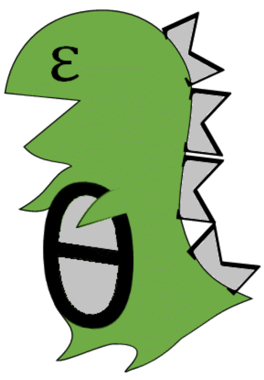
数研 2020

早稲田大学系属　早稲田実業学校

数学研究同好会

会誌第 5 号



数研マスコットキャラクター

すうけんザウルス

はじめに

こんにちは，数学研究同好会です！

今年で数研は文化祭参戦５周年．部誌も第５号となります．今年度は新入生がなんと９人も！特に中１はみんな活発で，数研は毎日にぎやかです．

数研では数学が好きな人たちが集まって，問題を一緒に解いたり，議論したり，数学にちなんだゲームをしたりなどして楽しんでいます．講義を開いたり，各種コンテストに参加したりすることもあります．

この部誌では，数研部員たちが各々のテーマで数学の面白さ，凄さ，魅力を紹介します．この部誌で数学を楽しい！面白い！と感じていただけたら幸いです．ただ，中にはとても難しい内容も含まれます．今，難しい！わからない！と思われたとしても，数年後にもう一度読んでみてください！新たな発見があるかもしれません．

また，今回の部誌のために，個人名の代わりとして部員それぞれの“アイコン”を作成しました．記事タイトルの右下に記事を書いた人のアイコン, p.39 の「すうけん 2020 メンバー」にアイコンの一覧があります．初めての試みなので，アイコンにも注目し，楽しんでもらえたら嬉しいです．

それでは，数学研究同好会部誌第５号をお楽しみください！

目次

数学の用語・記号について

この部誌をより楽しむために必要最低限の知識をまとめました.

[整　数]　$\cdots, -2, -1, 0, 1, 2, \cdots$
[自然数]　$1, 2, 3, 4, \cdots$
[有理数]　二つの整数の比で表される数（分母は 0 でない整数）.　例, $\frac{1}{2}$　$-\frac{3}{4}$
[無理数]　二つの整数の比で表すことができない数.
[実　数]　有理数と無理数をあわせて実数と呼ぶ. 数直線上に表せる数.
[正(せい)の実数]　0 より大きい実数.
[負(ふ)の実数]　0 より小さい実数.

[定　数]　定まった数.　 例, 2, 3（一般的に表すときにはa, bなどの記号を用いる.）
[変　数]　定まっていない数. x, yなどの記号を用いる.

[加　法]　足し算
[減　法]　引き算
[乗　法]　掛け算
[除　法]　割り算

[命　題]　正しい（真）か誤っている（偽）か判断できる文章や式.
[証　明]　ある命題が正しい（真である）ことを明らかにする一連の流れ.
[定　理]　真であることが証明された命題.
[補　題]　ある命題を証明するときに補助として用いる定理.
[背理法]　ある命題を証明したいときに, その命題が偽であると仮定して, そこから矛盾を導くことで, 偽であるという仮定が誤っていた, つまり命題は真であると結論付ける証明方法.
[$\therefore$]　ゆえに, よって
[$\because$]　なぜならば
[□]　証明終了

[任意の～]　どの～でも, いずれの～でも
[∽]　相似　 例, $\triangle ABC \backsim \triangle DEF$
[a^2]　aの 2 乗. $a \times a$（aを 2 回掛ける.）　例, $3^2 = 3 \times 3 = 9$
[$\sqrt{a}$]　2 乗するとaになる数. ルートaと読む.　例, $\sqrt{4} = 2$

第 1 章

3か月で「ジュニア数学オリンピック(JJMO)」本選出場への体験記

私たちの早稲田実業学校(中等部・高等部)の「数学研究同好会」は，数学好きが集まったアットホームな同好会です.

しかし昨年，算数好きだった私は入部したものの，好きな分野を突き詰める先輩や同級生の情熱に圧倒され，中学生と高校生では天と地ほどの学力レベル差に愕然とするばかりで，夏休みには「退部しようかな…….」とくじけていました.

しかし，そんな中 1 だった私でも，3 か月の勉強で JJMO の予選に通過し，本選に出場するというミラクルが起きました.

そこで，これから JJMO を目指す後輩や小学生のみなさんが，楽しく勉強できる参考になればと思い，恥ずかしながら紆余曲折の体験を書いてみました.

<チャレンジしたきっかけ>

アットホームな数研でしたが，楽しかった文化祭が終わると 11 月に突然，数学オリンピック(JMO)に向けて先生や先輩の講義や，疑似問題などが始まり，いきなり戦闘モードになったのでびっくり！勉強していなかった私は，ますます居場所もなく肩身の狭い思いでした.

しかも 1 月の予選まで，あと 3 カ月しかありません. 受験算数＋中 1 程度の勉強経験では JJMO の過去問を解いても合格点の 6 割いくかどうかで，残りの 4 割など答えを見てもチンプンカンプン. しかもその時になって気づいたのは，JJMO の勉強範囲は数 I A どころか数 II B もあるということ……. 歴史で例えるなら，飛鳥時代までは勉強済みだが，合格するには残りの奈良時代から現代までの膨大な範囲が残っているという感じ. 絶望的でした.

しかし，すでに出願していたし，自分だけ全然勉強していないのも恥ずかしく，どうせ来年も受験するなら今やるしかないでしょう！と，そこから気持ちを切り替えて参考書を集めるという，まるで富士山にサンダルで登るような無謀な挑戦がスタートしました.

<参考書や問題集のこと>

マイペースな私は，市販の書籍で独学しながら中学受験をしたのですが，その経験からすると，JJMO・JMO 関連の書籍数は，本屋にあった受験算数書籍(難関校レベル)の 10 分の 1 もないと感じました. 本番レベルの問題集がとても少ないのです. 基礎ができないうち

にたくさん挑戦してしまうと，初見の問題がなくなりそうでした．

おまけに大学受験でたまに出題されるようなマニアックな問題もあるので，時間がないこともあり，とりあえずいろいろ書籍を購入して，全体を把握して計画的にすすめることにしました．

まず，膨大な高校数学の範囲を，青チャートや分野別の問題集などで基礎固めをすることに．それに 1 カ月半かかりました．それから徐々にレベルアップで 1 カ月．最後の半月は冬休みだったので，過去問レベルの問題を集中してやりました．ブログや YouTube もありますが，JJMO・JMO 関連はたいてい問題の解説なので，数Ⅰ・数Ⅱの基礎固めのために活用するのがよいと思います．

どんな書籍や動画がよいかは，数学好きや体験者のブログなどに情報があるので，ぜひ探してみて下さい．探しているうちに，いろいろな情報を吸収して未知の世界だった高校数学の全体像が見えてきます．そして「こんなのもあるんだ？やっておこう.」と，どんどんやる気が増します．評判のよい参考書でも自分に合わないと思ったら，すぐに違う物に替えました. JJMO 用の書籍はほとんどないため，実際には JMO レベルの問題集をやることになるので，それぞれの実力や好き嫌いで，いろいろ試すのがよいと思います．

<問題のレベルを知ろう>

予選は 3 時間で 12 問を解くのですが，全国で上位 100 人位が予選合格となるため，年度によって合格点が違います. 7 点~ 8 点以上取れたらだいたい合格です.

開成・筑駒・灘などの全国の数学猛者たちとともに 100 人に入るには，問題のレベルを知って，時間をうまく使うことです.

① 問 1～問 5　　ミスせずに確実に正解しておく
② 問 6～問 8　　やや難しいが確実に 2 問以上を正解できれば合格の可能性あり
③ 問 9~問 10　　かなり難しいが解けることもあるので，時間があればチャレンジ
④ 問 11～問 12　恐ろしく難しいので，まず手をつけないほうがよい

これはあくまで私の体感です．年度で難易度も変わるので自分で試してください．

<くじけそうになっても>

中 1 で高校数学を独学でやるので，最初は迷宮をさまよっているような感じでした．しかし，だんだん解ける問題が増えると楽しくなりました．ところが，JJMO の勉強で困るのは，私には難しすぎてモチベーションが保てなくなること．もしくは，解けたのにくだらない計算ミスでテンションがガタ落ちしてやる気が 0 になることです.

そこで，最後の半月は「抽選箱方式」で気分転換していました．問題集をコピーして 1 問ずつバラバラに切ってクッキーの空き缶に入れ，ドラフトの抽選箱みたいに手を突っ込ん

で取り出した問題をやる方式です．ちなみに，解けた問題は捨てて，解けなかった問題は缶に戻すので，だんだん中身が減っていくので，実力が可視化できて楽しいです．

<会場でのハプニング>

東京の予選会場は中央大学と早稲田大学だったのですが，私たちは早稲田大学の教室でした．１月にもかかわらず暖房が効きすぎて，真夏日か？と思うほど暑かったです．慣れている人はＴシャツでした．

先輩から暑いと聞いてはいたのですが，そこまでとは思わず，長そでシャツにトレーナー，スパッツにスカートの重ね着でしたが，あまりの暑さに「これで 3 時間は集中できない!」と試験直前にトイレに駆け込み，脱げるものは脱いで，最終的にシャツとスカートにハイソックスを下げるという，まるでリビングでくつろぐような格好になって，なんとか集中できました．もしあのままなら暑さで合格できなかったと思います.(途中でトイレに行くことは可能ですが，時間に余裕がなくなるかも.)

本選会場も早稲田大学の建物でしたが，大学の敷地外にあり，当日は大学受験の厳戒態勢で閉門していて，迷って守衛さんに尋ねる人がかなりいました．本選会場は温度も心地よく，ゆったりした雰囲気でした．机に飲み物をいっぱい並べている人もいたし，同じ机の人は試験開始と同時に余裕でサンドイッチを食べていました.（試験官に注意されていませんでした．ただし JMO の会場では飲み物以外は注意されていたそうです.）

ちなみに，本選問題は予選とはケタ違いに難しいです．私は本選の練習までできなかったので，なんとか 1 問書きましたが，まるでスニーカーでエベレストに登るようでした．

<昨年の問題からアドバイス>

2020 年の JJMO 予選問題の問 2 について，ちょっとアドバイスです．

> a,bを正の整数とする．a以上b以下の整数をすべて足すと2020であるような(a,b)の組のうち，aが最も小さいものを求めよ．

この問題，簡単なのですが，ネット上の口コミでは「答えを書き間違えた!」という人が多かったそうです．私も答えを書くときに，一瞬間違えそうになりました．

> 答えは$(\boldsymbol{a},\boldsymbol{b})=(\mathbf{31},\mathbf{70})$なのですが，$\boldsymbol{a}=\mathbf{31}$と書いてしまった人が多かったらしいのです．

落ち着いて全体を読めば「(a,b)の組のうち」なので「組」が問われているとわかるのですが，求めていくうちに問題文の最後の「aが最も小さいものを求めよ.」につられてaだけ答えてしまうという読み間違えをしたケースです．

数学オリンピック関連の問題を解いていると，数学では当たり前なのかもしれませんが

「ん？」と一瞬戸惑うような言い回しの問題文に時々出会います．外国の大会の過去問を日本語に訳した問題などはけっこう戸惑います．できるだけたくさんの問題にチャレンジして慣れておくとよいと思います.

<最後に>

　これを読んでくれた後輩や小学生のみなさんは，私よりずっと優秀だと思うので，この体験記が参考になるかはわかりませんが，少しでも JJMO の雰囲気が伝わって，あきらめずに楽しく勉強をしてもらえたら嬉しいです．残念ながら今年の JJMO はコロナの影響で中止となりましたが，次の機会までみんなで数学を楽しみましょう!

第２章

世の中を支える数学

＜はじめに＞

数学は役に立つでしょうか．ドキュメンタリーで時々取り上げられている，ある分野や特定の問題に人生を捧げている数学者の方々を見て，世の中に直接役に立つことをしているわけじゃないのに何で人生を捧げられるのだろう，と思ったことはありませんか．正直に言って，私も昔はそう思いました．しかし，数学はとても役に立つのです．そういわれても具体的な想像は難しいでしょう．そこで今やこの世界中を支えている通信技術とそれに大きく関わる数学の定理，フェルマーの小定理について書きたいと思います．

この記事では次の四部構成で行きたいと思います．

１．フェルマーの小定理とは
２．フェルマーの小定理の証明１
３．フェルマーの小定理の証明２
４．フェルマーの小定理と RSA 暗号

１．＜フェルマーの小定理とは＞

1.1　フェルマーの小定理の内容

pを素数とし，aを任意の自然数とするとき

$$a^p \equiv a \bmod p$$

特にaとpが互いに素な自然数のとき

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

という定理のことです．

1.2　補足知識

・互いに素

ある二つの整数があって，それらが共通の素因数を持っていないとき
その二つの整数は互いに素であるといいます．

Ex）$21 = 3 \cdot 7, 40 = 2^3 \cdot 5$より共通の素因数を持っていないので
21 と 40 は互いに素．

・合同式

ある整数a, b, nがあって，aをnで割った余りがbをnで割った余りと等しいとき

$a \equiv b \bmod n$ と表します．　　Ex）$10 \equiv 40 \bmod 6$

・合同式の加減乗除

両辺に加法，減法，乗法を行っても合同式は成り立ちます．つまり，加法，減法，乗法は通常通り行えるということです．

Ex）$10 \equiv 40 \bmod 6 \Rightarrow 10 \pm 2 \equiv 40 \pm 2 \bmod 6$，$10 \cdot 2 \equiv 40 \cdot 2 \bmod 6$

除法は割る数に注意が必要です．$a \equiv b \bmod n$の両辺を整数mで割るとき, nとmが互いに素であるならば合同式が成り立ちます.

Ex) $10 \equiv 40 \bmod 6 \Rightarrow 10 \div 5 \equiv 40 \div 5 \bmod 6$，$10 \div 2 \not\equiv 40 \div 2 \bmod 6$

・二項定理

$(x+a)^n = \sum_{k=0}^{n} {}_nC_k a^k x^{n-k}$　　（$\sum$を習った高校生向けの表現）または

$(x+a)^n = {}_nC_0 a^0 x^{n-0} + {}_nC_1 a^1 x^{n-1} + \cdots + {}_nC_{n-1} a^{n-1} x^1 + {}_nC_n a^n x^0$　（未修者向け）

※${}_nC_k$はn個の中からk個を取り出す組み合わせの数です.

つまり二項定理は，$(x+a)^n$を降冪の順に展開した時の各項の係数が${}_nC_k$になると主張しているのです.

（$\sum$は, kを 1 からnまで 1 ずつ動かしてその式をすべて足し合わせる記号です.）

２．＜フェルマーの小定理の証明１＞※不完全

※ここではaとpが互いに素である場合に限って証明をします．こちらの方が理解しやすいでしょう.

補題「$a, 2a, 3a, \cdots, (p-1)a$を$p$で割った余りはすべて異なる」を証明します.

証明の方針…背理法によって導きます.

[証明]

$a, 2a, 3a, \cdots, (p-1)a$を$p$で割った余りが等しいものが少なくとも一組存在すると仮定する.

その組を$ia, ja (i > j)$とすると，$(i-j)a$もpの倍数となる.

しかし$1 \leq i-j < p$であり，かつaとpは互いに素であるのでこれは成り立たない.

最初の仮定が誤っているので$a, 2a, 3a, \cdots, (p-1)a$を$p$で割った余りはすべて異なる.

・フェルマーの小定理の証明

[証明]

補題より, aとpが互いに素な場合は$a, 2a, 3a, \cdots, (p-1)a$は全て$p$の倍数ではないので，その余りは$1, 2, 3, \cdots, p-1$までがすべて一回ずつ出てくる.

よって

$a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a \equiv (p-1)! \bmod p$

$(p-1)!\,a^{p-1} \equiv (p-1)! \bmod p$

ここで$(p-1)!$はpと互いに素であるから

$a^{p-1} \equiv 1 \bmod p$ （終）

3．＜フェルマーの小定理の証明２＞

証明の方針…数学的帰納法によって導きます.

[証明]

まず$p=1$のとき，明らかに$a^1 \equiv a \bmod 1$

次に，仮にpでこれが成り立つとき（$a^p \equiv a \bmod p$が成り立つとき）

$p+1$でも成り立つかを確認する.

二項定理より（xに 1 を代入）$(a+1)^p = a^p + \sum_{k=1}^{p-1} {}_pC_k a^k + 1 \equiv a^p + 1 \bmod p$

（${}_pC_k = p(p-1)\cdots(p-k+1)/k!$より，$\sum_{k=1}^{p-1} {}_pC_k a^k$は$p$の倍数であることから.）

よって$a^p \equiv a \bmod p$が成り立つとき，$(a+1)^p \equiv a+1 \bmod p$も成り立つ.

従って全ての整数pについて$a^p \equiv a \bmod p$が成り立つ.

またaとpが互いに素であるとき両辺をaで割れるから

$a^{p-1} \equiv 1 \bmod p$ （終）

4．＜フェルマーの小定理と RSA 暗号＞

4.1　公開鍵暗号方式

暗号の基本的な仕組みを説明します.

受信者…公開鍵k_1（メッセージを送る時，暗号化にこれを使うようにと公開）

秘密鍵k_2（自分しか知らない復号用の鍵）を用意します.

（手順１）　送信者がメッセージmと公開鍵k_1で$f(m, k_1)$を作り送信

※$f(m, k_1)$とk_1からでは復号できないようにします.

（手順２）　受信者が$f(m, k_1)$と秘密鍵k_2から復号

※当然$f(m, k_1)$とk_2からは復号できなければなりません.

この方法は公開鍵を使っても秘密鍵がわからなければ復号できないのでセキュリティ上の問題はありませんが，※の条件二つを満たすような状況を作ること自体が難しいです．そのような状況を作り出すためには暗号化のための素数と復号のための数学が必要なのです.

4.2　補足知識の説明と証明

ここからの話の理解には合同式（参照：1.2 補足知識）とフェルマーの小定理, そして次に説明する定理の理解が必要です.

定理：整数mとnが互いに素であるとき, $mx \equiv 1 \bmod n$となるxが
$1 \leq x \leq n-1$ の範囲に必ず一つだけ存在する.
（以降フェルマーの小定理と区別し定理 1 とします）

証明の方針…フェルマーの小定理の証明 1 で示した補題から導きます.

[証明]

補題「$a, 2a, 3a, \cdots, (p-1)a$を$p$で割った余りはすべて異なる」より, $m, 2m, 3m, \cdots, (n-1)m$は全て$n$の倍数ではないからその余りは$1,2,3, \cdots, n-1$が一回ずつ出てくる．よって$m, 2m, 3m, \cdots, (n-1)m$のなかに余りが 1 のものがただ一つ存在するので,
$1 \leq x \leq n-1$ の範囲で$mx \equiv 1 \bmod n$となるxがただ一つ存在する.　　（終）

4.3　RSA 暗号の仕組み

・受信者の準備

1. 大きな素数（※）pとqを定めて$t = pq$とします.
2. $(p-1)(q-1)$と互いに素な整数k_1をとって公開鍵とします.
3. $k_1 k_2 \equiv 1 \bmod (p-1)(q-1)$となる$k_2$を定めて秘密鍵とします.
（定理 1 より, mをk_1, nを$(p-1)(q-1)$, xをk_2とすれば）
$1 \leq k_2 \leq (p-1)(q-1)$ の範囲でk_2がただ一つに定まります.

・送信者

送りたいメッセージs（$0 \leq s < t$）と公開鍵で$s^{k_1} \bmod t$を計算し暗号文Aとして送ります.

・受信者

送られてきた暗号文と秘密鍵k_2で$A^{k_2}\ mod\ t$ を計算するとこれが送られたメッセージsとなります.

※大きな素数を 150～300 桁として掛け合わせると, 現在の技術ではtからpとqを求めるのに何億, 何兆年とかかるようです. 現在分かっている最大素数は 24,862,048 桁なので 150～300 桁の素数など数えきれないほど見つかるでしょう.

4.4　RSA 暗号が成り立つことの証明

なぜこの操作で元のメッセージがわかるのでしょうか．その証明をしてみます．

[証明]

$(s^{k_1} \bmod t)^{k_2} \equiv s \bmod t$ を証明したい．

$(s^{k_1 k_2} \bmod t) \equiv s \bmod t$より$s^{k_1 k_2} \equiv s \bmod t$を示せばよい．

（modの操作を既に行ったものにmodの操作をしても答えは変わらないので.）

$t = pq$より，$\bmod p$（またはq）だけ示せばよいので$s^{k_1 k_2} \equiv s \bmod p$を示す．

sによって場合分けをする．

・sがpの倍数である場合

両辺ともpの倍数になるので明らかに成り立つ．

・sがpの倍数ではない場合

$k_1 k_2 \equiv 1 \bmod (p-1)(q-1)$ から，$k_1 k_2 - 1$が$p-1$の倍数であるので整数Nを用いて

$k_1 k_2 - 1 = (p-1)N$, $k_1 k_2 = 1 + (p-1)N$と表せる．

フェルマーの小定理より

$$\mathrm{s}^{k_1 k_2} = s^{1+(p-1)N} = s\left(s^{(p-1)N}\right) = s(s^{p-1})^N \equiv \mathrm{s} \cdot 1^N \bmod p$$

よって $$\mathrm{s}^{k_1 k_2} \equiv \mathrm{s} \bmod p$$

（終）

4.5　素数と RSA 暗号

RSA 暗号は現代の通信技術の要ともいえるアルゴリズムですが，将来的には使えなくなるかもしれません．なぜなら大きな数の素因数分解が簡単にできると受信者と同じ手順を踏んで RSA 暗号は簡単に破られてしまうからです．

将来コンピュータの性能が向上したりそれに関する数学的な発展があったりすれば RSA 暗号は使えなくなってしまいます．

＜あとがき＞

今回の文化祭は早実生だけで行われるということで，見る人が少ないのなら中学一年生から高校三年生までわかる文章にしようと思って書き始めました．そのはず，なのですが実際はそうなっておらず自分の文章力を嘆きました….

ところで，数学が生活の支えになっていることが感じられたでしょうか．フェルマーの小定理も数百年前は数学の最先端でした．今の数学の最先端もいつか中学生が記事を書き目に見えて世の中を支える時が来るでしょう．数学が身の回りのすぐ近くにあることを感じてもらえれば嬉しいです．拙い文章でしたが最後まで読んでいただきありがとうございました．

＜参考＞

高校数学の美しい物語

東京都市大学自然科学科　数学領域

（NHK スペシャル『魔性の難問～リーマン予想・天才たちの闘い～』）

※この記事は自分の言葉で書きましたが，暗号の仕組みなど既存の情報と内容が似通っているものがありました．

OB の先輩にも
書いていただきました！

コラム 1

数研 OB より

初めまして！数研で 2 年間部長を務めておりました W.T.といいます．ここでは，私が OB 目線で数研の今までの歩みを振り返っていきたいと思います．たくさん書いてください！とお願いされたので，ちょっと長くなりますが時系列順にみていきましょう．

2005 年　初代　数学研究同好会設立

実は，数学研究同好会は以前にもあったそうです．しかし，その後部員数が減ってしまい，消滅してしまったと先生から聞きました．

2015 年　“数学研究会”設立

この年の秋，当時の高 2 生（現・大 3）を中心に有志団体“数学研究会”が発足します．
当時はまだ，中学生は私と後輩 1 人で，中高合わせても 10 人弱でした．数学が好きな人が集まって，話し合ったり問題を解いたりする場所が生まれたのはこの時でした．私は当時中 2 でしたが，アットホームな雰囲気で，先輩たちからいろいろな数学の内容を教えてもらいました．数研はこの時から数学甲子園や数学オリンピックにも参加していたので，これらの対策もみんなで行っていました．数オリ予選通過者も出ました！

2016 年　文化祭に初めて参戦！

16 年から，数研の文化祭での出展が始まります．展示の他に数学体験コーナー，部誌，黒板での問題コーナーなどを作りました．「多くの人に数学の面白さを伝えたい！」というモットーはこのころからずっと変わっていません！
文化祭以外では，「解析概論」の輪講などが行われていました．大学で勉強する分野を，みんなで勉強する，というものです．当時の私はあんまり理解できなかった記憶があります．そして，設立メンバーの大半を占めていた当時の高 3 生が卒業してしまいます．

2017 年　数研史上最大のピンチ？

実は，数研に参加していた人の学年が偏っていたために，ピンチが訪れます．まず，人数が少ない！ということ．新入生含めてメンバーは 6，7 人ぐらいで，活動日によっては 2，3 人しかいないということもよくありました．こうして当時高 1 の私，中 3 の後輩が中心となる新たな世代が心配な形でスタートしました．前年度の活動を真似して，なんとか

文化祭にも出展し，後輩と対策して数学オリンピックにも参加しました．この年はジュニアと合わせて 2 人が予選通過しました！

2018 年　有志団体“数学研究会”から“数学研究同好会”に昇格！！

そして，4 月に転機が訪れます．数研が正式に同好会として認められたのです！これは顧問の先生をはじめとする，先生方のおかげです．本当に嬉しかったです．新入生も入り人数も増えて，また正式に同好会になったこともあり，活動の幅が広がっていきます．前年は出場をあきらめた数学甲子園の予選に参加し，稲門ジュニア(早稲田大学附属・系属中高の研究発表会)での発表，さらに早稲田中高数学研究同好会との合同数研も開催しました．実は文化祭での部誌の発行部数が年々すごく増えていたり，入試予想問題の配布も始まったりしています．

2019 年　さらに飛躍の一年

さらに新入生が入り，この年初めて，全学年に部員がいる！という状態になります．文化際の展示スペースが広くなったり，数オリ，ジュニアで予選通過者が計 4 名出たりと実績もどんどん上がっていった一年だと思いました．２回目の合同数研も行われ，部活動の運営に関しても情報の交換が行われました．久しぶりに解析ゼミもすることができました．数研のウェブサイトも立ち上げましたね．

2020 年　さらににぎやかな数研

卒業後に数研で講義をした時の印象は，「人が多い！にぎやか！」というものでした．これは本当にいいことです．なぜならばたくさん人がいればできることが増えるからです．文化祭はオンラインでの開催となったり，コンテストが中止になったりと大きく変わったところはありますが，活動の本質は変わらないと言えます．

振り返ってみれば，数研はたくさんの人のおかげで成り立ってきました．そして基本的な創設時のスタイルを維持しながら，新たにできることを見つけて積極的にチャレンジしてきまし．そして人数が増え部活自体が成長してきたことを改めて実感します．今後の数研の活動も楽しみですね．
以上で OB による数研振り返りコーナーは終わりにしたいと思います．お読みいただき，ありがとうございました．

第３章

証明を考える

１　はじめに

この記事では，証明(幾何)を考えていきたいと思います．その中で数学の面白さをお伝えできればと思います．この記事では個人的に好きな定理(2 つ)を取り上げていきます．

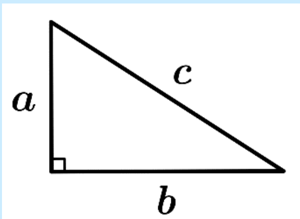
２　三平方の定理（ピタゴラスの定理）

定理

直角三角形の直角をはさむ 2 辺の長さを a，b，斜辺の長さを c とすると，

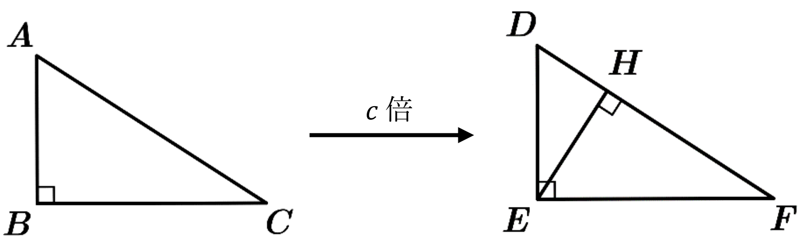
$$a^2+b^2=c^2$$

が成り立つ．



超有名な定理ですね．証明方法は相当な数があります．ここでは自分の好きな証明を 2 つ紹介していきます．

（証明１）



$\angle B=90°$の直角三角形ABCにおいて，$AB=a$，$BC=b$，$AC=c$とおく．

$\triangle ABC$を c 倍拡大する(これを$\triangle DEF$とする)．EからDFに垂線をひき，その足をHとする．

$\triangle DEF$と$\triangle EHD$において

$\angle DEF = \angle EHD = 90°$（∵仮定）

$\angle EDF = \angle HDE$（∵共通）

∴ $\triangle DEF \backsim \triangle EHD$

∴ $DF : ED = DE : DH$

∴ $c^2 \cdot DH = a^2c^2$

∴ $DH = a^2$ …①

また，$\triangle DEF$と$\triangle EHF$において

$\angle DEF = \angle EHF = 90°$（∵仮定）

$\angle DFE = \angle EFH$（∵共通）

∴ $\triangle DEF \backsim \triangle EHF$

∴ $DF : EF = EF : HF$

∴ $c^2 \cdot HF = b^2c^2$

∴ $HF = b^2$ …②

①と②を辺々足して

$DH + HF = a^2 + b^2$

$DF = a^2 + b^2$

∴ $a^2 + b^2 = c^2$

よって，示された．□

垂線を引き，相似を用いて示す，というかなり有名なものです．この方法では$\triangle DEF$を登場させましたが，登場させなくてもきれいに示せます．これを紹介したのは完全に私の好みだからです(笑). 2 乗ということで，（内項の積）＝（外項の積）を使うというイメージですね.

さて，今度の証明は知らない方も多いのでは？(発見されたのが 2015 年ですしね.）

（証明２）

$\angle B = 90°$の直角三角形ABCにおいて，BC上に中心Oがあり，点PでACと接しているOBを半径とする内接半円を考える．$AB = a,\ BC = b, AC = c, OB = r$とおく．

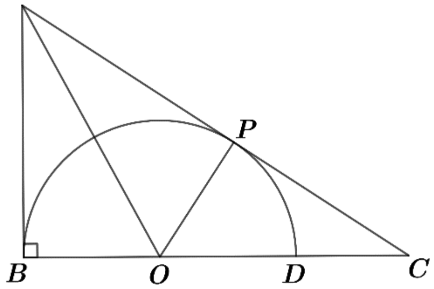
$CP = c - a,\ CD = b - 2r$

$\triangle OPC \backsim \triangle ABC$

∴ $OP : PC = AB : BC$

$OP = \frac{PC \cdot AB}{BC}$

$r = \frac{(c-a)a}{b}$ …①



また，方べきの定理により$CP^2 = CD \cdot CB$

$(c-a)^2 = (b-2r)b$

$r = \frac{b^2-(c-a)^2}{2b}$ …②

①，②より$\frac{(c-a)a}{b} = \frac{b^2-(c-a)^2}{2b}$

$\therefore\ a^2 + b^2 = c^2$

よって，示された．□

美しいですね．内接半円を使って証明する，というのがまた面白いです．

3　ちょっと休憩　1 = 2の証明【問題編】

いわゆる偽証というやつです．間違いが含まれている証明ですね．みなさん間違いを探してみてください．結構偽証を見破るのが難しいものもあるかも？

（証明１）

$0 = 0$

$0 \div 1 = 0, 0 \div 2 = 0$であるから

$1 = 2$　□

（証明２）

$a = b$とする．

両辺にaをかけて

$a^2 = ab$

両辺からb^2をひいて

$a^2 - b^2 = ab - b^2$

$(a+b)(a-b) = b(a-b)$

両辺を$a-b$で割って

$a + b = b$

$a = b$であるから

$2a = a$

両辺をaで割って

$2 = 1$

両辺を入れ替えて

$1 = 2$　□

（証明３）

背理法で示す．

$1 \neq 2$であると仮定する．

両辺に0をかけると

$0 = 0$

となり，これは$1 \neq 2$であることと矛盾．

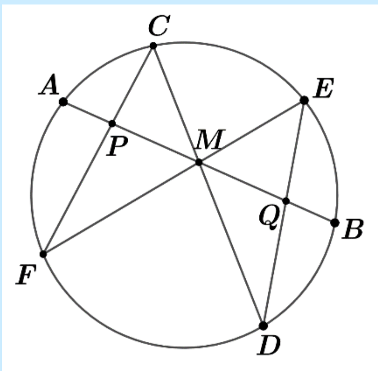
$\therefore\ 1 = 2$ □

さて，見つかりましたか？解答はまたあとで．

4　胡蝶定理

定理

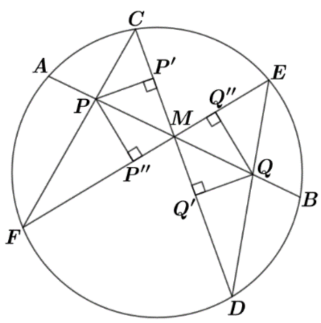
弦ABの中点をMとする．Mを通る２つの弦CD，EFをC，EがABに対して同じ側にあるようにひき，CF，DEがABと交わる点をそれぞれP，Qとする.このとき，MはPQの中点である．



綺麗な定理ですね．上の図のように蝶の形に見えるので胡蝶定理と呼ばれます．この定理を証明していきましょう．

（証明１）

PからCD，EFにおろした垂線の足をそれぞれP'，P''，QからCD，EFにおろした垂線の足をそれぞれQ',Q''とする．



$\triangle MP'P$と$\triangle MQ'Q$において

$\angle MP'P = \angle MQ'Q = 90^\circ$（∵仮定）

$\angle P'MP = \angle Q'MQ$（∵対頂角）

$\therefore\ \triangle MP'P \backsim \triangle MQ'Q$

$\therefore\ \frac{MP}{MQ}=\frac{MP'}{MQ'}$

同様に$\triangle MPP''\backsim\triangle MQQ''$

$\therefore\ \frac{MP}{MQ}=\frac{MP''}{MQ''}$

$\triangle CPP'$と$\triangle EQQ''$において

$\angle CP'P=\angle EQ''Q=90°$（∵仮定）

$\angle PCP'=\angle QEQ''$（∵円周角の定理）

$\therefore\ \triangle CPP'\backsim\triangle EQQ''$

$\therefore\ \frac{PP'}{QQ''}=\frac{CP}{EQ}$

同様に$\triangle FPP''\backsim\triangle DQQ'$

$\therefore\ \frac{PP''}{QQ'}=\frac{FP}{DQ}$

以上より

$$\left(\frac{MP}{MQ}\right)^2=\frac{MP'}{MQ'}\frac{MP''}{MQ''}$$

$$=\frac{CP\cdot FP}{EQ\cdot DQ}$$

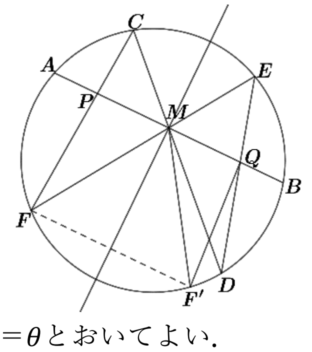
$$=\frac{AP\cdot BP}{AQ\cdot BQ}\text{（∵方べきの定理）}$$

$$=\frac{(AM)^2-(MP)^2}{(AM)^2-(MQ)^2}$$

$\therefore\ MP=MQ$

よって，示された．□

なかなか思いつきにくい気がします．比をうまく使えればという感じで，高度な気がしますね(私はこの証明，見るまで思いつきませんでした)．



（証明２）

ABの垂直二等分線に関してFと対称な点をF'とする．

$\triangle PFM$と$\triangle QF'M$において

対称性から$PF=QF'$ …①

$\angle PFM=\angle QMF'$ …②

FF'はABに平行であるから$\angle AMF=\angle MFF'=MF'F=\angle F'MB=\theta$とおいてよい．

$FF'DE$は共円である．

$\therefore\ \angle F'DE = 180° - \angle F'FE = 180° - \theta$

$\angle F'DQ + \angle F'MQ = 180°$がわかるので，$F'DQM$は共円．

$\therefore\ \angle MF'Q = \angle MDQ = \angle MFP$ …③（∵円周角の定理）

$\therefore\ \triangle PFM \equiv \triangle QF'M$　（∵①，②，③）

$\therefore\ PM = QM$

よって，示された．□

先ほどの証明よりは思いつきやすいと思います（$PM = QM$を示したい→どこか合同な図形がないか，という感じで）．私もこの方法で示しました．自分でとった，たった 1 個の点，線によって見える景色がガラッと変わり，新たな発見ができるのも幾何の醍醐味ですね．

5　ちょっと休憩　1＝2 の証明【解答編】

（証明１）

関数$y = \frac{0}{x}$のグラフをかいてみれば，すぐにわかります．

そう！ざっくりいうとy軸の値が等しい$\Rightarrow$ x軸の値も等しいという主張をしているんです．むちゃくちゃですね（対偶が二次関数等のときに成り立たないですから）．

（証明２）

0で割ってしまっています($a-b$で割っている)．0除算はやってはいけません．説明は 2018 年の部誌のはじめの方にこれについての先輩の記事が載っていますのでそちらをご参照ください．

（証明３）

$\neq$と$=$を一緒のようにとらえています．$A = B \Rightarrow AC = BC$は成り立ちますが，$A \neq B \Rightarrow AC \neq BC$は成り立ちません．$A \neq B \Rightarrow AC \neq BC$が成り立つということで仮定を否定しているのでこれが間違いですね．

偽証のどこが間違っているのかを考えてみると，結構頭を使えて勉強になると思います．

6　証明について

①別証を考えること，②個人的に思うことの 2 点について書こうと思います．

まず，①について．別証を考えることは，考える力が付きますし，別証を考えることで違った見方ができていいことだらけです．数学の奥深さも味わえると思います．

②について，範囲を絞ったり，幾何だったら図を描いてみたり，そうだとしたら何が成り

立つのか考えたりします．だいたい，わからないものが見えてくる→わからないことに気づく→またわからないものが見えてくる→わからないことに気づく…という感じになりますが，頭を使って考える楽しさは証明問題の方が味わえると思います（個人の感想です．私は頭使ったら使った分，証明できた／気づいたときの感動が大きくなるので）．証明か…と敬遠することなく，爽快感を味わってほしいです（数学オリンピック・ジュニア数学オリンピックなどを調べれば様々な問題が出てくるはずです）．ぜひ数学好きな方も，そうでない方も！

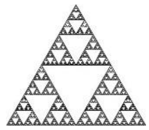
7　まとめ

いかがでしたか？説明不足やあいまいな点も多かったとは思いますが，少しでも面白いと感じていただけましたか？

私自身，そう数学を理解しているわけでもなく，すらすらできませんが，その分証明など，自分の頭で考えて（人より遅くても）新しいことに気づくときの嬉しさ・爽快感が，モチベーションになっている気がします．この文章・ひいてはこの部誌で一人でもより数学の楽しさに浸っていただければ，それはこの上なく嬉しいことです．そうなることを祈っています．最後の最後まで（拙い文章でしたが）読んでいただき，ありがとうございました！

第4章

$\sqrt{2}$ は無理数？



はじめに

$\sqrt{2}$ が無理数であることは皆さん知っていることだと思います．学校でも「背理法」を用いた証明を習うでしょう（下記参照）．しかし，背理法を用いなくても証明はできないのかと疑問に思ったことはありませんか？そこで，ここでは背理法以外の証明を考えていきます．

＊背理法による証明

教科書にも載っていて一番有名な証明です．

[証明]

$\sqrt{2}$が有理数であると仮定する．

このとき，互いに素な正の整数p, qを用いて$\sqrt{2} = \frac{q}{p}$とおける．

両辺二乗して分母を払うと，$2p^2 = q^2$

左辺は2の倍数なのでq^2は2の倍数．よってqは2の倍数．

すると，q^2は4の倍数になるので，p^2が2の倍数．よってpも2の倍数．

これはpとqが互いに素であることに矛盾．

＊背理法以外の証明

① 素因数分解を用いた証明

まず始めに，素因数分解を使った証明です．

[証明]

$\sqrt{2}$が有理数$\Leftrightarrow \sqrt{2} = \frac{a}{b}$を満たす整数$a, b$が存在する

なので,

$a^2 = 2b^2$を満たす整数a, bが存在しないことを証明すればよい．

a, bを素因数分解したときの2の指数（2で何回割り切れるか）を考えることで,

左辺は2で偶数回，右辺は2で奇数回割り切れることになる．つまりそのような整数a, bは存在しない．

② 二次方程式を用いた証明

この証明では，下の定理を使います．

「(整数係数多項式）=0 の形の方程式が有理数解$\frac{q}{p}$（既約分数）を持つなら，pは最高次の係

数の約数でqは定数項 の約数である.」

この定理がなぜ成り立つのか気になった方は，証明を調べてみてください.

[証明]

$x^2-2=0$という二次方程式を考える.

・$\sqrt{2}$はこの二次方程式の解である.

・この方程式に有理数解があるとしたら，それは「(整数係数多項式）=0 の形の方程式が有理数解$\frac{q}{p}$（既約分数）を持つなら，pは最高次の係数の約数でqは 定数項 の約数である.」という定理より$\pm1,\pm2$のいずれかだがどれも解でない.

以上により$\sqrt{2}$は無理数.

③ 正則連分数展開を用いた証明

最後に，「有理数⇔正則連分数展開が有限回で終了する」という定理を使って証明します.（補足参照）

[証明]

$\sqrt{2}$の正則連分数展開は$\sqrt{2}=[1;2,2,2,\cdots]$と無限に続く（※）ので「有理数⇔正則連分数展開が有限回で終了する」という定理より$\sqrt{2}$は無理数である.

※

・$\sqrt{2}$の整数部分は1，小数部分は$\sqrt{2}-1=\frac{1}{\sqrt{2}+1}$より，

$$\sqrt{2}=1+\frac{1}{\sqrt{2}+1}$$

・$\sqrt{2}+1$ の整数部分は2，小数部分は$\sqrt{2}-1$より

$$\sqrt{2}=1+\frac{1}{2+\frac{1}{\sqrt{2}+1}}$$

以下この操作が無限に続く.

$$\sqrt{2}=1+\frac{1}{2+\frac{1}{2+\frac{1}{2+\cdots}}}=[1;2,2,2,\cdots]$$

まとめ

「$\sqrt{2}$が無理数である」という簡単そうなことでも，証明方法はたくさんあります. 物事を違った視点から考えることは大切ですね.

補足

分数の分母にさらに分数が含まれている分数を連分数と言います.
特に，分子の部分がすべて1で，分母の部分がすべて自然数である連分数を正則連分数といいます．また，

$$\frac{y}{x} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

のような式変形を有理数$\frac{y}{x}$の正則連分数展開といいます.

ここで話は変わりますが，
aをbで割った商をp，あまりをqとすると，

$$\frac{a}{b} = p + \cfrac{1}{\cfrac{b}{q}}$$

となります.

つまり，$\frac{a}{b}$を正則連分数展開するには$\frac{b}{q}$を正則連分数展開すればよい，ということになります.

このように，aとbの問題をbとqの問題に帰着させるというのはユークリッドの互除法の考え方と同じです．ユークリッドの互除法は有限回で終了するので，有理数なら正則連分数展開は有限回で終了します.
こうして，「有理数⇔正則連分数展開が有限回で終了する」という定理が成り立ちます.

コラム２

数研アンケート2020

K)「皆さんこんにちは．早稲田実業学校数学研究同好会所属のＫです．今回，部誌の企画の一環として数研部員たちに実施した「数研アンケート」の質問と個人的に面白いと思った回答を掲載しました，早い話が「わらしべ」の~~パクリ企画~~パロディ企画です．さっそく本題へ行きましょう.」

Q１　数学は好きですか？

K)「嫌いとか言われたら悲しいなぁ.」

回答

・ご想像にお任せします
・好きじゃない
　K)「・・・え？」

・もちろん！
・はい
　K)「まともな回答があってよかった.」

・う（原文ママ）
　K)「一体何があったんだ.」

Q２　好きな数は？

回答

・0655 , 2355
・1293
・一不可説不可説転
・33550336
・加藤一二三

K)「なんだこの数・・・？と思っている読者の方も多いと思いますが・・・・，

理由を聞くのを忘れてしまったので，

何を意味するか（なぜその数が好きなのか）

僕もわかりません．

一応検索すると元ネタらしきものは出るので，気になった方は是非調べてみてください（責任放棄）.」

Q３　好きな数学の偉人は？

K)「とある人が部員の個人名を直接書いたせいでここに載せられないものがありました」

回答

・鈴木貫太郎

鈴木 貫太郎（すずき かんたろう，1868 年 1 月 18 日〈慶応 3 年 12 月 24 日〉- 1948 年〈昭和 23 年〉4 月 17 日）は，日本の海軍軍人，政治家．最終階級は海軍大将．栄典は従一位勲一等功三級男爵.

海軍士官として海軍次官，連合艦隊司令長官，海軍軍令部長（第 8 代）などの顕職を歴任した．予備役編入後に侍従長に就任，さらに枢密顧問官も兼任した．

出典:フリー百科事典『ウィキペディア（Wikipedia)』
URL:https://ja.wikipedia.org/wiki/%E9%88%B4%E6%9C%A8%E8%B2%AB%E5%A4%AA%E9%83%8E

閲覧日時:2020 年 9 月 28 日 20 時 40 分

K)「上の名前を見てこの人以外を想像した人は多分かなりの数学マニア」

・モリアーティ（シャーロックホームズのライバル．数学の教授）

K)「上の一つ前のやつもそうですけど，元ネタ知ってる人ってどのくらいいるんでしょうね?」

・カラテオドリ

K)「初めてこの回答見たとき存在するのかどうかも知らなくて，調べたら本当に実在していてすごく驚きました.」

・オイラーさん

K)「偉人の方に対しても敬語を忘れないとはなんて礼儀が整った後輩なんだ!」

その他多数回答

Q４　部を一言で表すと？

回答

・人種のサラダボウル

K)「意味が分からない・・・」

・チンダル現象

K)「もっと意味が分からない・・・」

・大きい塚

K)「さらに意味が分からない・・・」

・Δ

K)「もはや文字ですらない・・・」

・自由なところ

・ゆるさの象徴

K)「おそらく部員のほとんどはこのように感じていると思います．そのくらいゆるーく活動しています．そのせいで去年の文化祭は準備の時間が足りなくなり，当日の朝まで準備が終わらないという恐ろしいことになりましたが.」

Q５　部員はどんな感じ?

回答

・多様性

・多様性に満ちてる．ブラウン運動してる．

・ダイバシティー

K)「多様性に満ち溢れすぎだろ数研.」

・ALL 変人

K)「割と事実だから反論できない・・・. ちゃんと普通の人もいるのでご安心を. ~~と数研で一番の変人が言う~~」

・優しく強く頼もしい.

K) (TπT)ｱﾘｶﾞﾄｩ

Q6　好きな（興味のある）分野は？

回答

・微積（解析）

・微分積分

・統計

・確率

・幾何　整数

K)「やはり結構ばらけましたね. うちの部活ではナブラ演算子ゲームというものが流行っているのでそれの影響と一時期, 解析学について数研のみんなで学んでいたためか, 解析系のことに興味のある部員が多いような気がします.」

・閉回路

・因数分解

K)「僕の学力が欠如しているせいで本人たちがふざけて書いたのか, 真面目にこれらのことを書いたのかが分からない・・・」

Q7　好きな格言, 名言, ことわざ

回答

・「10 進法」という言葉は, 10 進法の世界に住む人からしか作られない.

K)「数弱の僕には言葉の意味が見ただけではあまり分からないので, わかる方がいたら教えてください.」

・3K 主義（not 三敬）（K：高学歴, 高身長, 高収入）

K)「早実に入って得られるとは限りません.」

・線分 EG を求めるのは easy.

K)「お, おう.」

Q８　みんなに自慢したいもの

回答

・銃撃ったことある（実弾）（ハンドガンとライフル）（ハワイで体験した）

K)「跳弾で自分に当たるんじゃないか？という懸念があるので銃撃つなんて僕には到底できないです.」

・算オリと数オリどちらも本選にでたこと

K)「算オリと数オリは面白い問題がたくさんあって楽しいし，本選まで出場するといいことがたくさんあるのでこれを見て興味を持った人は是非「すうけん」公式ホームページの「数オリ予選勉強法」を見てください！（露骨なステマ）．ちなみに僕は一回も本選に出場したことがありません.」

・特にない！

K)「すごく潔い」

Q９　今後の目標

回答

・面白い人になる

・億万長者！

・自分らしく生きていく.

・英検準二級

・アクチュアリー

K)「十人十色で様々な回答でした」

中にはこんな回答も

・高校進学

K)「留年するのだけはやめておけ（by マジで去年留年しかけた先輩）.」

Q 10　新入生に一言

K)「これが最後の質問です.」

回答

・よろしく

・趣味:ゲームとかより，唯一性があった方が覚えてくれるから一芸はもっとけ.

・僕が新入生です！

・健康で楽しい生活を送って下さい.
・気━つけろ
・音楽選択はやめておけ（高等部）
K)「最後の回答がかなり闇が深いですが，新入生の方は楽しい学校生活を過ごしてください！」

終わりに

K)「数研アンケート，いかがでしたでしょうか？ このような企画は数研でも初めての試みで何かと上手くいかないことが多かったですが，少しでも楽しんで頂けたらと幸いです.

実は元々この企画は僕以外にもう一人担当する人がいたのですが，その人が自分の記事にあまりにも時間がかかりすぎて実質僕一人でこのコラムを書くことになりました.

これからも「すうけん」をよろしくお願いします.」

〜終〜

第 5 章

確率変数を乱数で作る

＜はじめに＞

この記事には統計学の話が大いに含まれています．代数や幾何といった華やかな分野とは違い，特に中学高校の統計は単純かつ面倒な計算ばかりで面白くないと思う人も多いのではないでしょうか．さらに，統計学は数学ではないという専門家の方の意見も少なからず耳にします．しかしながら，奥が深い学問というのは統計学も例外ではないこと，また「数学」という道具をつかって幅広い分野で戦えることを，この拙い文章から理解していただけると幸いです．

＜なぜ乱数か＞

連続型確率変数は確率密度関数や**図 1** のようなグラフを使って表す事ができます（詳しくは高校数学 B の統計分野を参照すること）．確率密度関数を解析的に計算することで店の売り上げなどの予測ができるようになりますが，場合によっては計算が複雑になったりもしくは解くことが出来なかったりということが起こりえます．このようなときでも大量に乱数を使って統計的手法で解くことが可能です．これはモンテカルロ法と呼ばれています．例えばさいころの目の期待値を求めるとき，$(1+2+3+4+5+6) \div 6 = 3.5$というように計算するのが解析的手法であるのに対し，実際にさいころを何回も振ってみて出た目の回数を分析するのがモンテカルロ法です．

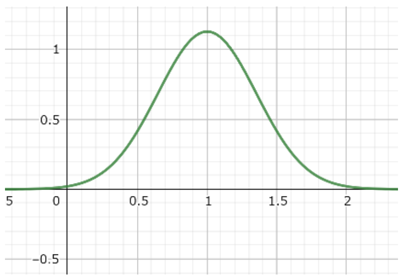


図 1

ただ，乱数によって確率分布を表現するのは一筋縄では行きません．連続型確率変数で 0 や 1 のようにきりの良い数だけではなく範囲内の実数ならばどんなものでも出現しうるし，**図 1** で言うならば 0.5 付近よりも 1 付近のほうの確率（密度）が高いといったように出現率が一定ではないのです．そのため単にさいころで出た数字を採用すると，さいころにある目の数字しか採用されず，さらにそれぞれの確率が一定になってしまいます．こういったことをどう解決し，確率変数として再現するかということを以下で解説します．

＜まず連続一様乱数を作る（読み飛ばしても構わない）＞

連続一様乱数は，a以上b未満（以下の場合もある）の任意の実数を等しくとる（密度が一定の）乱数です．これのもととなる連続一様分布は確率密度関数が

$a \leq x < b$で$f(x) = \frac{1}{(b-a)}$，それ以外の範囲では$f(x) = 0$と表されます．

これを完全に再現するというのは，正確な正方形を作ることと同じように不可能なので，これまでに様々な生成方法が考案されています．

今回は代表例として有名な線形合同法で作ります．線形合同法とは，前の整数に定数をかけたり足したりして自然数の定数Mで割ったものを次の整数とすることを繰り返す方法です．Mで割った余りなので0以上M未満の整数が等しい確率で出ることが期待できます．前の数をX_K，次の数をX_{K+1}とすると，

$$X_{K+1} = (pX_K + q) \bmod M \quad （p, q\text{は整数の定数，}M\text{は自然数の定数}）$$

と表せます．$p = 3$，$q = 0$，$X_K = 1$，$M = 10$として具体的に求めると，

$X_1 = (3 \times 1 + 0)\mathrm{mod}10 = 3$，$X_2 = (3 \times 3 + 0)\mathrm{mod}10 = 9$，$X_3 = (3 \times 9 + 0)\mathrm{mod}10 = 7, \cdots$

となり，$3, 9, 7, 1, \cdots$というような値がとれます．しかしこれはたった 4 つの数字でパターン化しているため，一様乱数として適しているとは言えません．実際はパターンの周期が長い数の組み合わせで乱数の理想に近づいたものを作ります．これらの数値をMで割ってから$(b-a)$をかけ，aを足すと$a \leq x < b$が範囲の連続密度関数を再現できます．

＜一様乱数から一般の確率変数を作る＞

一様分布以外の確率分布を乱数で表すには，基本的に一様乱数を加工して再現する必要があります．今回は変数に応じた生成法をいくつか紹介します．

〇逆関数法

逆関数法とは，分布関数$F(x)$をもとに，0以上1未満の一様乱数Uを加工して$U = F(x)$，つまり$F^{-1}(U) = X$となる確率変数Xを求める方法です．$F(\alpha) = \int_{-\infty}^{\alpha} f(x)dx$となるような分布関数$F(x)$をだすと，$F(\alpha)$の値から確率分布を大きさごとに並べた時に小さい方からどのくらいにあるかということが分かります．例えば$F(\alpha) = 0.6$ならば，αは下から $0.6(60\%)$の点にあるのです．$f(x)$の値を下から順番に並べているために$F(x)$の分布は0以上1以下の一様乱数で表せるから，Uを使って$U = F(X)$として確率変数Xを求められるのです．

具体例で確認しましょう．

今回は$f(x) = \frac{\sin x}{2}\ (0 \leq x < \pi)$とします（**図2**）．積分して$F(x) = \frac{-\cos x + 1}{2}$であると分かります．そして一様乱数$U$を使って$X = F^{-1}(U)$を計算します．この確率変数では$F^{-1}(U) = \cos^{-1}(1 - 2U)$です．ここで$U_1 = 0.7$（点A）となったとき，$X_1 = \cos^{-1}(1 - 2 \times 0.7) = 1.92\cdots$となり（点C），同様に一様乱数$U_2, U_3, \cdots$から確率変数$X_2, X_3, \cdots$を導くことで$f(x)$を再現できるのです．図の$x = \frac{\pi}{2}$あたりからもわかるように$f(x)$の値が大きい部分の$F(x)$は傾きが急で，$U$を多数計算したときに結果としてその周辺の$X$の値が出る割合が多くなるのです．

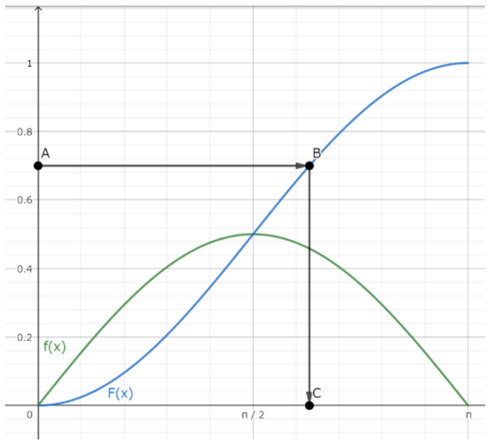


図2

○棄却法

棄却法では，あらかじめ別の確率変数（一般的に一様乱数）を作り，そのうちの一部を棄却することによって目当ての確率変数を作る方法です．一様乱数が従う一様分布の任意の値αでの密度（範囲上ならどこでも等しい）に定数cをかけたものを$cg(U)$，その時の目当ての確率密度関数の密度が$f(U)$ならば，一様乱数Uを$\frac{f(U)}{cg(U)}$の確率で採択，それ以外では棄却されるようにすると$f(x)$ができるのです．これはUとは別の0以上1以下の一様乱数Vを使い，$V < \frac{f(U)}{cg(U)}$のとき採択，$\frac{f(U)}{cg(U)} \leq V$のとき棄却することで表現します．採択された$U$の値はそのまま目当ての確率変数$X$の値になります．

逆関数法が金属を曲げるなどの加工をすることに例えられるならば，棄却法は大きな丸太を切ったり彫ったりして手ごろなサイズの物を作ることであるといえます．一様乱数を作るのは細かい作業をする前に丸太をちょうどよい大きさの直方体や円柱に切り分けること，棄却するのはその直方体を彫っていらない部分を取り除くことというイメージです．この時，丸太から切り分けるときの大きさはどの位でもよいというわけではないのです．大きすぎると，その後彫るときに木くずとなって捨てる部分が多く出て効率的ではありません．逆に小さすぎると，継ぎはぎしない限り物が作れません．棄却法でも$0 < \frac{f(U)}{cg(U)} \leq 1$が範囲内で常に成り立つようにしつつ，そのなかでもできるだけ小さいcを設定する必要があるのです．

ということで棄却法の具体例も見ていきましょう．**図3** のとおり，$f(x)=\frac{1}{18}(x^3-9x^2+15x+4)$ で，範囲は積分するとちょうど 1 になる$0 \leq x \leq 2$と設定します．$x=1$で$f(x)$の最大値$\frac{11}{18}$となるので，$cg(1) \geq \frac{11}{18}$となる中の最も小さいcを出します．この場合範囲内で常に$g(x)=\frac{1}{2}$なので，$c=\frac{11}{9}$，$cg(x)=\frac{11}{18}$となります．そして一様乱数$U(0 \leq U \leq 2)$，$V(0 \leq V \leq 1)$をそれぞれたくさん作ります．

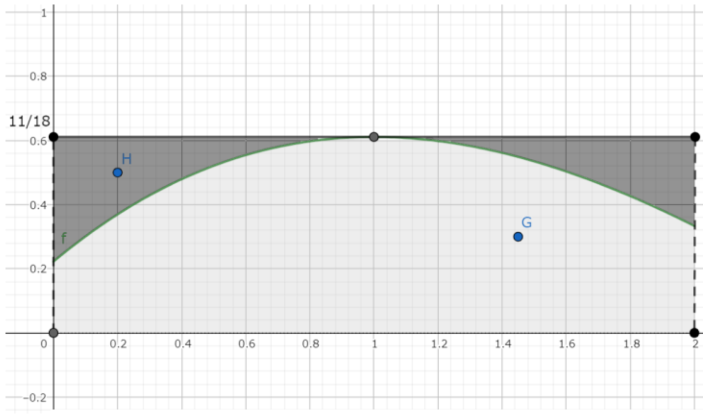


図3

今回，一回目では$U_1=1.45,\ V_1=0.49$となったとします．

このとき$\frac{f(x)}{cg(x)}=f(1.45) \div \frac{11}{18}=0.89\cdots$であり，$V_1<\frac{f(x)}{cg(x)}$となるので採択され$X_1=U_1=1.45$となるのです．では次に棄却される例をやってみましょう．二回目では$U_2=0.2,\ V_2=0.82$となったとします．このとき$\frac{f(x)}{cg(x)}=f(0.2) \div \frac{11}{18}=0.60\cdots$であり，$\frac{f(x)}{cg(x)} \leq V_2$となるので棄却され$X_2$は存在しないことになるのです．

図3 からわかるように，一様乱数の値U,Vからx座標の値がU，y座標の値が$V \times cg(U)$である点をとり，それが$f(x)$の下側（$V \times cg(U)<f(U)$，つまり$V<\frac{f(U)}{cg(U)}$）にあるなら採択，上側（$f(U) \leq V \times cg(U)$，つまり$\frac{f(U)}{cg(U)} \leq V$）にあるなら棄却になるとグラフ上で説明ができます．ちなみに採択される確率は，Uによってできた長方形の大きさによって決まります．この場合は$cg(x)$を積分すると$\frac{11}{9}$，$f(x)$を積分すると1なので，$\frac{9}{11}$の確率で採択されるのです．

逆関数を求める事が難しいときは棄却法が便利です．しかし，棄却法では一回の計算で二つの一様乱数が必要であることと棄却される分多めに作らなければならないので，逆関数法よりも手間がかかる場合があります．状況に応じて使い分けるのが大事なのです．

＜参考文献＞
モデリング　2005 年 4 月　日本アクチュアリー会

立命館大学知能システム研究室　擬似乱数の生成法 乱数 一様乱数 生成法　2020－8－3
http://sys.ci.ritsumei.ac.jp/probability/2011/10-6.pdf

コラム 3

好きな数は？

皆さんこんにちは．今年の数研の文化祭に全く関わってないという罪悪感から，文化祭２日前にコラムを書くことを決めた者です．1 つ前のコラムで，K さんが数研アンケートというのをやっていましたが，「好きな数は？」という質問に対して，その好きな理由が書いてないため，「気になるだろ，ふざけんな！！」と殺意を抱いた方も多いと思います．なので，僕は，もう一度アンケートを取り，数研メンバーが好きな数字とその理由をまとめてみました．それでは見ていきましょう！！！

① 256

２の８乗で使いやすいから．

② 1024

誕生日が 10 月 24 日なのと，２の 10 乗だから．

やはり２の累乗は人気ですね．ちなみに今回のアンケートで，数研内には，誕生日が 10 月 24 日の人が３人もいることが分かりました．すごいですねー．数研部員としては，部活内に同じ誕生日の人が３人いるという確率求めたくなります．

③ 1728

12×12×12 だから．受験の時立体切断でお世話になったから．あと，稲庭うどんうまいから．

④ 6

完全数だから．立方体の面の数が６つだから．

完全数とは，自分自身を除く正の約数の和に等しくなる自然数のことです．小さいものから，6（＝1+2+3），28（＝1+2+4+7+14），496（＝1+2+4+8+16+31+62+124+248），8128，33550336 などがあります．僕は完全数の中では，496 が一番好きです．

⑤ 1001

10 の３乗に１を加えた数であり，1001＝7×11×13 と３つの連続する素数の積だから．

（ちなみにこの記事を書いたのは 10 月 01 日）

⑥ 17

今から 200 年以上前のある朝，天才数学者ガウスは目を覚ましてベッドから立とうとしたとき，正 17 角形の作図方法を思いついた．$x^{17}-1=0$の解が整数の四則演算と$\sqrt{\ }$（3 乗根，4 乗根などは含まない）だけを組み合わせて表せることを示した．ガウスはこのことで自信がついて数学者になろうと決意した．

また，フェルマー数と呼ばれる，2 の2^n乗（n は非負整数）で表される自然数があり，素数であるフェルマー数はフェルマー素数と呼ばれるが，17 は現在知られている 5 個のフェルマー素数のうちの 1 つである．n がフェルマー素数のとき正 n 角形が作図可能であることが知られている．フェルマー素数が無限に存在するかどうかは現在未解決である．
（ついでに自分は今 17 歳）

はい，初めてめちゃくちゃ数学っぽいこと話した気がします．僕も中 1 の頃，レポートで正多角形の作図について書いたことがありますが，正 17 角形の作図の話などはすごく面白いので，ぜひ調べてみてください．

⑦ 1729

これは僕が一番好きな数字です．1729 はタクシー数やラマヌジャン数などと呼ばれ，2 つの立方数の和としての表し方が 2 通りある最小の数です．（ここでの立方数とは，ある自然数の 3 乗の数を表す．）1729 は 1 の 3 乗と 12 の 3 乗の和であり，9 の 3 乗と１０の 3 乗の和です．

ある日，インドの天才数学者ラマヌジャンの友人であるハーディが「今日乗ってきたタクシーは 1729 でつまらなかったよ」と話したところ，ラマヌジャンが「いやいや，1729 は 3 乗数の和として 2 通りで表せる最小の数だよ！」などと言ったというエピソードから，このように呼ばれています．

さらに，僕がこの数字が好きな理由がもう一つあって，1729 は素因数分解すると，7×13×19 と表され，19×91 と表すことが出来ます．7 と 13 と 19 というそれぞれの数字も好きですし，3 つの数の差がどちらも 6 になっているのが好きです．また，19 と 91 という前後を入れ替えた数字の積なのもすごくきれいだと思います．ちなみに，91 は，タクシー数の定義の，立方数に 0 と負の整数の 3 乗も含めた場合の最小の数で，キャブタクシー数と呼ばれます．どうですか？？？美しくないですか！？！？！？！？

これ以上話すと，さすがに引かれそうなので，この辺でやめておきます．

終わりに

今回，数研メンバーの好きな数字を一部まとめてみましたが，それぞれ好きな数字が色々あって，理由も様々だったり，誕生日が同じ人が３人も見つかったり（しかも 10 月２４日で２の 10 乗だし）してとても面白かったです．半分くらい，自分の好きな数字について語っていたような気もしますが…．

これを読んでいる皆さんも，理由は何でもいいので，好きな数字を持っておくと楽しいと思います．ありがとうございました～．

おわりに

会誌第 5 号を読んでいただきありがとうございました．今年は部誌を印刷・配布しないということで，いつもよりたくさん書いてくれた人が多かったですね．また，コラムの内容も充実していて，多くの人が楽しめる部誌に仕上がったと思います．

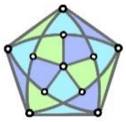
さて，突然ですが皆さんは数学に対してどのようなイメージがありますか？
数学は身近なところでとても役に立っていますし，論理的な思考力が身についたり，本質を見抜く力がついたりなどの学ぶメリットもあります．
しかし，やっていて楽しい！面白い！と感じられなければ，続けることは辛いです．「数学」と聞くとどこか難しそうなイメージがあり，避けられがちではないでしょうか．
この部誌を通して数学の面白さ，奥深さを感じてもらえたら幸いです．

今回の文化祭では例年のような展示を行うことができませんでしたが，今後も文化祭などを通して，多くの人に数学の魅力を伝えられるよう，活動していきます．
これからの数研にご期待ください！！

すうけん 2020 メンバー

顧　　問　Mr.Y.S.

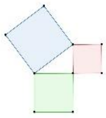
副 顧 問　Mr.S.M.　Mr.N.H.

O　　B　 Y.I.　 W.T.

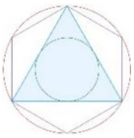
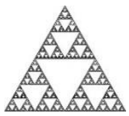
高等部 3 年　

K.K.　 S.K.　

A.H.　 H.W.

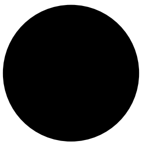
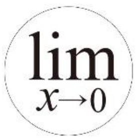
高等部 2 年　 S.A.　 H.O.　 T.H.　 S.Y.

高等部 1 年　 R.A.　 T.I.　 G.I.　 S.O.

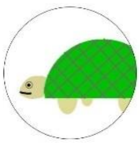
 I.O.　 Y.T.　 K.H.　 Y.Y.

中等部 3 年　 S.M.　 S.T.

中等部 2 年　 R.I.　 N.U.　 Y.N.

中等部 1 年　 H.I.　 Y.O.　 T.K.　

K.S.

 S.S.　 K.S.

すうけん