can think of is the *Ceasar Cipher*. Here $\mathcal{P}$ and $\mathcal{C}$ are just the alphabet. The key $k = k'$ is just a word, for example "ceasar". Then we set $\text{enc} := \text{enc}_k$ such that $\text{enc}(a) := c$, $\text{enc}(b) := e$, $\text{enc}(c) := a$, $\text{enc}(d) := s$, $\text{enc}(e) := r$, $\text{enc}(f) := b$ and so on.

This type of cryptographic scheme is obviously not very secure and used in practice only by low grade school kids to exchange secret love letters. But symmetric schemes are used in practice quite often. The most popular scheme of that type is called *Rijndael*. It can be thought of as the origin of modern symmetric encryption developed by Daemen and Reijmen. Nowadays we know the scheme under the name *advanced encryption standard (AES)*. A one page summary by H.W. Lensta can be found in [2].

> Encryption saves lives.
> Encryption protects property.
> Without it, our economy stops.
> Our government stops.
> Everything stops.
>
> *- Edward Snowden*

For the presentation of an example of a public key scheme we need a little bit more mathematical background.

Definition *Let* S, S' *be sets. An invertible map* $f : S \to S'$ *is called a* ***trapdoor*** *if* $f(x)$ *is easy to compute for* $x \in S$ *but* $f^{-1}(y)$ *is hard to compute for* $y \in S'$.

Example *We know that every integer can be written as a product of prime numbers in a unique way. Consider the sets* $S := \{(p, q) \in \mathbb{Z}^2 \mid p, q \text{ prime}\}$ *and* $S' := \{pq \in \mathbb{Z} \mid p, q \text{ prime}\}$ *with the invertible map* $f(p, q) := pq$. *Multiplying two integers is easy, but finding the prime factorization of an integer is assumed to be a hard problem.*

Such a trapdoor can be used by making an element $k' \in S$ the secret key and the image $f(k') =: k$ the public key. The idea is to construct an encryption function that depends only on k but the decryption function needs the knowledge of k'. The first scheme of that type was invented by the mathematicians Rivest, Shamir and Adleman in 1977 [3]. We will give a short description of the RSA scheme.

Definition *Let* $p \neq q$ *be primes and set* $N := pq$. *Choose an element*

$$e \in (\mathbb{Z}/(p-1)(q-1)\mathbb{Z})^*$$

and compute its inverse d. Set the public key $k := (N, e)$ and keep $k' := (p, q, d)$ secret. The plaintext and the ciphertext space both are given by

$$\mathcal{P} = \mathcal{C} = (\mathbb{Z}/N\mathbb{Z})^* .$$

For $m \in \mathcal{P}$ we set $\mathrm{enc}(m) := m^e$ and for $c \in \mathcal{C}$ we set $\mathrm{dec}(c) := c^d$.

Proof Let $m \in \mathcal{P}$. Then we have

$$\begin{aligned}\mathrm{dec} \circ \mathrm{enc}(m) &= \mathrm{dec}(\mathrm{enc}(m)) \\ &= \mathrm{dec}(m^e) \\ &= (m^e)^d = m^{ed}.\end{aligned}$$

Since $\#\mathcal{P} = (p-1)(q-1)$ and $ed \equiv 1 \pmod{(p-1)(q-1)}$ we have $m^{ed} = m$.

The security of the RSA scheme is based on the fact that given *e* the element *d* can be only computed with the knowledge of $(p-1)(q-1)$. But if $(p-1)(q-1)$ is known to an attacker, then he also knows *p* and *q*.

Lemma *If N and $(p-1)(q-1)$ are known to an attacker, he is able to find p,q.*

Proof We have $(p-1)(q-1) = pq - (p+q) + 1 = N - (p+q) + 1$. Therefore, knowing N and $(p-1)(q-1)$ implies the knowledge of $p+q$. Now observe $(x-p)(x-q) = x^2 - (p+q)x + N$; therefore, finding *p* and *q* is finding roots of a quadratic polynomial. This is an easy task.

This lemma states that an attacker who is able to decrypt a ciphertext is also able to factor *N*. We want to present another trapdoor that is practically used in cryptographic applications.

Definition *Let $G = \langle g \rangle$ be a finite cyclic group. Given $h \in G$, the smallest positive integer m such that $h = g^m$ is called **discrete logarithm** of h with respect to g.*

A typical example of a finite cyclic group is the group of units $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ of a finite field $\mathbb{F}_q$ with q elements. If we consider for example a prime number *p*, then the ring $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is such a field.

Given a finite group $G = \langle g \rangle$ and $h \in G$, the determination of the discrete logarithm of *h* in G is called *discrete logarithm problem (DLP)* and is assumed to be a hard problem for many groups. This can be used to accomplish the exchange of keys between Alice and Bob.

Example Diffie-Hellman Key Exchange *Alice and Bob agree publicly on a finite cyclic group G with generator g where the DLP is assumed to be hard. Now Alice, resp. Bob, choose a secret integer $a < \#G$, resp. $b < \#G$, and compute g^a, resp. g^b. These elements they send each other via a public channel. An attacker has to solve a DLP to obtain the secrets of Alice and Bob. Now both Alice and Bob can compute g^{ab} which can deal as a secret key for a symmetric communication between them.*

In the modern times where the communication becomes easier and faster for every one, a lot of effort was spend by various mathematicians and computer scientists to optimize attacks on the DLP especially in the group $\mathbb{F}_q^*$. Due to algorithms that are called *index calculus methods* the prime power *q* has to be chosen large to keep schemes like the above example secure. These algorithms split the instance of the DLP into a lot of small and easy solvable instances of the DLP. These solutions are then combined to a solution of the original DLP by using linear algebra. Due to this development, a search for suitable groups that have a chance to be resistant to attacks of this type is an active area of research.

Elliptic Curves

We now want to turn to more sophisticated ways of encryption. For this we introduce a geometric object called *elliptic curve*.

Definition *Let K be a field with $1+1 \neq 0$ and $A, B \in K$ such that $4A^3 + 27B^2 \neq 0$. Then the set*

$$E(K) := \left\{(x,y) \in K^2 | y^2 = x^3 + Ax + B\right\} \cup \{\emptyset\}$$

*is called **elliptic curve** over K.*

We want to remark some things about the definition. First, the condition $4A^3 + 27B^2 \neq 0$ means that the polynomial $X^3 + AX + B \in K[X]$ has no multiple roots. This fact implies that every point has a unique tangent line attached to it. The element $\mathcal{O}$ is called the *point at infinity* which is needed to make $E(K)$ a group, as we see later. To be more precise, we need to say $E(K)$ is the set of K-rational points on the elliptic curve E.

Theorem [4] *Let K be a field and $E(K)$ an elliptic curve. Then $E(K)$ is an abelian group with neutral element $\mathcal{O}$ and three points $P, Q, R \in E(K)$ sum up to $\mathcal{O}$ if they lie on a straight line.*

We have already seen that we can consider the DLP in any group. In the case that $K = \mathbb{F}_q$ is a finite field, the DLP in $E(\mathbb{F}_q)$ for a suitable chosen E is assumed to be a hard problem [3]. This makes elliptic curves over finite fields suitable for cryptography. Actually, they are used for the encryption of the data on the German ID card.

Conclusion

The existence of modern cryptographic schemes makes it possible to handle sensitive data in a more and more connected world. It secures our privacy and our possibility to keep our secrets. We differentiate between symmetric and asymmetric schemes. A lot of these modern schemes are available for free in the web and can be used for example to encrypt your private emails, for instance using PGP, http://www.pgpi.org •

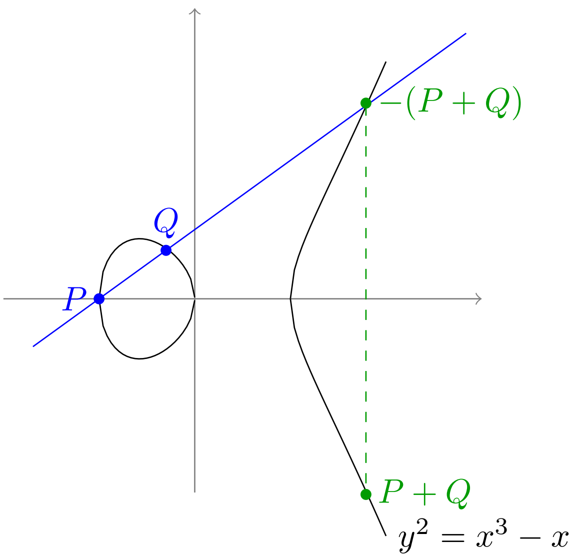


FIGURE 1 The group law on an elliptic curve over the field $\mathbb{R}$.

References

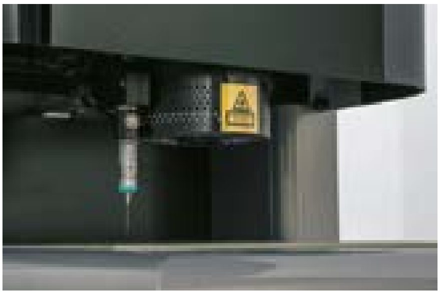
[1] Neal Koblitz and Alfred J. Menezes. A survey of public-key cryptosystems. In SIAM Review 46 (2004) 599– 634. OVERVIEW OF BRAID GROUP CRYPTOGRAPHY 13, 2004.

[2] H.W. Lenstra. Rijndael for algebraists, 2002. URL http://www.math. berkeley.edu/~hwl/papers/rijndael0.pdf.

[3] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM, 21(2):120–126, February 1978. ISSN 0001-0782.

[4] Joseph H. Silverman. The arithmetic of elliptic curves, volume 106 of Graduate Texts in Mathematics. Springer, Dordrecht, second edition, 2009.




Schut Geometrische Meettechniek is een internationale organisatie met vijf vestigingen in Europa en de hoofdvestiging in Groningen. Het bedrijf is ISO 9001 gecertificeerd en gespecialiseerd in de ontwikkeling, productie, verkoop en service van precisie meetinstrumenten en -systemen.

Aangezien we onze activiteiten uitbreiden, zijn we continu op zoek naar enthousiaste medewerkers om ons team te versterken. Als jij wilt werken in een bedrijf dat mensen met ideeën en initiatief waardeert, dan is Schut Geometrische Meettechniek de plaats. De bedrijfsstructuur is overzichtelijk en de sfeer is informeel met een “no nonsense” karakter.

Op onze afdelingen voor de technische verkoop, software support en ontwikkeling van onze 3D meetmachines werken mensen met een academische achtergrond. Hierbij gaat het om functies zoals ***Sales Engineer***, ***Software Support Engineer***, ***Software Developer (C++)***, ***Electronics Developer*** en ***Mechanical Engineer***.

Je bent bij ons van harte welkom voor een oriënterend gesprek of een open sollicitatiegesprek of overleg over de mogelijkheden van een **stage-** of **afstudeerproject**. Wij raken graag in contact met gemotiveerde en talentvolle studenten.

Voor meer informatie kijk op www.Schut.com en Vacatures.Schut.com, of stuur een e-mail naar Sollicitatie@Schut.com.

APPROVE for DeMeet