2018 Study trip in Ottawa, Mathematics in English[1]

Kazuo AKIYAMA
Shigehisa YANAGITA

<Summary>

This was the 4th Canada study trip. Most of the schedule was the same as in the previous. The difference is that Professor Mingarelli turned into Professor Ingalls for sabbatical leave. This time it was up to 34 students, the number of participating students has increased. It is my responsibility that the time involved in the 10 problems this time is roughly 2 months and I could not give students enough time. Despite lacking enough time, the students bravely tried to answer the given problems. There is no major change in the trip itself. However, this trip itself has been the subject of evaluation as part of the class from this time. This class is one of the liberal arts courses.

<Dr.Colin INGALLS>

https://carleton.ca/math/people/colin-ingalls/

Research Interests:
Non-commutative Algebra, Algebraic Geometry

He gave us one hour lecture. The title is “Magic Trick”. The topic was about Hamming coding theory. It was very interesting talk and some quiz which was given. After that we presented the solutions of his 10 problems which were given in advance. Many of the problems were difficult for high school students, and it took a great deal of work just to understand. Furthermore, the tense feelings over what to explain in English overlapped, and the students became nervous, but professor's gentle advice was given, and it was a sufficiently effective presentation.

[1] This study trip in Ottawa which is certified class as SSH(Super Science HighSchool)programme and supported by SSH grant 平成 30 年度採択# 30-3011.

<10 problems, solution, presentation and students' impression>

Dear Mr. Akiyama,

I wanted to mention that I have booked the MacPhail Room HP 4351 from 10:00 to 12:00 on October 24.

See you then,

Colin Ingalls

On Thu, 27 Sep 2018 at 11:39, Colin Ingalls <colin.ingalls@gmail.com> wrote:

Dear Mr. Kazuo,

I talked with Angelo about giving your class some problems to work on.? I realise they will not have so much time to work on these, but I've attached a list of problems.

They could present solutions to these problems as they did last year.? If you prefer I could give a talk instead.? If you prefer a talk I could suggest several possible topics.

I'm looking forward to meet you at 10:00 am on October 24.

Colin Ingalls

10 Problems from Dr. Colin INGALLS

1. You know there are solutions to the equation $x^2+y^2=z^2$ where x, y, z are integers and $xyz \neq 0$. Can you describe all the solutions ?

2. Fermat's Last Theorem says there are no solutions to $x^n+y^n=z^n$ where x, y, z, n are integers and $n \geqq 3$ and $xyz \neq 0$. This was stated by Fermat in 1637. It was proved by Andrew Wiles 1994. Can you describe some of the history and some overview of the proof ?

3. Can you derive Kepler's laws from Newton's Law of Universal Gravitation.

4. Explain time dilation as a consequence of Einstein's theory.

5. What is the biggest known prime number? What can you say about how it was found ?

6. Describe the RSA cryptosystem.

7. Elliptic curves are also used in cryptography. What are they ?

8. What is the abc conjecture? What is known about it ?

9. You know the quadratic equation. What is the cubic equation ?
   The quartic equation? Is there a quintic equation?

10. What are comlex numbers? What is the Fundamental Theorem of Algebra ?

氏　　名	student name	problem#
青木　優憲	Masakazu AOKI	1
小川　瑞貴	Mizuki OGAWA	
毛塚　大貴	Daiki KEZUKA	
堀越誠一郎	Seiichiro HORIKOSHI	
原澤　　光	Hikaru HARASAWA	
後藤　綾佑	Ryousuke GOTO	5
松村　　悠	Yu MATSUMURA	
山田　崇暉	Takaki YAMADA	
桝田　悠吏	Yuri MASUDA	
三宅　　岳	Gaku MIYAKE	
齋藤　　楓	Kaede SAITO	6
清水　悠斗	Yuto SHIMIZU	
杉山　怜央	Reo SUGIYAMA	
村田　英心	Eishin MURATA	
東郷　秀哉	Syuya TOGO	7
真貝　友彬	Tomoaki SHINGAI	
滝沢　　渉	Wataru TAKIZAWA	
津島　一輝	Kazuki TSUSHIMA	
西田　　龍	Ryu NISHIDA	
細貝　優人	Yuto HOSOKAI	
大野　裕衣	Yui ONO	8
片田詩映奈	Shiena KATADA	
野村　萌生	Moe NOMURA	
矢﨑　　楓	Kaede YAZAKI	
野原　　葵	Aoi NOHARA	9
土井川早季	Saki DOIGAWA	
友野　菜那	Nana TOMONO	
髙橋美優香	Miyuka TAKAHASHI	
亀田　優夏	Yuka KAMEDA	10
菅沼茉莉花	Marika SUGANUMA	
大森　優那	Yuna OHMORI	
吉田　瑠那	Runa YOSHIDA	
井上　美優	Miyu INOUE	
藤田　果子	Kako FUJITA	

<Problem#1: Pythagorean Theorem>

Daiki KEZUKA, Hikaru HARASAWA
Masakazu AOKI, Seiichiro HORIKOSHI, Mizuki OGAWA

Question

You know there are solutions to the equation $x^2+y^2=z^2$ where x, y, z are integers and $xyz \neq 0$. Can you describe all the solutions?

Solution

We can solve this question by proving $x^2+y^2=z^2$ shows $(m^2-n^2)^2+(2mn)^2=(m^2+n^2)^2$ by expression of Diophantos. m and n are integers.

(i) We think when x and y are both even numbers. We can express them with natural numbers x_0 and y_0. In addition , we let d be the common factor of x and y. We can show $\begin{cases} x = x_0 d \\ y = y_0 d \end{cases}$ at this time.

$$\begin{aligned} z^2 &= x^2+y^2 \\ &= (x_0^2+y_0^2)d^2 \end{aligned}$$

We find *Z* is multiple of *d*. x and y don't have a common factor and the y don't become even numbers. That's because it contradicts the assumption that it doesn't have a common factor.

(ii) When x and y are both odd numbers, We can express them with natural number x_0 and y_0 :

$$\begin{cases} x = 2x_0+1 \\ y = 2y_0+1 \end{cases} \cdots ①$$

At this time,

$$
\begin{aligned}
z^2 &= x^2 + y^2 \\
&= (2x_0 + 1)^2 + (2y_0 + 1)^2 \\
&= 4{x_0}^2 + 4x_0 + 1 + 4{y_0}^2 + 4y_0 + 1 \\
&= 4({x_0}^2 + x_0 + y^2 + y_0) + 2
\end{aligned}
$$

Then, we know z is even number, and z^2 by 4 leaves 2. But when even number is squared, the number becomes multiple of 4, so ① contradicts to this.

In conclusion, x and y are not both odd numbers.

From (i) and (ii), one side is odd number and the other side is even number.

(iii) Assuming that y is even number.

$$x^2 + y^2 = z^2$$

$$y^2 = z^2 - x^2$$

$$\left(\frac{y}{2}\right)^2 = \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right)$$

square of x plus square of y equal square of z. So square of y equal square of z minus square of x, calculating this result in square of y half equal $\left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right)$. Following $\left(\frac{z+x}{2}\right)$ and $\left(\frac{z-x}{2}\right)$ don't have common factor. If there is common factor of them. We can set

$$\frac{x+z}{2} = kp$$

$$\frac{z-x}{2} = kq$$

Number k is there common factor. Calculating this result in

$$x = 2qk$$
$$y = 2k\sqrt{pq}$$
$$z = k(p+q)$$

But then x, y, z has common factor k. There are contradiction the assumption.

(iv)
$\frac{z+x}{2}$ and $\frac{z-x}{2}$ are showed by disjoint the natural numbers squared. Let $\frac{z+x}{2}$ and $\frac{z-x}{2}$ are m^2 and n^2 are relatively prime

$$x = \frac{z+x}{2} - \frac{z-x}{2} = \overline{m^2} - n^{\overline{2}}$$

$$\left(\frac{y}{2}\right)^{\overline{2}} = \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right), \quad \frac{y}{4} = \overline{m^2}\,n^{\overline{2}}, \quad y^{\overline{2}} = 4\,\overline{m^2}\,n^{\overline{2}}, \quad y = 2\,\overline{mn}^{\overline{2}}$$

$$z = \frac{z+x}{2} + \frac{z-x}{2} = \overline{m^2} + n^{\overline{2}}$$

Lastly, substitute $x = \overline{m^2} - n^{\overline{2}},\ y = 2\,\overline{mn},\ z = \overline{m^2} + n^{\overline{2}}$ for $x^2+y^2=z^2$.
We can prove the equation of Diophantine.

conclusion

Expression of Diophantus is consisted disjoint nature number in m and n. There are a lot of x, y, and z solution or value, not so counted. Also, this question is "Can you describe all solutions of x, y and z when these are intengers and xyz not equal 0."

Therefore,describing all the solutions are impossible!
There are our group's idea at Question1.

But we can only use this expression when m and n are both disjoint numbers, For example, $(6,8,10)$

$$6^{\overline{2}} + 8^{\overline{2}} = 10^{\overline{2}}$$

$$(2\times 3)^{\overline{2}} + (2\times 4)^{\overline{2}} = (2\times 5)^{\overline{2}}$$

$$2^{\overline{2}}(3^{\overline{2}} + 4^{\overline{2}}) = 2^{\overline{2}} \times 5^{\overline{2}}$$

At this point, we can find $3^{\overline{2}} + 4 = 5^{\overline{2}}$, expression applies the expression of Diophantus. We can replace ① by character.
(a is common factor)

$$a^2\{(m^2-n^2)+(2mn)^2\}=a^2(m^2+n^2)^2$$

<Another Solution>

Here, we describe another solution. The Flexibility of this solution is worse than the Main solution, but we can describe this with graph of function.

$$\begin{cases} x^2+y^2=1 & \cdots ① \\ y=mx+m & \cdots ② \end{cases}$$

Substitute ② for ①

$$x^2+(mx+m)^2=1$$

$$(1+m^2)x^2+2m^2x+m^2-1=0$$

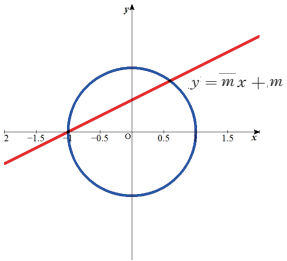
$$x=\frac{-m^2+1}{1+m^2}\ ,\ y=\frac{2m}{1+m}$$

An intersection point is $(-1, 0)$ and $\left(\frac{-m^2+1}{1+m^2}, \frac{2m}{1+m^2}\right)$

Substitute this for ①

$$\left(\frac{-m^2+1}{1+m^2}\right)+\left(\frac{2m}{1+m^2}\right)=1$$

$$(1-m^2)+(2m)^2=(1+m^2)^2$$



<Impression>

This problem was very difficult but it was fun to solve it. The reasons are follows. First, I had to prove more than one to derive the mathematical expression that answered. It was difficult to think about case division and it was hard to derive the formula that was the source of the answer. However when I was able to derive the formula using case classification, I felt the best. Second, generalizing all numbers that apply to Pythagorean's theorem is extremely difficult. Although I was not good at calculating using characters, I thought very hard but I was able to solve it in cooperation with members of the group. So, this problem has increased my knowledge of mathematics. I also learned many specialized words on mathematics. I believe this experience will surely be useful in the future.

— D. KEZUKA

This trip has made me very active in Canada and Japan. I don't like mathematics very much, but I studied many things through all experiences. For example, the difficulty of
using English. If I don't speak English, everyone cannot understand me, so I had to manage to communicate with them. The classes in university is good example. From experiences in Canada, studying mathematics showed me the importance of mental strength and I have studied the ways for communication. I will never forget this trip.

— H. HARASAWA

This trip of Canada was the first overseas travel for me, and I was able to gain many valuable experiences. I could feel local culture and was very glad because I wanted to go to there. For example, cityscape of Montreal, a French signboard, and so on. In addition, in the Carlton University, we received an interesting lecture in a simple game form. It was very scared for me who have poor to go to abroad. But a sense of fear disappeared through a trip. I regard this experience as important and want to be connect to the future from now on.

— M. AOKI

I have never been to abroad before I went to Canaba Travel. So, I was very impressed by real foreign buildings, foods, people and so on. I was not goot at English. Even thought I was talking to by the local people I could not respond. However, I noticed something when I learned math in English from Dr.Colin Ingalls at Carleton University. That is to tell my opponent my intentions that I can do without saying accurate sentences. Example is simple words and gestures. Then I tried hard to speak English from myself when buying a souvenir, etc. I was glad when my intention was told to my opponent. I learded amusement of talking English and I got precious experience from Canada Travel.

— M.OGAWA

"A swing to look, and not to watch" strides in Japan. When I walk, I say nothing even if I find a troubled person. There may be the person grinding a voice cliff to a tourist, but after all does not avoid the impression called a strange person.

It is that there were a lot of people such as the embodiment of friend Lee we go to Canada, and to have felt. I talked with three Canadian people even if I watched only a thing in the trasport cafe of the expressway. Though this talked in broken English, the partner talked with a smile. I realized that it was very warm people. A Japanese has a Japanese rule, and there is the tacit consent. However, you may follow such a warm will.

— S.HORIKOSHI

<Problem#5: The Biggest Prime Number>

Ryousuke GOTO, Takaki YAMADA,
Gaku MIYAKE, Yuri MASUDA, Yu MATSUMURA

<Summary>

Why do we learn math in English. Many people think like this after hearing. Math is very important to improve our technology in the future. To tell our new idea to the world, English is also important. So we have to learn both of them (math and English).
However, it is impossible for high school students to do such a thing (transmit our new idea to the world). By the way, we could make first step in this project. In this project, we had 10 problems from university professor. And our group chose a problem which was “Find a largest prime number.” However, this problem have not solved yet. So we found good processes and ways to find largest prime number in this problem.

Question
What is the biggest known prime number ? What can you say about how it was found ?

Solution
Sieve of Eratosthenes.

Use “Sieve of Eratosthenes.” This way is to find prime number.

First, write the numbers.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
26 27 28 29 30.....

Second, we erase 1 and the multiple numbers of 2 (other than 2).
After that, we erase multiple numbers of 3, 4, 5, and so on.

And we do this work many times.
By using these ways, we can find prime number. But there were a lot of prime number, so we cannot find all of them by ourselves.

Second we introduce “Mersenne primes.”

What is the “Mersenne primes” ?

“Mersenne numbers” are natural numbers which can be expressed 2^n-1. In Mersenne numbers, the numbers with prime numbers are called Mersenne primes.
For example, $2^2-1=3$, $2^3-1=7$, $2^4-1=15$ …
These are Mersenne primes.

To image the size of Mersenne number, it is a good idea to calculate 2^n. Put the numbers (1.2.3.4.5.6…) to n, 2^n will be 2 4 6 8 16 32 64 …. And 2^{10} =1024.
When n is 20, 2^n will be 1048576.
It is very big number, and 2^n will increase with amazing speed.

Binary notation.

A binary number is the number of the world where only 0 and 1 exist. Generally, decimal number is used a lot. However, binary number is used a lot in the computer world.
Binary notation’s order is ..... 2^4 ,2^3 ,2^2 ,2^1 ,2^0 .

For example, 13= 1101, 17= 10001.

In binary notation, we count the numbers from the place below.
Mersenne numbers will be 1111111.... in binary notation. All places will be 1.

The history of prime number.

1600 B.C., prime numbers are known partially. Because of Egyptian fraction. This way uses different type of calculate (use prime numbers and composite numbers). Ancient Greeks are the first to study prime numbers clearly.
For example, 300B.C., Euclid said “Prime numbers are infinite.” And also, he made perfect number from Mersenne prime.
Erathosthenes also find “Sieve of Erathosthenes.” This method is enumerate the prime numbers.
After ancient Egypt era, there was no progress. But recently, prime numbers discovery move on gradually.

The largest prime number and Lucas Romer test.

In 2018, 51th Mersenne prime was found.
The largest prime number is $2^{82,589,933} - 1$. It has 24,862,048 digits. We can’t find largest prime number by ourselves. So we need to use computer. There are many prime number determination methods.

For example, Lucas Romer test.
This method was found by Lucas and Romer.

First, we make Lucas Romer sequence. And start from 4.

$$4 \rightarrow 4\times4-2=14 \rightarrow 14\times14-2=194 \rightarrow 194\times194-2=37634.$$

Second, write this n item as $S(n)$, for odd prime p, $2^n - 1$ is a prime only when $2^n - 1$ divides $S(n-1)$.

For example, n = 5 = 31 → S (4) = 37634.

$$37634 \div 31 = 1214, \text{ It will be divisible.}$$

This is Lucas Romer test.

Perfect number.

Perfect number is big relationship with Mersenne prime. When the total number of divisors excluding itself is itself. Such numbers are called perfect number.
The least perfect number is 6. The divisor of 6 are 1, 2, 3, 6.

According to the rules, $1+2+3=6$.

Second least perfect number is 28, and third is 496.

Why does Mersenne prime relate to perfect number ?

Factorize 6, 28 and 496.

These numbers will be $6=2\times 3$, $28=2^2\times 7$, $496=2^4\times 31$.

These are in the form of "power of 2 × Mersenne prime." This method can use only even number. Because odd number perfect numbers haven't been discovered yet. So all perfect numbers found so far relate to Mersenne primes.

<Conclusion>

Over time, discovery of the largest prime number has been carried out all over the world. And it is impossible for human to find such a number. So we have to depend on computer to find the largest prime number.
Discovery of the largest prime number hasn't finished yet. In the future, we would like to expand our knowledge to be involved in this research.

<Impression>

Through this Canadian expedition, I felt that mathematics is a universal language. Also, I thought that learning mathematics in English is a very global approach and necessary for society in the future.

— Y. MASUDA

I have traveled to Canada to study mathematics in English this time. It was not enough at all with my own knowledge of mathematics and I could prove the problem by deeply understanding various theorems.

— Y. MATSUMURA

I was able to feel the interestingness of mathematics on this research trip. Because I became able to think about mathematics from the view point I had never had before. Actually, although I felt the difficulty of solving mathematics problems in English. It could be one of my good experience. This time I learned at Carleton University in Canada is only a small part of mathematics, so I wanted to learn more.

— R. GOTO

I went to Canada on a research trip this time. When I studied math in English at Carleton University, I could understand what university professor was saying. Because I knew the letters and laws of mathematics although I don't understand English.
I thought that little knowledge of mathematics was needed until now. However, I found that mathematics can also be language.

— G. MIYAKE

First, I didn't think that studying math in English was very difficult. However, I could grow my math and English ability. In Canada, Carleton university professor's class was so fascinating that I was interested in math more than before. And I also realized that my abilities of math and English are insufficient.So I thought I wanted to improve my math and English ability for the future.

— T. YAMADA

<Problem#6: RSA cryptosystem>

Eisin MURATA, Yuto SHIMIZU, Kaede SAITO, Reo SUGIYAMA

Qustion

Describe the RSA cryptosystem.

Solution

1) What is RSA?

RSA is one of the public key cryptosystems.

The public key cryptosystem is cryptosystem that use public key and private key (pair of public key) in encryption and in decryption.

It uses the difficulty of prime factorization problem of composite numbers with large numbers of digits. This was found more than 40 years ago, but the formula has not been discovered yet.

2) RSA history

People have used shared key encryption for a long time. It is used same key when encrypting and conjugating. For example, there are those with numbers plus 20. But they needed to share keys so that they could not get out to others. It is hard work.

One day in 1976, Whitfield Diffie and Martin Hellman present the public-private key cryptosystem. It is to use different key when encrypting and conjugating. However, many mathematicians tried to make cryptogram, nobody could make it.

In 1977, three people, Ron Rivest, Adi Shamir and Leonard Adlemon, succeeded make cryptogram. They named it RSA. The name comes from the first letter of their initials. RSA is first public key cryptosystems.

In 2000, Patent expires of RSA expire, everyone can use it. Now RSA is one of the most safely cryptogram and it is used many things in the world.

Ron Rivest

Adi Shamir

Leonard Adlemon

3) How to use RSA

(1) Put p, q (p, q are prime numbers) put $pq = \mathrm{N}$

Find $(p-1)(q-1)$ $\quad((p-1)(q-1) = \varphi(\mathrm{N}))$

(2) Make the public key.

Let the key be k_1 (k_1 and $(p-1)(q-1)$ are coprime.)

k_1 and N are public key.

(3) Make the secret key.

Let the key be k_2

Find the key by $k_1 k_2 \equiv 1 \bmod (p-1)(q-1)$

k_2 is secret key.

(4) Make the code by using public key

Let the message be $\mathrm{M}\ (0 \leqq \mathrm{M} < \mathrm{N})$

Find $\mathrm{M}^{k_1} \bmod \mathrm{N}$

Let $\mathrm{M}^{k_1} \equiv \mathrm{C} \bmod \mathrm{N}$

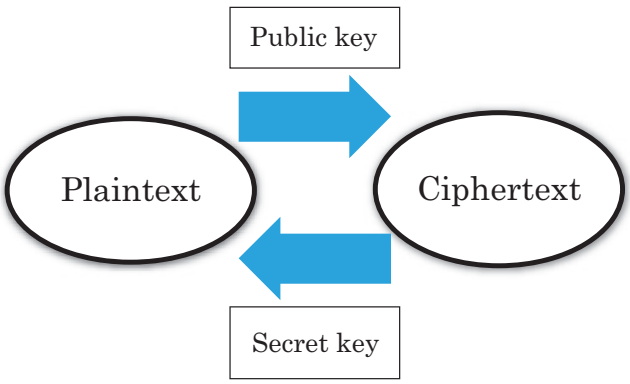
C is the code.

(5) Find the message from C

Solve $\mathrm{C}^{k_2} \bmod \mathrm{N}$

Its answer is the message M

*(1), (2), (3), (5) for Receiver, (4) for Sender



(Example1)

$p=7, q=11$ so, $N=77$ $(p-1)(q-1)=60$

$k_1=7, N=77$ are public key $k_2=43$ is secret key

$M=38$

$38^7 \equiv 3 \mod 77$ $C=3$

$34^3 \equiv 38 \mod 77$

(Example2)

Let the word "RSA" be 12663

Set $p=211, 1=199$ so, $N=41989$ $(p-1)(q-1)=41580$

$k_1=13$ $N=41989$ are public key

$13k_2 \equiv 1 \bmod (p-1)(q-1)$

$k_2=6397$ is secret key

$M=12663$

$12663^{13} \equiv C \bmod 41989$ $C=28492$

$28492^{6397} \equiv 12663 \mod 41989$

Why can it been conjugated

Proof) Prove $(M^{k_1})^{k_2} \equiv M \pmod N$ $N=pq$

First, prove $(M^{k_1})^{k_2} \equiv M \pmod p$

(1) If M is multiple of p, both sides are multiple of p. So, it is OK.

(2) If M is not multiple of p

Because k_1k_2-1 is multiple of $(p-1)$, we use an integer " a ", put $k_1k_2=1+(p-1)a$

$(M^{k_1})^{k_2} \equiv M^{k_1k_2} \equiv M^{\{1+(p-1)a\}} \equiv M \cdot M^{(p-1)a} \equiv M \cdot 1^a = M$

↑

Use the Fermat's little theorem

So $(M^{k_1})^{k_2} \equiv M \pmod p$

Second, prove $(M^{k_1})^{k_2} \equiv M \pmod q$ in the same way as above.

(1) If M is multiple of q, both sides are multiple of q. So, it is OK.

(2) If M is not multiple of q

Because k_1k_2-1 is multiple of $(q-1)$, we use an integer " a ", put $k_1k_2=1+(q-1)a$.

$$(\mathrm{M}^{k_1})^{k_2}\equiv \mathrm{M}^{k_1k_2}\equiv \mathrm{M}^{\{1+(q-1)a\}}\equiv \mathrm{M}\cdot(\mathrm{M}^{(q-1)a})\equiv \mathrm{M}\cdot 1^a=\mathrm{M}$$

So $(\mathrm{M}^{k_1})^{k_2}\equiv \mathrm{M} \pmod{p}$

$$\therefore\ (\mathrm{M}^{k_1})^{k_2}\equiv \mathrm{M} \pmod{\mathrm{N}}$$

※ Fermat's little theorem

Put p is natural number, a is any integer.

$a^p\equiv a \pmod{p}$

Especially, a are coprime

$a^{p-1}\equiv 1 \pmod{p}$

4) Why is the RSA cryptogram safe?

The safety of the RSA cryptogram is based on difficulty of the factorization in prime numbers.

In fact, it is said that the factorization in prime numbers over one hundred digit require astronomical time even if we use computer.

※Polynomial time and Exponential time

Polynomial time… It doesn't spend time on calculation processing even if "N" grow big number.

For example: N^5

Also the problem which can be solved in it is P problem.

Exponential time…Time of calculation processing increase exponentially it "N" grow big number.

For example: 5^N

Also the problem which can be solved in it is P problem.

The problem which can be found out whether answer is correct by polynomial time is NP problem. But polynomial time algorithm to solve NP problem such as factorization in prime number have not been discovered yet.

In this way, it is very difficult to solve prime factorization of number with a large number of digits. RSA encryption is a security technique that uses it. But, more than 700 bits of prime factorization was succeeded by computer. These days, computer technology has been rapidly advancing. So, there is possibility that RSA encryption will be solved in the future.

5) RSA is in danger.

General computers use bits. Bits use two patterns “0” and ”1”. “0” is a statue where electric current doesn’t flow. “1” is a statue where electric current flow. It moves to control “0” and “1”.

Quantum computers use quantum bits. Quantum bits can be two patterns at the same time. So, quantum computer can calculate move and faster than general computers. Also, to decryption RSA only use prime factorization. If we use quantum computer, the possibility that find two prime numbers is increase. So it is danger to use RSA forever.

<Impression>

To use RSA is difficult for me. But RSA is used many ways. I think it is good experience to study about RSA. When I want to tell only on person, I want to use it. — Y. SHIMIZU

I am not good at English and Math. At first I could not understand RSA. But, I was able to gradually understand it while I was investigating. This is my first visit to Canada. We went various places. I was able to feel the difference with Japan. So, it is a good experience for me to go to Canada. I want to go again in the future. — R. SUGIYAMA

It was the first time that I visited Canada.

A lot of things are different from Japan. I was very surprised. There are few vending machines in Canada. Compare Japan with Canada I found good points and bad points of Japan. I really learned a lot. This study trip directly influenced my life.

I changed thinking a little. I would like to visit there again. — K. SAITO

This trip for Canada is the second trip of my life. Though Canada was very cold, I didn’t bring coat or jacket, glove. So, it is hard for me to go out. Meanwhile, I felt the difference of climate from Japan. In addition, I found several differences in hotel, university, town. Also, I have studied RSA with other students since I was in Japan. The problem is very difficult. So, making the solution by cooperating with others was worthwhile job. Thus I could learn not only math but also differ culture. This experience became my important memory. If the opportunity arises, I want to go to Canada or other countries. — E. MURATA

<Problem#7: Elliptic Curves and Cryptography>

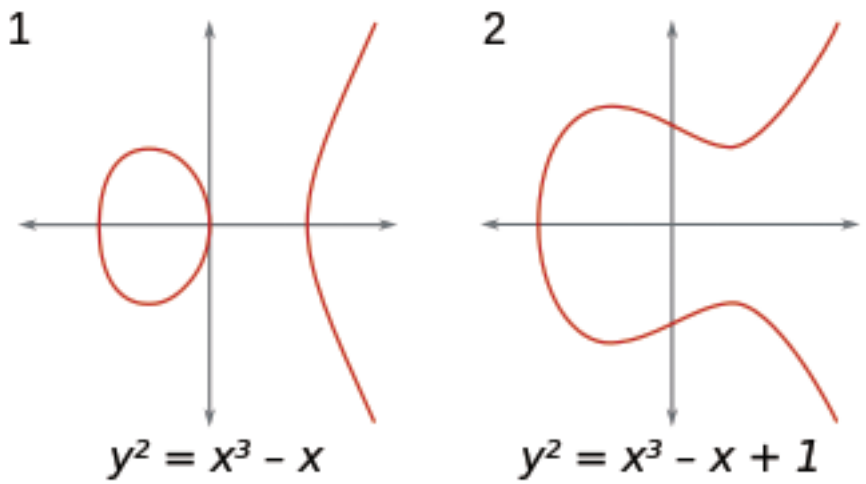
Ryu NISHIDA, Tomoaki SHINGAI, Kazuki TSUSHIMA
Syuya TOGO, Wataru TAKIZAWA, Yuto HOSOKAI

Question

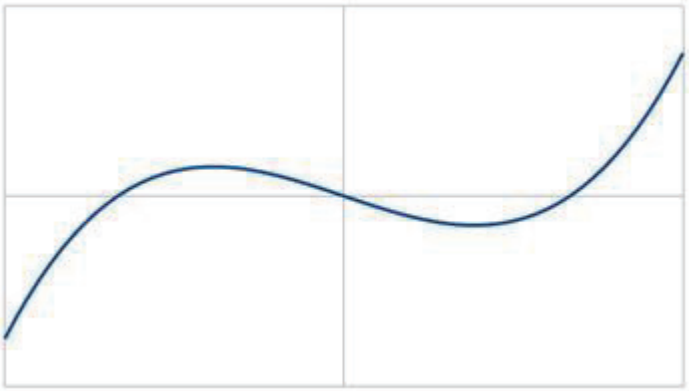
Elliptic curves are also used in cryptography. What are they?

Solution

We are going to answer the question. “Elliptic curves are also used in cryptography. What are they?” Elliptic curve is a plane algebraic curve defined by an equation of the form “ $y^2=x^3+ax+b$ ” (a and b are constant). The curve is like under graph. If (x, y) is complex number, the space looks like a doughnut. In cryptography, the equation is used this form, “ $y^2=x^3+ax+b$ modification p ”

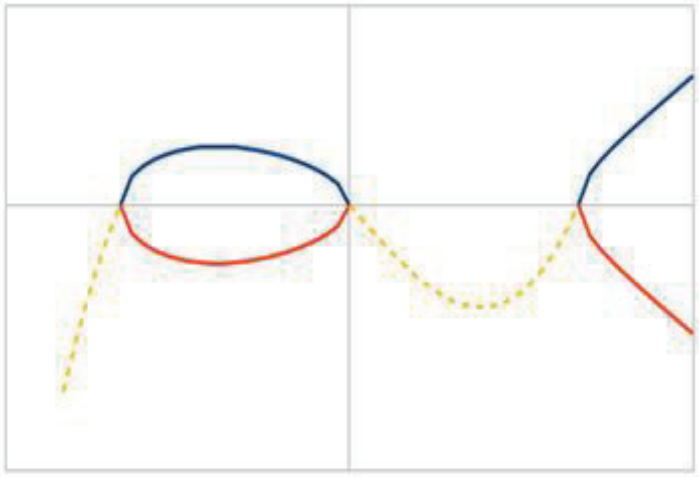


We will explain the elliptic curve.



$$y = x^3 + ax + b$$

When looking at the right side, it is a figure of a cubic equation so it will be as shown above.



$$y^2 = x^3 + ax + b$$

As we see y^2 on the left side, the negative part of the cubic expression is cut off.

If you look at the right side once again, since x is the third power, there is a possibility of minus in the graph of the form defined earlier. Therefore, we can create a symmetric graph on the x-axis.

It is because there are such complicated solution that are used as encryption technology.

Addition of Points

For elliptic curves, the operation $\mathrm{P}+\mathrm{Q}=\mathrm{R}$ can be carried out by drawing a chord through P and Q. This chord intersects the elliptic curve at a third point. This point is $-\mathrm{R}$. R is found out by reflecting $-\mathrm{R}$ in the x axis. (see Figure1)

The operation is denoted by

$$\mathrm{P}+\mathrm{Q}=\mathrm{R} \quad \text{or}$$

$$\begin{pmatrix} x_p \\ y_p \end{pmatrix} + \begin{pmatrix} x_q \\ y_q \end{pmatrix} = \begin{pmatrix} x_r \\ y_r \end{pmatrix}$$

$$\lambda = \frac{y_q - y_p}{x_q - x_p}$$

$$x_r = \lambda^2 - x_p - x_q$$

$$y_r = (x_p - x_r)\lambda - y_p$$

It can easily be seen that this operation is commutative, associative and distributive.

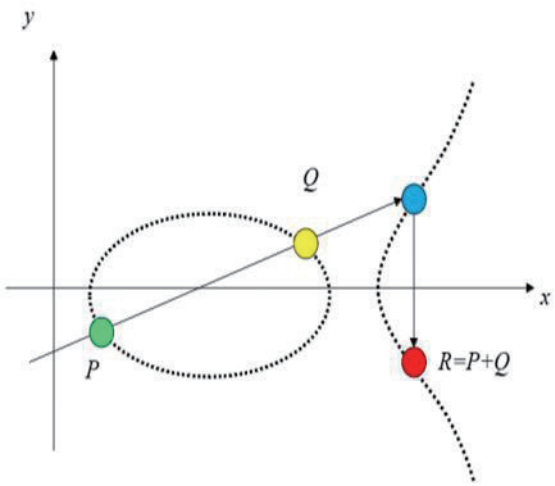


Figure 1

Discrete logarithm problem

Example)

We define $a = 2, n = 5, p = 11$ and $b = a^n \mod p$
This answer is $b = 32 \equiv 10 \mod 11$.

Discrete logarithm problem is a problem of finding n from a and b only. We can not know by just seeing how much it will be 10 if you multiply n .

$$2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 = 32$$

there is only a way to research one by one.
This example question is easy. But, if n gets bigger it will not be easy to answer with computer.

Elliptic Curve Discrete logarithm problem

I will do the same as above.

Example)

In the elliptic curve E, there are a point P and an integer D on E .

It is easy to calculate $\mathrm{Q} = d \times \mathrm{P}$.
Conversely From point P and point Q, it is difficult to find d satisfying $\mathrm{Q} = d \times \mathrm{P}$. This is called an elliptic discrete logarithm problem.

This problem is used for encryption because it can make it difficult to solve using a computer.

How and why the elliptic curve is used in bitcoin

As you know the elliptic curve is being used in the cryptography fields, and one famous example of these is Bitcoin. It uses the technology in order to generate addresses which are used to receive

funds, identify where to send them and computed from private keys. In addition, as the private keys are used when spending funds, they are required to be kept secret, but we do also have to connect the addresses to the private keys to allow their holders to control over their assets as well. Since the elliptic curve is a thing which can easily get values from given values but the difficulty to compute given values from gotten values is unbelievably high, in other words, the process is impossible, the elliptic curve is the proper solution.

Let's generate a bitcoin address

I'll use python in order to do this.

```
#!/usr/bin/env python3
# coding: utf-8
import secrets
import ecdsa
import hashlib
import base58

class Generater():
    def __init__(self):
        p = 2**256-2**32-2**9-2**8-2**7-2**6-2**4-1
        privkey = self.new_privkey(p)
        pubkey = self.new_pubkey(privkey)
        address = self.new_address(bytes.fromhex("00"), pubkey)

    def new_privkey(self, p):
        privkey = secrets.randbelow(p)
        privkey = format(privkey, 'x')
        print("PrivateKey = " + privkey)
        return privkey

    def new_pubkey(self, privkey):
```

```
        bin_privkey = bytes.fromhex(privkey)
        signing_key = ecdsa.SigningKey.from_string(bin_privkey, curve = ecdsa.SECP256k1)
        verifying_key = signing_key.get_verifying_key()
        pubkey = bytes.fromhex("04") + verifying_key.to_string()
        pubkey = pubkey.hex()
        print("PublicKey = " + pubkey)
        return pubkey

    def new_address(self, version, pubkey):
        ba = bytes.fromhex(pubkey)
        digest = hashlib.sha256(ba).digest()
        new_digest = hashlib.new('ripemd160')
        new_digest.update(digest)
        pubkey_hash = new_digest.digest()

        pre_address = version + pubkey_hash
        address = hashlib.sha256(pre_address).digest()
        address = hashlib.sha256(address).digest()
        checksum = address[:4]
        address = pre_address + checksum
        address = base58.b58encode(address)
        address = address.decode()
        print("Address = " + address + "\n")
        return address

address = Generater()
```

Firstly,

```
p=2256−232−29−28−27−26−24−1
def new_privkey(self, p):
        privkey = secrets.randbelow(p)
```

```
        privkey = format(privkey, 'x')
        print("PrivateKey = " + privkey)
        return privkey
```

We do get a random private key which is smaller than p with new_privkey function.

Secondly,

```
 def new_pubkey(self, privkey):
        bin_privkey = bytes.fromhex(privkey)
        signing_key = ecdsa.SigningKey.from_string(bin_privkey, curve = ecdsa.SECP256k1)
        verifying_key = signing_key.get_verifying_key()
        pubkey = bytes.fromhex("04") + verifying_key.to_string()
        pubkey = pubkey.hex()
        print("PublicKey = " + pubkey)
        return pubkey
```

We obtain a public key from the private key by computing with the elliptic curve.

Thirdly,

```
 def new_address(self, version, pubkey):
        ba = bytes.fromhex(pubkey)
        digest = hashlib.sha256(ba).digest()
        new_digest = hashlib.new('ripemd160')
        new_digest.update(digest)
        pubkey_hash = new_digest.digest()

        pre_address = version + pubkey_hash
        address = hashlib.sha256(pre_address).digest()
        address = hashlib.sha256(address).digest()
```

```
    checksum = address[:4]
    address = pre_address + checksum
    address = base58.b58encode(address)
    address = address.decode()
    print("Address = " + address + "\n")
    return address
```

We need to create checksum when generating an address, and it requires the public key's hash.
so get the hash first.

pubkeyhash=ripemd160(sha256((pubkey)))
And the checksum's material is
address=sha256(sha256(payload))
However the real checksum is before 4 bytes from the variable `address` so
checksum=address[:4]
The resoponse should be
PrivateKey = c31ad13427f28c429c443d6058129051614875ab5f576364e0e2866e3ab87aae
PublicKey = 048813b6143a1316041ff1fb4f3af6061a05f7803ef01e32cf3ff1a71422f95a6d600638c460a49f5c6125b11cbc5bdfff30c0545c6f208d9a1fa6ed504b2d2c29
Address = 176wVvyL4NzecB9nm7DmuQ3x5rfqXCo1n5

Resource

https://qiita.com/kaz1shuu2/items/921dcbebb7fbea14f085
I will do the same as above.
Example)
In the elliptic curve E , there are a point P and an integer D on E.
It is easy to calculate $\mathrm{Q}=d\times\mathrm{P}$.
Conversely From point $\mathrm{P}$and point Q, it is difficult to find d satisfying $\mathrm{Q}=d\times\mathrm{P}$. This is called an elliptic discrete logarithm problem.
This problem is used for encryption because it can make it difficult to solve using a computer.

<Impression>

I thought that I was good at mathematics. However, learning mathematics in English made me realize a new perspective and I realized that I am immature.
I faced the problem of university level and did not fully understand it but I think the time to understand the problem can be utilized in the future.

— W. TAKIZAWA

At first It is difficult for me to study mathematics in English. Howerver by cosulting a dictionary for the meaning of a word I was able to understand the formula. it is fun to solve the difficult problem in a team. We went to Canada and taught us. It was a good experience for me. I want to make this experience useful for my study in thefuture.

— T. SHINGAI

We solved difficult math problems that at university level. At first, I despaired too much difficulty.
So, I am relieved to finished. We solved these problems with cooperation and study. That made me enjoying and stimulation. And it was be a trigger to know our ability in mathematics is immature. I noticed need effort more and more through this project.
This was wonderful experiences. I want make use of this it in my future.

— K. TSUSHIMA

I went to Canada for 5 days from October 22nd. I have been overseas. But it was real for the first time as it was childhood. So I got a new stimulus.
The one I got impressed is Notre Dame Cathedral. This building was a big church I do not see much in Japan. It was fresh as we never touched Christianity. Mural paintings and statues were wonderful. I am practicing a song called "Notre Dame no Bell" in brass music now. That is one of the reasons left in the impression.
Mr. Collin got accurate advice on the elliptic curve. I want to make use of it and want to make the next announcement successful.

— Y. HOSOKAI

We have been to Canada in order to obtain some advice from a professor, Mr. Collin. I think this was really a good opportunity to get experienced what a university in Canada or abroad was like.
Personally, as I'm attempting to enter a university abroad, it was a great chance to examine myself whether I will be able to understand classes conducted in English.
During my stay in Canada, I was really surprised because its capital city, Ottawa was unbelievably small. It was like a village honestly. Since I live in Tokyo, Japanese capital city and obviously the biggest city in Japan, also I had only been to big capital cities in Europe, Eastern Asia, I had been believing that a capital city must have been the biggest city in its country. As a result, I could know what a capital city dedicated for governing its country was like as well.
Through this trip, I came to be eager to travel abroad and study abroad.

— R. NISHIDA

We'd been to Canada for 5 days to answer the question from Dr.Colin and visit some famous places in Canada. Actury, we answered the quesion in third day. In same day, we had his class about the plactical use of Binary. We learned Binary is used in infomation technorogy to collect some fault words in sentenses. this class was very interesting because it was not too difficult to understand and I found how to use mathmatic we learned in our high school in daily life. After that, we answered the question. I think I could tell him all we learned and we could do our best, and I could get a lot about Eliptic Curve. So this experiment was very presious and good for us. Making use of this experiment, we would make SSH Academic Recital.

— S. TOGO

<Problem#8: ABC Conjecture>

Moe NOMURA, Kaede YAZAKI, Shiena KATADA, Yui ONO

Question

What is the abc conjecture? What is known about it?

Solution

ABC conjecture was raised by Joseph Oesterlé and David Masser in 1985.

In August 2012 Shinich Mochizuki, who is professor of Kyoto university, published paper about ABC conjecture. He is Japanese, and he entered Phillips Exeter Academy when he was 16. The paper said that Mr. Mochizuki proved about ABC conjecture. By mean of this, ABC conjecture got more attention.

Next, we will explain contents of ABC conjecture.

『There are a pair of disjoint natural number (a,b,c), which fulfill the condition "a+b=c". On the contrary, the product of abc that "product of mutually different prime factors." is expressed "d". At this time, against the optional condition "ε>0", the pair of (a,b,c) which fulfill the condition" $c > d^{1+\varepsilon}$ " is existed at most finite number.』

This is content of ABC conjecture.

If it gone on like this, it is difficult to understand. So, we think this with concrete figures.

For example, we suppose a=9, and b=31.

a+b=9+31=40. So, c=40.

Let a, b, c solved into factors, and we multiply them one by one.

$9=3^2$

$31=31$

$40=2^3\times5$

When we multiply 3, 31, 2 and 5, it is 930. This is d, and c < d. It is very common, but sometimes, c is bigger than d.

To put "a=1, b=8".

a+b=1+8=9. So, c=9.

To prime factorization a, b, c and multiply the prime factor that came out one by one.

1=1
$8=2^3$
$9=3^2$

So, 1×2×3=6. This value is "d". Then, it become c > d.
When c < 100, the number of three sets, a, b, c(c > d) is only six. However, if c is not limited, there are innumerable sets.

Then, we have to think that the number of three sets can be determinate if we let d bigger.
Now we use ε. ε means very small number.
Let compare the value of d^2 and c. The value of d^2 is the value of $d^{1+\varepsilon}$ when ε =1. Then, there is no sets that meet the condition when c < 100.
We knew the value of d^2 is too big, so we compare $d^{1+\varepsilon}$ and c when ε=0.28.
Then there is only one set that c > d when c < 100.
In this way, the number of three sets which meet the condition is finite if ε is larger than 0 despite of the value of ε is very small. That is the claim of ABC conjecture.

Then, why ABC conjecture is said to be amazing. Have you ever heard Fermat's last theorem? It is theorem what many mathematicians were challenged and struggled. Fermat's last theorem is expectation that when n is a natural number which is more then 3, 「$x^n + y^n = z^n$」 isn't hold.
When n=3, it doesn't hold was proved by Euler. When n=4 was proved by Fermat. When n=5 was proved by Sophie Germain and Dirichlet and Legendre.

Given ε>0, there exists a constant K(ε), for integer a,b,c that all non-zero relatively prime number with a+b = c, we can be established the inequality

$$\max(|a|, |b|, |c|) \leqq K(\varepsilon)\left(N_0(abc)\right)^{1+\varepsilon}$$

x, y, z are positive integer that are relatively prime to each other and to satisfy

$$x^n + y^n = z^n.$$

Let a=x^n, b=y^n, and c=z^n.

Then

$$N_0(x^n y^n z^n) = N_0(xyz) \leqq xyz$$

Applying the abc conjecture, we can get

$$x^n \ll (xyz)^{1+\varepsilon} \ , \ y^n \ll (xyz)^{1+\varepsilon} \ , \ z^x \ll (xyz)^{1+\varepsilon}.$$

However, Sign $\ll$ is represent by omission that there exists a content K(ε) determined by ε. And the inequality α ≦ K(ε)・(α) is hold.

So, the value on the left side of Sign $\ll$ is equal to the value on the right side times K(ε) or smaller than that. By multiplying the side of these inequalities,

we can get

$$(xyz)^n \leqq (xyz)^{3+3\varepsilon}.$$

Additionally, take the logarithm of both sides of this inequality, we can get

$$(n-3-3\varepsilon)\log(xyz) \leqq \log K.$$

But, a content K = K(ε)

From $xyz \geqq 2$, this last inequality shows that there is an upper bound in n.

With this, we proved enough that Fermat's last theorem holds for large value of n.

If ABC conjure is correct, we can prove that it doesn't hold when it is 6 or more. And also, the 20 problems that is not solved will be proved such as Wieferich primes, gaps between primes, Erdo˝s-Woods Conjecture, Roth's Theorem, Mordell's Conjecture (Faltings' Theorem), and Baker's Theorem.

When ABC conjecture are proved, Fermat's last theorem are proved as usual.

We have little chance to be exposed to math, and we can't feel greatness of abc conjecture, but it had a huge impact in mathematics world. However, it is not unrelated with us. If the ways to think like abc conjecture is improved, we may be able to predict a course of typhoon more exactly.

Bibliography

・“独創的すぎる証明”「ABC予想」をその主張だけでも理解する
http://www.ajimatics.com/entry/2017/12/16/175035

・ABC予想のすごさがなんとなく分かるように説明してあるよ。フェルマーの最終定理との関係で。
http://normahead.seesaa.net/article/293209840.html

・THE ABC CONJECTURE AND ITS APPLICATIONS
https://core.ac.uk/download/pdf/77977806.pdf

・S. LANG, *Math Talks for Undergraduates*, Springer-Verlag, 1999

<Impression>

At this time, I got the math class in English for the first time. It is difficult for me to understand English immediately. I felt that I should improve my English skill. And, I was surprised that the teacher could speak Japanese at the end of the class.

— K. YAZAKI

It was very interesting for me traveling to Canada. That was my first visite to Canada. I could have a valuable experience there. Canada had many difference points from Japan. For example, food. Foods are delicious. But they had a strong taste and a lot of quantity.
Especially, I was surprised that Canadian use two mother languages. Morning call was done English and French. It was very impressive for me.
Canada’s cityscape is cute and beautiful. I became like it through this trip. And Canadian are very kind. So, I strong desire to visit there again.

— S. KATADA

In Canada, I felt very cold at first. It is colder than winter in Japan but there are many devices in Canada. What impressed me most about them was a tunnel on campus. I was interested in the difference like this because it is hard to be noticed them, but there is it in the imminent place. It has an example elsewhere. For example, Canada does not have the culture called earrings. I could notice their difference of culture in this study trip, so I want to be interested in such a thing from now on.

— Y. ONO

I have been to abroad before, but I don't remember about that time, so I was looking forward to visiting Canada. I felt Canadian is very kind because many people spoke to us. Through this travel, I thought English is one of useful tools, so I want to be able to speak English better.

— M. NOMURA

<Problem#9: Cubic Equation>

Saki DOIGAWA, Nana TOMONO, Aoi NOHARA, Miyuka TAKAHASHI

Question.

You know the quadratic equation. What is the cubic equation? The quartic equation? Is there a quintic equation?

Solution

We know this formula.

$$ax^2+bx+c=0$$

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

Let's also solve this equation.

$$x^3+ax+b=0$$

Using this equation.

$$\alpha^3+\beta^3+\gamma^3-3\alpha\beta\gamma$$

$$=(\alpha+\beta+\gamma)(\alpha^2+\beta^2+\gamma^2-\alpha\beta-\beta\gamma-\gamma\alpha)$$

Put $\gamma=x$

$$x^3-3\alpha\beta x+\alpha^3+\beta^3$$

$$=(x+\alpha+\beta)\{x^2-(\alpha+\beta)x+\alpha^2+\beta^2-\alpha\beta\}$$

From Sum and Product of Roots,

$$-3\alpha\beta=a$$

$$\alpha^3+\beta^3=b$$

Solve this equation.

$$x^3+ax+b=(x+\alpha+\beta)(x^2+\alpha^2+\beta^2-\alpha x-\beta x-\alpha\beta)$$

$$\alpha\beta=-\frac{a}{3}\ \ implies\ \ \alpha^3\beta^3=-\frac{a^3}{27}$$
$$\alpha^3+\beta^3=b$$

So,

$$t^2-(\alpha^3+\beta^3)t+\alpha^3\beta^3=0$$

$$t^2-bt-\frac{a^3}{27}=0$$

$$t=\frac{b\pm\sqrt{b^2+\frac{4}{27}a^3}}{2}=\alpha^3,\beta^3$$

Solve this formula,

$$\alpha=\sqrt[3]{\frac{b+\sqrt{b^2+\frac{4}{27}a^3}}{2}}$$

$$\beta=\sqrt[3]{\frac{b-\sqrt{b^2+\frac{4}{27}a^3}}{2}}$$

$$x=-\alpha-\beta,\ -\alpha\omega-\beta\omega^2,\ -\alpha\omega^2-\beta\omega$$

So,

$$x=-\sqrt[3]{\frac{b+\sqrt{b^2+\frac{4}{27}a^3}}{2}}-\sqrt[3]{\frac{b-\sqrt{b^2+\frac{4}{27}a^3}}{2}}$$

$$x=-\omega\sqrt[3]{\frac{b+\sqrt{b^2+\frac{4}{27}a^3}}{2}}-\omega^2\sqrt[3]{\frac{b-\sqrt{b^2+\frac{4}{27}a^3}}{2}}$$

$$x=-\omega^2\sqrt[3]{\frac{b+\sqrt{b^2+\frac{4}{27}a^3}}{2}}-\omega\sqrt[3]{\frac{b-\sqrt{b^2+\frac{4}{27}a^3}}{2}}$$

※ $\omega^2+\omega+1=0$,

$\omega=\frac{-1+\sqrt{3}i}{2}$, $\omega^2=\frac{-1-\sqrt{3}i}{2}$

Cardano's solution

We now introduce two new unknowns u and v and write $x = u + v$.

Then on substituting for x, we get

$$\begin{aligned} f(x)=f(u+v)&=(u+v)^3+a(u+v)+b\\ &=u^3+3u^2v+3uv^2+v^3+au+av+b\\ &=u^3+v^3+(3uv+a)(u+v)+b \end{aligned}$$

Now, we choose u and v so that $3uv+a=0$, which removes the $u+v$ term. This gives us $v=-\frac{a}{3u}$. So if $f(x)=0$, we get, in terms of u and v.

If we multiply through by u^3, we get

$$v^6+bu^3-\frac{a^3}{27}$$

Which we recognize as a quadratic equation in u^3. We solve for u^3 using the quadratic formula:

$$u^3+v^3+b-0-u^3-\frac{a^3}{27u^3}+b,$$

$$u^3=\frac{-b\pm\sqrt{b^2+\frac{4}{27}a^2}}{2}$$

Let's try an example that Cardano gave in the Ars magna, namely, find the roots of $x^3+6x-20=0$, which Cardano would have expressed as $x^3+6x=20$, to avoid nagative quantities. Here $a=6,\ b=-20$. Then

$$b^2=400,\ \frac{4}{27}a^3=32,\ b^2+\frac{4}{27}a^3=432=12^2\times 3$$

Therefore, $u^3=10+6\sqrt{3}$ and, in principle we can extract cube roots to find three possible values for u (two of which involve complex cube roots of unity). From what we have said above, $v^3=10-6\sqrt{3}$ and thusarootofthe cubic is.

This is a rather complicated expression. It is not so hard to show that it in fact equals 2, something that Cardano noted, but was not able to prove.

Gerolamo Cardano.

He was born in Milan and died in Rome. He is known as a mathematician. His main business was also a doctor, an astrologer, a gambler and a philosopher. He entered Pavia University in 1520, studied medicine, and later moved to Padua University to learn pharmacology. Eventually he became a doctor and gained fame as a remarkable doctor later Today Gerolamo Cardano is known for showed a solution to the cubic equation and quadratic equation in the book called Ars magna de Rebus Algebraicis.

However, in fact it is not Cardano that discovered a solution to the cubic equation. This has the following background.

In the 16th century, mathematical contest were held frequently, and often problems of cubic equation was set.

Scipione del Ferro (who already knew the solution of the cubic equation), Niccolò Fontana "Tartaglia" (meaning "stutterer") and Gerolamo Cardano participating in the contest. Although Scipione del Ferro was undefeated, Tartaglia wanting not to be outdone, solved himself and won Scipione del Ferro. Cardano got a Tartaglia's solution with a promise not to announce it absolutely.

Of course Tartaglia got angry, but Cardano's announcement became a turning point in mathematical history. He shared the knowledge of mathematics for the first time.
Also he took the idea of imaginary for the first time by solving a cubic equation.
He may have made the foundation of mathematics now.

Bibliography

・三次方程式の解の公式 ［物理のかぎしっぽ］
http://hooktail.sub.jp/algebra/CubicEquation/

<Impression>

On this trip, I was able to be a interesting and valuable experience. I went to Canada for the first time. So, I have a lot of worries. I was not sure if I could buy something using English because I'm not good at English. But I could do shopping well by gesture and help of people around me. I tried speaking to many local people. It was fun to talk with them. I thought that it was important to challenge.
Also, we solved the problem one question per group by the time we go to Canada. Our problem was difficult for us to understand even if in Japanese. So, I was little worried whether I could explain in English in Carlton University. Dr. Colin's question was difficult, we thought and thought. He helped us gently. I'm glad to our speech was successful.
I think this project was a very nice choice. I will never forget this experience.

— A. NOHARA

I am not good at mathematics or English, so I was worried about my ability at the Carlton University. However, the lesson at Carleton University was very pleasant and I was glad that I could learn the characteristics about the numbers. Also, Mr. Collin's lesson was very easy to understand and I enjoyed taking classes. Working on this research, the most difficult thing was to look for concrete examples. Our group has deeply learned about cubic equations. At that time, beautiful numbers did not appear, or answers could not be deduced. However, when we announced our research results, we were confidently announced with members. Although it was serious, it was a nice experience to talk with Mr. Collin in English. Someday I would like to study various fields at Carlton University again.

— N. TOMONO

On this trip, I was able to do a lot of precious experiences that I can not usually do. Of course, the class at Carleton University is one of them. on the day We went to Carlton University, I was very nervous because I am not good at English, but Mr. Colin's class was easy to understand and fun. Especially, the class about Number guessing game was very interesting! After we made the presentation about cubic equations, Mr. Colin gently gave us advice. But I could not catch and understand his questions well, so I thought I would study English and math more. That was a good experience for me. Our problem was very difficult, but it was fun to solve problem with members of the group. On this trip, I was able to get along better with them. I want to make use of what I learned here for the future. I'd like to go to Canada again!

— S. DOIGAWA

My group studied cubic equations before going to Canada. While examining, we gradually understood about the cubic equation, but it was a very difficult problem. By overcoming that "difficult", we succeeded in researching cubic equations.

At Carlton College, we presenting the comments in front of everyone in the class, Mr. Akiyama, and the professor. I was very nervous, I could not speak well and I could not talk accurately it, but our presentation has ended. However, the subsequent professor's question was very difficult.

I went sightseeing around Canada. I bought some sweets that I can not buy in Japan at supermarket. I also bought a lot of maple syrup for souvenirs. In a park and a museum, I experienced a different atmosphere from Japan. This is an unforgettable memory. I want to go again.

— M. TAKAHASHI

<Problem#10: Complex numbers and n th order Equation>

Runa YOSHIDA ,Yuka KAMEDA , Yuna OHMORI
Miyu INOUE, Marika SUGANUMA, Kako FUJITA

Question.

What are comlex numbers? What is the Fundamental Theorem of Algebra?

Solution

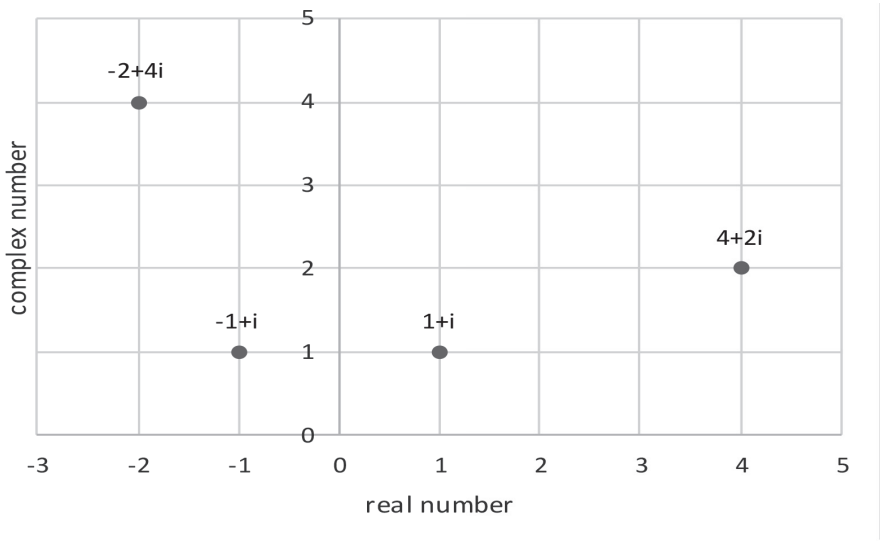
We thought about the problem of "What are complex numbers?" and "What is the fundamental theorem of algebra?".

First, we thought about the problem "What are complex numbers?". The real number is the number that actually exists. Example is $1, 3, -7$. An imaginary number is a number that becomes a real number less than 0 when squaring. Example is $i, 5i, -4i$. A complex number is a combination of an imaginary number and a real number. Example is $3-i, -7+5i$ The imaginary number is a number that does not actually exist, and since the complex number also includes the imaginary, it is a number that does not exist.

However, "imaginary number" may be defined as "a complex number that squared value is a real number not exceeding zero". The imaginary unit represented by is an example of a representative imaginary number. In 1572 Rafael Bombelli defined imaginary numbers. However, at that time, even zero or negative numbers were considered fictitious, useless, and the imaginary number which is the square root of the negative number was still more. René Descartes also neglected and named "imaginary number" in the book "La Gémétrie (geometry)". Descartes used the word "imaginary" for the first time in 1637. However, the idea of imaginary number itself was discovered by Gerolamo Cardano in the earlier 1500's, and it was accepted by people through Leonhardt Euler and Carl Friedrich Gauss.

Thanks to the imaginary number it is possible to express numerical values that can only be expressed in graphs. If you multiply the coordinates in this figure by i, the coordinates rotate counterclockwise 90 times and the position of the coordinate's changes. Therefore, the movement of the upper point can be represented by a mathematical expression.

It is also used to describe fields such as signal processing, control theory, electromagnetics, quantum mechanics, mapography, etc. in the application of imaginary numbers. As a rule of thumb, real



numbers are often used to represent various data. But fractions that are useless to count the number of people are also useful to compare the size of the stone and negative numbers that are useless to describe the weight of the object are also indispensable for representing the amount of debt. So imaginary numbers are needed.

For example, in electronics, the DC voltage generated by the battery is expressed as a real number such as $+12$ volts or -12 volts, but two parameters are required to represent the household AC voltage. One is an amplitude of 120 volts etc. and the other is a phase called a phase. Such two-dimensional values are expressed mathematically as vectors or complex numbers. In vector representation, the rectangular coordinate system is usually represented by X component and Y component. On the other hand, in a complex number expression called a phasor display, the two values are the real part and the imaginary part. For example, a pure imaginary number having a real part of 0 and an imaginary part of 120 means a voltage having a phase of 90 degrees and 120 volts.

Next, I will show you why complex numbers are necessary together with history.

René Descartes of France (1596-1650: 54 death age) insisted that this number is “fantasy”, and even after half a century Germany German mathematician Leipnitz (1646-1716: 70) Thought that it was “a splendid flight of the spirit of God” and thought that it was different from the “number” so far. That is, $'x^3=15x+4$ “What is this answer?” x has three answers. Solving in the figure, $y=x^3, y=15x+4$. You can find the intersection of the two lines, so if you write a graph using Excel you can see that there are answers to $x=4,\ -0.268,\ -3.732$.

This problem was a big problem for algebra student Gardano. Despite the fact that real answer is obtained It is because it is said that we cannot answer without using the imaginary number ($i=-1$)

when trying to handle it numerically. Mathematical rules necessary for handling this imaginary number were required even for several generations, among which Leipnitz (mentioned above) and Euler (1705-1783: 78) made a major contribution. But even Euler said, “It is obvious that the square root of a negative number should not be recognized as a member of a number ... ... they are only in our fantasies” It is. In this vessel, Norwegian surveyor Bethel (1745-1818: 67) who studied mathematics by self-taught to conceptualize this mysterious number, conceptualizing complex numbers and establishing relationships with the ancestor’s numbers was the first hurdle to overcome did. We announced in the newsletter of the Danish Academy in 1798.

Thanks to the imaginary number it is possible to express numerical values that can only be expressed in graphs. If you multiply the coordinates in this figure by i, the coordinates rotate counterclockwise 90 times and the position of the coordinate’s changes. Therefore, the movement of the upper point can be represented by a mathematical expression.

Next is the algebraic theorem.

First, I will introduce from the history. It was claimed by Albert Girard (French version, English version) and others in the first half of the 17th century, and since the mid-18th century Jean Le Ront D’Alembert, Leonhardt Euler, François Davier de Fonnes (English version), Joseph = Louis Lagrange, Pierre Simon Laplace and others tried to prove. Proof was refined, but none were incomplete.

In 1799, Karl Friedrich Gauss pointed out the lack of proof so far in the dissertation and gave the first full proof. Later year Gauss gave three theorems to this theorem. More proofs are known now.

The algebraic theorem is that there are n number of solutions of the n th order equation.

- $x^2+x-6=(x+3)(x-2)=0,\ x=-3, 2$
- $x^2=-1\ , x=i,\ -i$

This expression cannot be represented by an integer solution, but you can express it using imaginary number. (The fundamental theorem of algebra is a theorem that guarantees that n solutions are always found in the n th order equation if the range of searching solutions to the range of complex numbers is expanded.) So, the algebraic theorem requires an imaginary number. Complex numbers

extend the possibilities of mathematics.

Next, we will show that complex numbers can be expressed on a plane.

Bessel Proposed The following things.「$2+i11$ is East 2, North 11. $-3-i4$ is West 3, South 4.」It means to correspond to the coordinates of the plane. We use this complex plane for addition and subtraction of vectors on the plane. The one corresponding to the x axis of the xy plane is the "real axis", and the one corresponding to the y axis is the "imaginary axis". Consider the case of $1+i3$, $4+i5$, $3+i2$. These show addition / subtraction relationships.

$$(1+i3)+(3+i2)=(1+3)+i(3+2)=4+i5$$
$$(4+i5)-(3+i2)=(4-3)+i(5-2)=1+i3$$

It is understood that addition and subtraction should be performed on the real part and the imaginary part respectively.
Next, consider the case of multiplication.

$$(a+b)(c+d)=ac+ad+bc+bd$$

Therefore,

$$\begin{aligned}(a+ib)(c+id)&=ac+a\cdot id+ib\cdot c+ib\cdot id\\&=ac+iad+ibc+i^2bd=ac+i(ad+bc)+(-1)bd\\&=(ac-bd)+i(ad+bc)\end{aligned}$$

If you understand exactly only the value of the imaginary number, you can see that it is the same as the real numbers. Next in division,

$$(x+y)(x-y)=x^2-y^2$$
$$(a+ib)\div(c+id)=\frac{a+ib}{c+id}$$

It is troublesome that there is id in the denominator, so use $i^2=-1$ to represent it with real number.

$$(a+ib)\div(c+id)=\frac{a+ib}{c+id}=\frac{(a+ib)(c-id)}{(c+id)(c-id)}$$

$$=\frac{(a+ib)(c-id)}{c^2-(id)^2}=\frac{\{ac-(ib)(id)\}+i(bc-ad)}{c^2+d^2}$$

$$=\frac{(ac+bd)+i(bc-ad)}{c^2+d^2}$$

It can be expressed in the form $r+ix$ like this. These are the four arithmetic operations on complex numbers of $a+id$ type notation displayed in a complex plane.

Next consider the case where the coefficient is complex number. Even if the coefficients are complex numbers, the equation can be solved.

For example,

$$x^2+(1+i)x+(-2-i)=0$$

From solution formula of quadratic equation.

$$x=\frac{-1-i\pm\sqrt{8+6i}}{2}$$

$$\sqrt{8+6i}=(8+6i)^{\frac{1}{2}}$$

With $z=8+6i$

$$z=10\left(\frac{4}{5}+\frac{3}{5}i\right)=10(\cos\theta+i\sin\theta)$$

However, $\cos\theta=\frac{4}{5}$, $\sin\theta=\frac{3}{5}$

So,

$$z^{\frac{1}{2}}=\sqrt{10}\left(\cos\frac{\theta}{2}+i\sin\frac{\theta}{2}\right)=\sqrt{10}\left(\frac{3}{\sqrt{10}}+\frac{1}{\sqrt{10}}i\right)=3+i$$

Therefore,

$$x=1,\ -2-i$$

However, the quantic equation is an exception from the insolvability of the quintic equation.

<The insolvability of the quintic equation.>

1. Subgroup of solvable group is solvable group at all.
2. Quintic alternating group is simple group.
3. Factor group obtained by dividing quintic alternating group by simple group is not cyclic group.
4. Make sure that quintic alternating group is not solvable group.

If we prove that the quintic equation does not hold, the formula of the solution of the quadratic equation

$$x^2+ax+b=0 \text{ is } \frac{-b\pm\sqrt{b^2-4ac}}{2} .$$

Assuming that solutions of this quadratic equation are x_1 and x_2, the contents of the radical are

$$a^2-4b=(x_1+x_2)^2-4x_1x_2=(x_1-x_2)^2 \qquad (2)$$

(2) is invariant to swapping between x_1 and x_2

However, taking the square root, two values of $y_1=x_1 \cdot x_2$ and $y_2=x_2 \cdot x_1$ appear. These values have the following properties: y_2 is replaced with x_1 and x_2 of y_1

y_2 is the value obtained by multiplying y_1 by the square root of 1 (one not being 1) (that is, $y_2=-y_1$) Therefore, x_1, $-x_2$ is changed by the replacement of x_1 and x_2, but if it squares it becomes symmetric.

Let's consider a cubic equation. Similar to the right side of (2)

$$\{(x_1-x_2)(x_2-x_3)(x_3-x_1)\}^2 \qquad (3)$$

Consider the expression. This is a symmetric expression because values do not change no matter how x_1, x_2, x_3 are substituted.

However, they took the square root

$$(x_1-x_2)(x_2-x_3)(x_3-x_1) \qquad (4)$$

In the expression " x_1 " and " x_2 ", the sign changes depending on the replacement (substitution). It is the same even if replacing with pairs of x_1 and x_3 , x_2 and x_3 .

However, (4) does not change even if (x_2, x_3, x_1) or (x_3, x_1, x_2) cyclically replaces (x_1, x_2, x_3) (this substitution is called cyclic substitution). Therefore, there are three types of substitutions that do not change the value of (4), including identity substitution. It was possible to reduce the substitution which was originally six kinds to 3 types by taking the square root.

Next,

$$(x_1+x_2\omega+x_3\omega^2)^3 \qquad (5)$$

Let's think about the expression. Here, ω is the cube root of 1 (not 1). This expression is also invariant to the cyclic permutation of (x_2, x_3, x_1) or (x_3, x_1, x_2) (note $\omega^3=1$). Therefore, (5) can be produced by adding, subtracting, and subtracting the symmetric expressions a to c with (4) .

Taking the cube root of (5)

$$y_1=x_1+x_2\omega+x_3\omega^2$$
$$y_2=x_2+x_3\omega+x_1\omega^2$$
$$y_3=x_3+x_1\omega+x_2\omega^2$$

Three values come out. These values,

y_2 and y_3 are obtained by applying cyclic permutations (x_2, x_3, x_1) and (x_3, x_1, x_2) to y_1 , $y_1=y_2\omega$ and $y_2=y_3\omega$.

It has the property of. So, y_1, y_2, y_3 are not immutable for any substitution, but cubing makes it invariant to cyclic permutation. If a number that is not immutable for any permutation is obtained, values of x_1, x_2, x_3 can be obtained by applying appropriate addition, subtraction, multiplication, multiplication, multiplication,

From the above, in order to solve a cubic equation, it is necessary to first take the square root and then the third cube.

In fact, according to Cardinal's formula, a cubic equation $x^3+px+q=0$

(Which can be transformed so that the coefficient of x^2 becomes 0 without losing generality) is $x=\sqrt[3]{-\frac{q}{2}+\sqrt{\left(\frac{p}{3}\right)^3+\left(\frac{q}{2}\right)^2}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\left(\frac{p}{3}\right)^3+\left(\frac{q}{2}\right)^2}}$

When it comes to a quartic equation, there are $4!=24$ possible substitutions for solutions x_1, x_2, x_3 and x . However, thanks to the uniqueness of $4=2^2$, by pairing the solutions into two pairs, it is possible to successfully decompose 24 substitutions.

For example, considering the expression $x_1x_2+x_3x_4$, this takes three different values for 24 permutations. Therefore, the solution of the quartic equation is reduced to solving the cubic equation. However, in the quintic equation, the coupling between the five solutions $a\ b\ c$ becomes strong.

(4) is expanded to five variables, in this case as well, it is possible to change the sign by an odd number of permutations between arbitrary pairs of x_1 to x_5. Therefore, $5!=120$ possible substitutions can be reduced to 60 ways. The problem is after this.

In the case of three original elements, even if the value changed by cyclic permutation of x_1, x_2, x_3 it was possible to make the value unchanged by repeating the cyclic substitution three times . So, by taking the third root, we were able to reduce the number of substitutions that do not change the value. However, if there are five elements, if the value obtained by repeating cyclic permutation of x_1, x_2, x_3 and cyclic permutation of x_3, x_4, x_5 p times (p : prime) is unchanged, it was done only once It is (relatively easy to prove) that the value of time is unchanged. That means that if you start from the symmetric expression a to e, you cannot change the number of permutations that makes the value invariant less than 60, regardless of how you add, divide, divide, or divide roots. Therefore, the solution of the quintic equation cannot be represented by addition, subtraction, multiplication, division and multiplication. This completes the proof.

In conclusion, complex number is necessary for the algebraic theorem to hold. By introducing i which is an imaginary number, we can solve not only the equation $x^2+1=0$ but also all algebraic equations.

Complex number is number that exist only in the mind. It is on the surface or it is a complex plane. It tends to be an artificial number made by force to force $x^2+1=0$ but in algebra it is a natural number as it existed from the beginning, a professional mathematician no one would think that it is artificial as one person.

In conclusion, a complex number can correspond to any expression, and it is a wonderful discovery.

<Impression>

Because I was traveling abroad for the first time, there were lots of impressive things. First, it was strange that all the signboards in the town are in English and French. In addition, the city was very beautiful and moved. And I was surprised that cooking taste is quite different between Japan and Canada. I am not good at English, so I was very worried about this trip, but I realized that if I tried my best trying to tell my idea using gestures etc even if I could not speak English, I could convey. Through this experience I thought I would make use of it for my future English study.

— Y. KAMEDA

I didn't thought that I wanted to go to Canada very much before, but when I went to Canada, I was surprised at that there was very beautiful city. All pictures which were taken there were different from Japan, I wanted to stay in Canada forever.

The different from Japan is that the correspondence of Canadian clerks is more complicated than Japan. The shop clerk of some stores was facing the correspondence, so I felt nervous.

I wanted to go to Canada again from the bottom of my heart. If I go to next time, I think I will buy more souvenirs.

— M. SUGANUMA

I was a little worried that I never went abroad, but local people were gentle and could talk a lot at shopping time. In the lesson, I learned the calculation method which I did not know until now, and I was able to spend meaningful time. In the presentation everyone was shared by all the members and was promoted smoothly. I went to Canada and learned how to talk with foreigners and I was able to learn mathematics and English happily. Also, if I have the opportunity to go to Canada I would like to study English more and I want to go there.

— Y. OHMORI

I was uneasy until I went to Canada, so I was thinking about Canada every day. However, I was surprised to wide land and the view different from Japan. The mathematical class and the presentation that were uneasy was difficult, but I think that it helped my growth.

I know that I can pay for the dollar, but I was not able to pay for the cents by myself. So, when I got back to Japan, I had plenty of cents. I want to be able to pay for the cents, if I have chance to go to Canada again.

— R. YOSHIDA

In Canada traveling there was something that was amazing and also enjoyable. Because understanding was difficult at the university because it can proceed in English, Collin teacher at Carleton University taught me in detail so I understood the content of the lesson. It is the size of the city that was surprised by the difference from Japan. I thought that the width of the road is also wide and the size of the vans etc is so large that it cannot pass through Japan. The coldness of Canada was colder than Japan's midwinter, but it survived with the pleasure of blowing off the cold. French cuisine I ate on the 3rd day was very delicious. Because there are not many famous Canadian cuisines in Canada, I ate a lot of food from other countries. Still it was fun to be able to feel overseas every time food of unexpected size comes out in Japan. It was very meaningful to enjoy a safe journey. It is full of appreciation to teachers who supported this Canada trip, tour operator and driver. I would like to go to Canada this summer as well.

— M. INOUE

I went to Canada. I was surprised by the difference in temperature with Japan. It was many times cold in Japan. In the winter the river becomes a skate link. So, river become skate link. By saying so, I did not get a lot of white breath. Perhaps there are few trashes in the air. Next, I went to Notre Dame Cathedral. I saw a beautiful view when I opened the door. It was very beautiful. We treat rice as vegetables in Canada. In Canada, there were no wires compared to Japan and the cityscape was beautiful. Each building was very big. It seems that we still know a lot.

— K. FUJITA

Day 1

Let’s Departure!

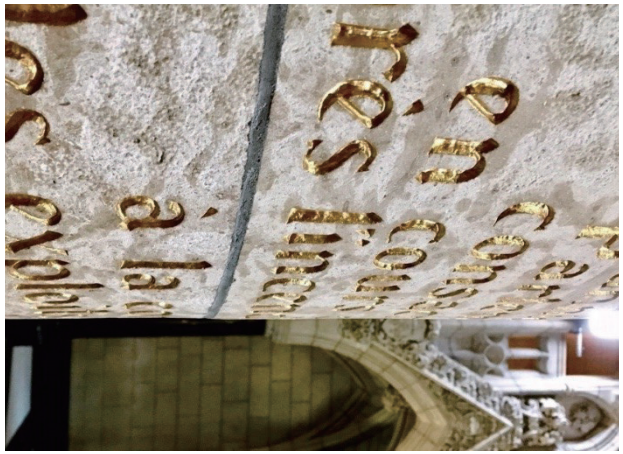
Where is this? This is airport in Ottawa!

This plane have maple leaf canada's symbol

Welcome to Canada!!

Day 2

They are group 7 in front of the Parliament Building



Pillar of the Parliament Building is beautiful

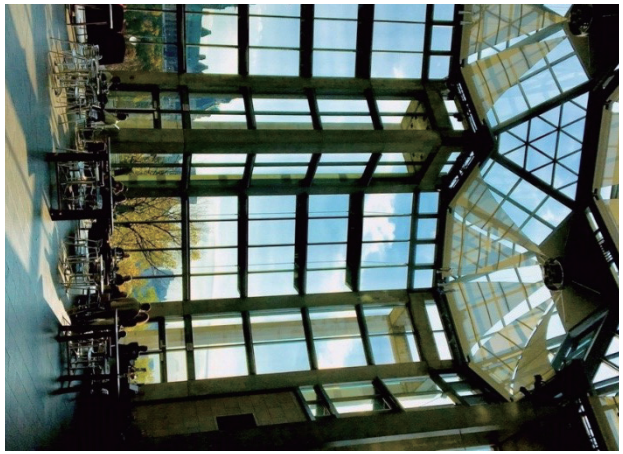
This is interesting tour guide

They have a very good smile!

Putin is very delicious!

HISTORY MUSEUM

We walked at Gatineau Park



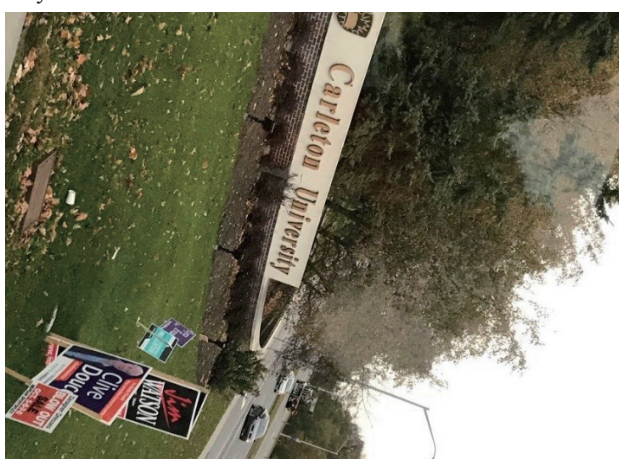
We appreciated National gallery of art

It is the shell of mussels of dinner

This is OTTAWA big object

Day 3

Are you ready? Say cheese!



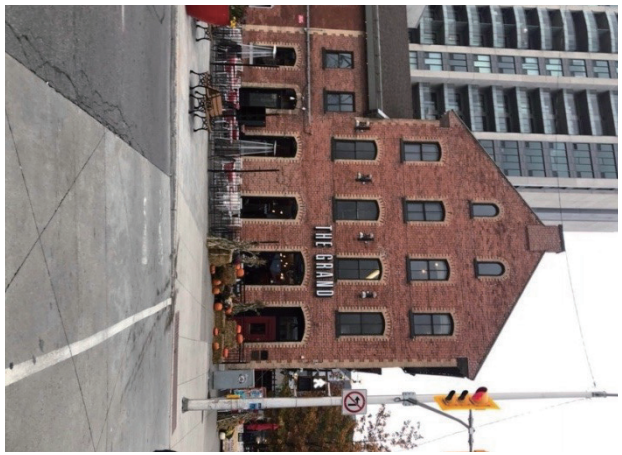
Carleton University is very big!

Learn Mathematics in English 1

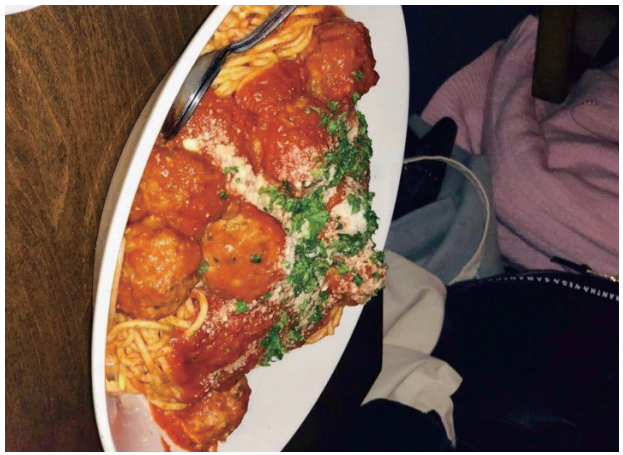
Learn Mathematics in English 2

Learn Mathematics in English 3

Souvenir is many maple syrup!



What are fashionable building this is!

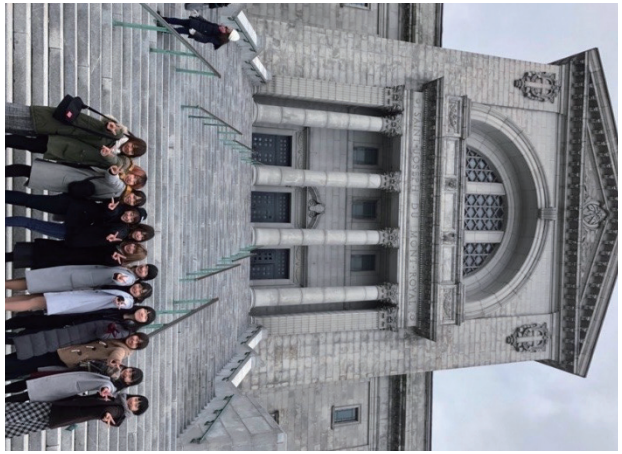


Food is boryumi in Canada!

Day 4

It was a tough day ;;;;

Group photograph at St. Joesph's Oratory



Girls' group photograph only!

Norte Dame Cathedral

Day 5, 6

We enjoyed free behavior at old town

See You Ottawa

平成 30 年 10 月 2 日

中央大学附属高等学校平成 30 年度フィールドワーク　日程表

カナダ：オタワ・カールトン大学体験授業　エアカナダ利用案

平成 30 年 10 月 22 日（月）～27 日（土）　　参加人数：生徒３５名様＋ご引率２名様＋添乗員１名

	月　日	地　　名	現地時間	交通機関	行程	食事
1	10/22 （月）	羽田空港集合 羽田空港発 ﾄﾛﾝﾄ空港着 ﾄﾛﾝﾄ空港発 ｵﾀﾜ 空港着 ｵﾀﾜ 空港発	15:30 17:40 16:45 19:10 20:11 21:30	各自 AC002 便 AC464 便	集合 エアカナダトロント直行便にて出発≪所要 12:05≫ 入国審査・通関後、カナダ国内線へ乗り継ぎ。 オタワへ≪所要 0:59≫ 弊社係員がお出迎えし、専用バスで市内のホテルへ （ホテルにておにぎり弁当を配布） **（宿泊ホテル：ｺｰﾄﾔｰﾄﾞ ﾊﾞｲ　ﾏﾘｵｯﾄ　ｵﾀﾜ）**	夕：機内 昼：機内 夕：○ （軽食）
2	10/23 （火）	オ　タ　ワ		専用バス	日本語ｶﾞｲﾄﾞ同行にてオタワ市内見学。 8:15 ホテル出発 （市内とカールトン大学付近を車窓見学） 9:30　国会議事堂 11:30 徒歩にてリドセンターにて移動 11:40-12:45　ランチ（各自） 13:15-14:15　ガティノー公園 14:45-15:45　歴史博物館 16:00　美術館入館 17:00　美術館閉館（徒歩にてホテルへ） **（宿泊ホテル：ｺｰﾄﾔｰﾄﾞ ﾊﾞｲ　ﾏﾘｵｯﾄ　ｵﾀﾜ）**	朝：○ 昼：× 夕：○
3	10/24 （水）	オ　タ　ワ		路線バス （各自支払）	朝食後、路線バスでカールトン大学へ。 午前中：体験授業（お客様手配） 大学のカフェテリアで各自昼食後、 市内中心部で自由行動。 **（宿泊ホテル：ｺｰﾄﾔｰﾄﾞ ﾊﾞｲ　ﾏﾘｵｯﾄ　ｵﾀﾜ）**	朝：○ 昼：× 夕：×
4	10/25 （木）	オ　タ　ワ モントリオール オタワ	8:30 18:00	専用バス	朝食後、専用バスにてモントリオールへ。 ホテル出発 （見学箇所） ・モンロワイヤル公園 ・ドーチェスター広場 ・ノートルダム・モンレアレ教会 ・旧市街散策 ホテル到着 **（宿泊ホテル：ｺｰﾄﾔｰﾄﾞ ﾊﾞｲ　ﾏﾘｵｯﾄ　ｵﾀﾜ）**	朝：○ 昼：○ 夕：○
5	10/26 （金）	ホ　テ　ル　発 オタワ空港着 オタワ空港発 トロント空港着 トロント空港発	08:00 08:30 10:00 11:03 13:40	専用バス AC447 便 AC001 便	朝食後、専用バスにて空港へ。 トロントへ≪所要 1:03≫ 帰国の途へ≪所要 12:55≫ **（機中泊）**	朝：○ 昼：機内 夕：機内
6	10/27 （土）	羽 田 空 港 着	15:35		通関後、解散 お疲れ様でした。	

教養総合「数学を英語で」カナダ・フィールドワーク

柳　田　茂　久（数学科）

今回のカナダでのフィールドワークには特筆すべき点が２つある。

第一に、教養総合科目「数学を英語で」の目指す教育が存分に実行され、参加した生徒にとって大変貴重な機会となったことが挙げられる。カールトン大学での英語による講義と、その後の生徒によるプレゼンテーションの場に同席したが、担当して下さったColin教授の話に真剣に聞き入る様子や、必死で答えを模索してコミュニケーションを図ろうと努力する姿を目の当たりにして、英語により数学を学ぶ過程での生徒の成長を実感した。英語はあくまでもコミュニケーションの「道具」であり、数学を介することで生徒たちは英語を「道具」として用いることの大切さを学んだのだ。

第二に、文化の多様性を肌で感じたことが挙げられる。言語や生活環境が異なることに加えて、制度やルールに差があるため、東京とは異なる首都オタワの在り方に驚かされることも多く、中でも簡単に国会議事堂に入館できたことは衝撃であった。また、モントリオールを訪れたことで、公用語が２つ存在する国であることを再認識し、オタワとは異なる現地の雰囲気を肌で感じて、言語の持つ影響力を生徒に伝えることができた。

このように、今回のカナダでのフィールドワークは教養総合科目として非常に価値のあるものであり、ただの観光旅行とは一線を画している。数学科教諭として、今後も継続して教養総合科目「数学を英語で」に関わり、生徒にとって有意義な学びとなるよう尽力していきたい。

2018　中央大学附属高等学校　フィールドワーク教養総合
オタワ　カールトン大学　研究発表　カナダ研修

JTB 添乗員　山　本　雅　美

皆さんの研修旅行が終わり、はや２か月新しい年を迎えました。
まずはあけましておめでとうございます。
そして昨年は皆さんの旅行に同行させて頂き、お役に立てなかったにも関わらず、最後にエルクの可愛らしいお人形まで頂戴して大変有難うございました。
たった６日間されど６日間皆さんがこの旅行の為に準備してきたことは大変なご苦労があったと思います。

「英語で数学を」という文系の私にはとんとわからない、むずかしい研究テーマで皆さんが大学でどのような発表をするのだろうかと興味深々でした。最初の Colin 先生の授業はまるでマジックのようでした。わかりやすく数字の不思議を解説してくださいました。
その後に各班ごとに１年をかけて研究、また英語で作ってきた内容を一所懸命に英語で説明しようとする姿を心の中で応援しておりました。（内容は・・・すみません。私には難解すぎました。）
これまでは修学旅行と言えば観光（もちろん大事ですが）や B&S という現地の大学生と班ごとに自由時間を過ごすというプログラムが多いのです。しかし皆さんのカナダの大学で教授の前で発表するなどの経験は絶対できない事だったと思います。この経験が将来の皆さんの人生にどのように影響するかわかりませんが、少なくともやってきたことの集大成を英語というツールで世界共通に伝えられた素晴らしさを感じたのではないでしょうか。

文系理系に関わらず、英語は世界共通の言葉で、社会に出たら出る前にも絶対に必要なツールです。文献は英語で書かれたものが多く、それを理解できなければそこから道を開くことは困難と言えるでしょう。研究分野以外にも経済面や文化面今やインターネットなしでは暮らせない毎日で英語の重要性は高まりますが、皆さんには日本人としての Identity も英語で発言できるようにして頂きたいなと思います。日本が Global Standard ではありません。日本風を当然と思わず、まず、その国の歴史や文化や習慣や人達を理解し日本人としての和をもって接しなおかつ自分の意見も怯まず発信する。
モントリオールではカナダの中のフランスも感じたと思います。オタワでは国会議事堂の中のエリザベス女王の肖像画も見ました。ビーバーテイルも食べました。メイプルシロップもお家で味わいましたでしょうか？
いろいろな体験を通じてその国に関心を持ち、Respect してどんどん外国に飛び出して行ってください。まとまらない文章ですみません。
またどこかの空でお会いできることを願っています。

<Overall Impression & Conclusion>

At the beginning of this course (April 2018), I didn't know many of the students who took my class, so I felt slightly anxious when considering what approach I should take for our lessons. After each passing lecture I began to realize that I was lucky to have such a motivated group, and wanted them to experience the Canadian university system. The main reason for this was to broaden their horizons by giving them the opportunity to experience a foreign university's atmosphere. I also wanted then to see how mathematics is taught in another country, and highlight the advantage of studying English.

During the first semester students studied mathematics in English as much as possible. To assist them in this process, I taught the students key English mathematical vocabulary and phrases accompanied by working examples so that they could understand the mathematical terms in English. As well as this, I wanted the students to apply logical thinking in an attempt to make English language learning easier for them to understand.

During the second semester, 10 mathematical problems were sent to us by one of the professors at Carleton University. The students focused on solving them according to their level of interest. I was pleasantly surprised that my students did not ask for much advice with regards to solving these problems. The students seemed to feel at ease using English to solve mathematical solutions, and their presentations were at a much higher standard than I expected. I was particularly delighted at how they challenged themselves in Ottawa, where they worked hard to express their ideas and present their findings in English.

I would now like to introduce an aspect of Canadian life that thoroughly impressed me during our stay in Ottawa. It is their version of what we call 'priority seating' in Japan.

What is Cooperative Seating?

All of their vehicles have clearly-labeled Cooperative Seating areas, either in front of the bus or by the O-Train's entrances. These seats are meant to make travel easier for customers who have a hard time standing in a moving vehicle or those who need to sit close to the entrance, including:

- *Persons with disabilities*
- *Seniors*
- *Persons with assistive devices (wheelchairs, scooters, walkers, canes)*
- *Pregnant women*
- *Customers with small children or open strollers*

Look for this logo marking the Cooperative Seating area!

Remember that many customers don't have an obvious disability, but may need a Cooperative seat for reasons we can't see. It takes courage to ask someone to give up their seat. If you are sitting in a Cooperative seat but don't need to be, please offer your place to someone who needs it.

Although this type of seating is called priority seating in the UK and Japan, I feel the wording does not express how important this gesture truly is. The term 'cooperative seating' is a much more pleasant phrase. I believe that this system goes a long way to making a society a great place to live. It was my greatest pleasure to have been given the opportunity to take my students to Ottawa, a place where such kindness is shown in their daily lives, as highlighted by their 'cooperative seating' program. I hope that other countries follow their lead and introduce this campaign.

It is very important to experience as many things as possible – including the failures.

K. Akiyama