《市民講演会》
「数学が何の役に立つの？」と言われているが…

講師：佐々木建昭（筑波大学 数学系）

本日はようこそお越し下さいました。ちょうど桜も咲き始め、お花見でもしたいところをお越し頂いたのですから、「来て良かった」と思って頂けるような話をしたいと思っております。

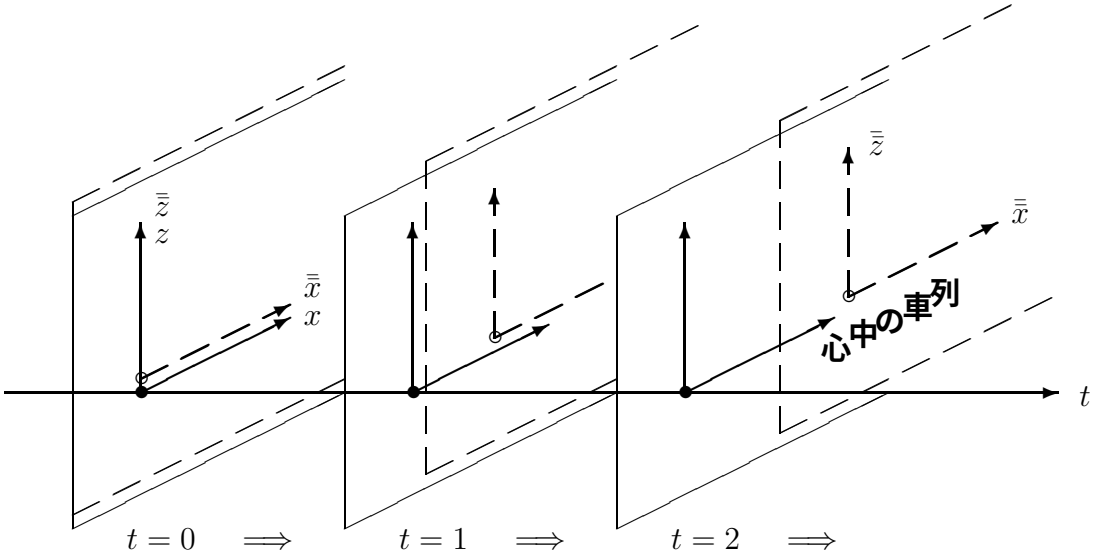
講演の題目は『数学が何の役に立つの？と言われているが…』、としましたが、これは勿論、「とても役に立つ」と言いたい訳です。近年、中学校や高校で理科離れ、数学離れが言われています。また大学においてさえ、学生から「数学がどのように応用されるのか、そのことも話して欲しい」との要望を多く聞きます。数学にたずさわる者としては、少くとも中学生や高校生から、「何故こんな数学を勉強するの？」と尋ねられたとき、きちんと答える必要があります。私の話の目的は、その答の一つを具体的な例を用いて説明することです。私が話したい相手は中学生や高校生、そして中学校や高校の先生です。ざっと見渡しますと、聴衆のみなさまには同業者らしき人が多く、中学生や高校生が少ないのが残念ですが、同業者は無視して、中学生・高校生を相手に話します。話の方はものすごく易しくしてありますので、御安心ください。実は、行きつけの飯屋の親父さんが「先生、オレも聞きに行こうかな」と言ったので、スライドは滅茶苦茶に易しくしました。お手元の講演予稿は以前に作ったので、やや難しいですね。スライドのコピーを用意していますので、欲しい方は講演のあとでお申し出ください。

さて、私の話の内容は大きく分けて二つです。一つは「数学とは強力無比な思考的武器である」こと。このことを相対性理論を例に説明します。もう一つは「数学とはハイテク製品における巧妙無比な理論的部分である」こと。このことを現代暗号を例に説明します。最後に、ここには隠してある話をしますが、それは後のお楽しみです。

まず第一の話、「数学は思考的武器である」、…思考的武器って何だろう？ みなさん、新しい科学的発見があったとき、新聞やテレビで「これは理論的に予言されていた。」という解説を見たことがあるでしょう。理論的に予言するとは一体、どうしてそんなことができるんでしょうね。また、「コンピュータでシミュレーションをして…」という言葉もよく聞きますが、実際に起きる現象が何故コンピュータで計算できるんでしょう。実は、これらの背後には数学があるんですね。その具体例として「時間と空間が入り混じる」という事を数学的に導いてみましょう。エーッ、そんなことが中学生や高校生に解るの？、とお思いでしょうが、どうぞ御心配なく。

「時間」って何でしょうね。ほとんどの人は、そんな事を考えたこともないでしょうが、時間には色がついていたり、味があることを知っていますか？。…あなたはどうですか？若い人なら甘く酢っぱい時間を過ごしたり、私なんぞはブルーな時間を過ごすことが多いのですが…。それは置いといて、時間と言えば時計、誰にも一定の割合で時間が過ぎる、というのが我々の感覚です。そこで、このように時間を直線で表わしましょう（次図）。その直線を一定の割合で刻んで、時間とは過去から現在、未来へと一定の方向に進むものですよね。さっき講演が始まったのが 2 時、私の講演の終わる頃が 3 時、という訳です。

時間のことを英語で time というので、この矢印のところに t と書いて時間を表わすことにします。さりげなく、記号を導入しておきます。時間に比べれば、空間の方は分り易いですね…誰の目にも見えますからね。演壇の机の端を基準にすると、この点は右の方向に 1 メートル、そちら方向に 30 センチ、上の方向に 50 センチという訳で、この室の任意の点が三つの数の組で指定できます。三つの数値が必要なので、我々の住む空間は 3 次元であると言いますが、これは誰も知ってますね。これを図にしたのがこのスライドですが、2 次元平面上に 3 次元の図は書きにくいので、図では我々の住む空間を 2 次元で表しています。時間と同じく空間も、直角に交わる直線を書いて表わします。これは住宅地の番地みたいなものですね。あなたの家は、市の中心から、北方向に 3 丁行き、そこから東方向に 5 番目だ、という具合ですね。そこで、このような図のことを『番地系』と名付けます。飯屋の親父さんにも解るように、苦労して話を作っていることが分るでしょう。



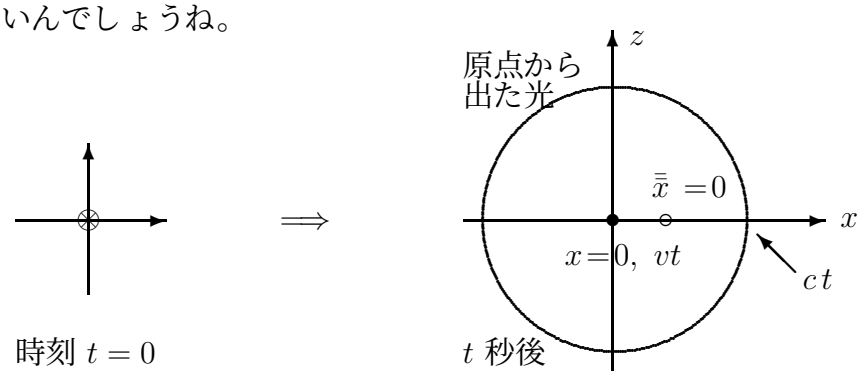
次に、x 方向に速さ v で走る列車に固定された番地系 $(\bar{\bar{x}}, \bar{\bar{y}}, \bar{\bar{z}})$ を考えましょう (上図)。時刻 $t=0$ では、止まっている番地系と列車上の番地系では、基準点が一致しているとします。時刻 $t=1$ では、静止番地系はここに来ますが、列車番地系はさらに x 方向に v だけ移動します。$t=2$ では、列車番地系は静止番地系に比べて、$2v$ だけ移動しています。この図で、この漢字（心中の車列）は、右側から読んでくださいね。左側から読むと全然違った意味になりますからね。 両方の番地系の中心の位置を静止番地系で表わしたのがこの図です。静止番地系では常に $(0,0,0)$ ですが、列車番地系では、$t=1$ では $(v,0,0)$、$t=2$ では $(2v,0,0)$、一般の時刻 t では $(vt,0,0)$ となります。これまで、さりげなく記号を導入してきましたが、記号を使うと任意の時刻の位置が一つで表わされて、非常に便利ですね。番地系の中心でなく、任意の点の間の関係を表わしたのがこの式です。

$$(\bar{\bar{x}}, \bar{\bar{y}}, \bar{\bar{z}}) \Leftrightarrow (x,y,z) : \ \bar{\bar{x}} = x - vt, \ \bar{\bar{y}} = y, \ \bar{\bar{z}} = z$$

こんなに簡単な式で、すべての点の間の関係が表せるのですから、数式がいかに便利であるか解りますね。こんなに易しいことをダラダラやっていて、はたして、「時間と空間が入り混じる」まで行けるのか？ どうぞ御心配なく。10 分後には間違いなく…。

ここで、一つの実験事実を示します。それは、『光の速さはどんな番地系の人が見ても同じ値である』ということです。因みに、光の速さは秒速約 30 万キロ、1 秒間に地球を

7回半回るぐらいの、ものすごいスピードです。これは、ボケッと考えては何も分りませんが、少しキチッと考えると非常に奇妙です。だって、そうでしょ。時速500キロで飛ぶ飛行機を時速250キロの新幹線から見ると、新幹線が飛行機を追っかけてる場合は飛行機の速さは250キロに見えるが、反対方向に行ってるときは飛行機の速さは750キロに見えるでしょう。動く物の速さというのは、どういう番地系で見るかによって速さが違うのが常識ですよね。この常識が光には通じない、という訳です。正に、常識を信じるか、実験を信じるか、ザット・イズ・ザ・クェッション という訳です。ここで常識を信じるようでは、江崎玲於奈先生や白川英樹先生のように、ノーベル賞はもらえません。しかし、どう考えればいいんでしょうね。



ここから数学の出番となります。番地系の中心から出た光を数式で表してやりましょう。時刻$t=0$に光が一瞬、パッと出たとします(上図)。時刻tでは、その光は半径ctの球面になりますよね、この図では2次元の円として表わされていますが…。静止番地系の記号(x,y,z)で表すと、光を表わす円の方程式は$x^2+(y^2)+z^2=c^2t^2$となります。ここで、(y^2)を入れると球の方程式となります。円の方程式は、高校生のみなさんは知っていますが、中学生は知らないのでちょっと説明します。実は、これは直角三角形に対するピタゴラスの定理、三平方の定理とも言いますが、それなんですね。直角三角形では、斜辺の2乗は底辺の2乗プラス高さの2乗である、という定理ですね。今の場合、斜辺の長さが半径ctで、xとzがどこにあろうと直角三角形ができるので、この方程式が成り立つことが解るでしょう。さて、同じ光を列車番地系で表してやりましょう。すると、$\bar{\bar{x}}^2+\bar{\bar{y}}^2+\bar{\bar{z}}^2=c^2t^2$となりますね。これらの式に、二つの番地系の間の関係式、$\bar{\bar{x}}=x-vt,\ \bar{\bar{y}}=y,\ \bar{\bar{z}}=z$を追加すると、これら全体の数式は$v=0$でない限り矛盾します。実際、$\bar{\bar{x}}$に$x-vt$を代入し、二つの円の方程式を引いてやると、$-2vtx+v^2t^2=vt(-2x+vt)=0$となり、$vt=0$あるいは$vt=2x$という変な式が出てきます。

これは困った、…考え方がどこかオカシイ。数式の立て方は間違ってないので、実際に簡単な式ですからね、どこか基本的な考え方が間違っているはずです。よくよく考えると、我々は時間のことをよく考えてはいなかった。安直に、時間は誰にも一様に、ということは番地系に依らないで一様に、進んでいくと考えていたが、このことは誰も確認した訳ではない、単にそう思っただけです。そこで、発想を根本的に変えて、時間の進み方が番地系に依る、と考えてみましょう。これはアインシュタインが約百年前に考えたことですが、こんな柔軟な発想ができるアインシュタインは偉いですね。この考え方に従い、

$$\bar{\bar{x}}=\alpha(x-vt),\quad \bar{\bar{y}}=y,\quad \bar{\bar{z}}=z,\quad \bar{\bar{t}}=\beta(t-\gamma x)$$

と置いてみます。ここで、α,β,γはこれから決めていく数です。先程の光の図を見ると、光の進む方向には空間が伸び縮みするように見えるから、x方向にはαをかけてやりま

す。同様の考えから、時間にも x を入れてやります。光の進む方向と直角な方向、y と z 方向では、たとえば新幹線がギリギリで通り抜けできるトンネルを考えると、番地系によってトンネルの幅が伸びたり縮んだりすると、番地系によって新幹線はトンネルを通過できたり、トンネルの幅が狭くて入り口で激突したりしますよね。だから、y と z 方向では伸びたり縮んだりしないはずです。

あとは簡単な計算です。光を二つの番地系で見ると、どちらも円となり、次の方程式で表されます。

$$x^2+y^2+z^2=c^2t^2, \qquad \bar{\bar{x}}^2+\bar{\bar{y}}^2+\bar{\bar{z}}^2=c^2\bar{\bar{t}}^2.$$

$\bar{\bar{x}}$ と $\bar{\bar{t}}$ をそれぞれ $\alpha(x-vt),\ \beta(t-\gamma x)$ で置き換え、二つの円の方程式を辺々引くと $x^2(\alpha^2-c^2\beta^2\gamma^2-1)+2xt(-\alpha^2v+c^2\beta^2\gamma)+t^2(\alpha^2v^2-c^2\beta^2+c^2)=0$ を得ます。この式はどの x, t にも成立しなければならないので、数学の定理から、各係数、この部分ですが、が 0 でなければなりません。すなわち、$\alpha^2-c^2\beta^2\gamma^2=1,\ \ \alpha^2v-c^2\beta^2\gamma=0,\ \ c^2\beta^2-\alpha^2v^2=c^2$ を得ます。この連立方程式は簡単に解けて、$\alpha^2=\beta^2=1/[1-(v^2/c^2)],\ \gamma=v/c^2$ が得られます。まとめると、この関係式が得られます。この式でもよいのですが、光速度を基準にした距離 $t'=ct$ で書き直すと、このように対称性のよい美しい式が出てきます。

$$\boxed{\bar{\bar{x}}\ =\frac{x-vt'/c}{\sqrt{1-(v^2/c^2)}},\quad \bar{\bar{t}}'\ =\frac{t'-vx/c}{\sqrt{1-(v^2/c^2)}}}$$

この式を見ると、「空間と時間が入り混じる」ということが実感できるでしょう。光速度基準距離というのは、宇宙では光が 1 秒間に進む距離 30 万キロを基準にとるということです。星までの距離を何光年と言う、あの距離ですね。1 センチだの、10 メートルだのというのは、狭い地球上の人間を基準にしたミミッチイ距離なんですね。宇宙から見ると、人間の小ささが本当によく分りますね。

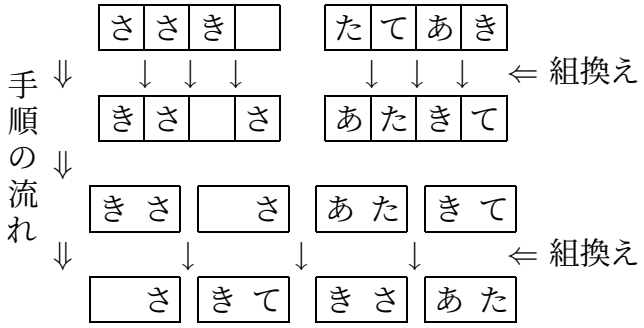
ここまで来ると、「数学は強力無比な思考的道具である」という意味がお解りでしょう。私はまず、時間や空間などの概念を記号化することの便利さを言いました。次に、現象を数式で表わしました。一旦、数式で表すと、あとは数学を使って解析していけば、空間と時間が入り混じるというような奇想天外なことが、ごく簡単な計算で出て来ました。もしも数式と数学を使わないで、言葉だけで物事を考えたのでは、到底、こんな訳にはいきません。数学を使ったからこそ、こんなに簡単に出て来たのです。

それと共に、「何故、数学を勉強するのか」も解っていただけたと思います。ほとんどの中学生や高校生は、放物線や円の方程式を学んで何の役に立つの？、と思っているのではないでしょうか。しかし、その円の方程式を使って、時間と空間が入り混じるという、とてつもない事が簡単に出て来ましたね。みなさんが学校で学んでいるそのことが、ものすごく役に立ったのです。数学は、科学や工学にとっては、無くてはならない存在です。そのことが当り前すぎて、みんな、その重要性を認識しなくなっているのです。ちょうど、空気や水が人間にとって不可欠な存在だが、普段は誰もその重要性を認識しないようにね。そして、数学がこんなに重要だからこそ、中学校や高校では、生徒たちに有無を言わせず、文字式の使い方をマスターさせ、2 次方程式の解き方を憶えさせ、微分法や積分法を授業し、そして理工系の全ての大学が入試問題に数学を出しているのですね。

≪ 講演会では、原爆や水爆の理論的予言の話を、$E=mc^2$ を数学的に
導くことにより、具体的に話したが、紙数の都合上、割愛する。≫

次は「数学はハイテク製品における理論的部品である」という話をします。みなさんのほとんどが持っているであろう携帯電話、あれ、スゴイと思いませんか。若い人は不思議に思わないかも知れませんが、昔の電話を知っている者にとっては驚異的ですよ。ほんの少し前までは、電話と言えば、全て電話線を通じて信号が流れていました。しかも、二つの電話機で話をするには、途中に中継機というのがあって、電話番号どうしを継いでいたんです。ずっと以前には、この中継も人間が行っていました。電話会社には大勢のおねえさんがいて、この番号に継いでくださいと言われると、その番号のところにコードをさし込んでいたんですね。それが、携帯は電線がなくても、世界中のどの番号にもすぐに継がるのですからね。ものすごいハイテク製品ですよ。このようなハイテク製品の中味はどうなっているんでしょうね。また、最近、大手の電子メイルの会社から、何百万人もの個人情報が流出した事件が大きなニュースになっていました。この事件を見ると、情報化社会の安全性はどうなってんの？、と思いますよね。限られた講演時間では、これらの疑問に全て答えることはできませんが、多くのみなさんが興味を持たれるであろう暗号を例に、理論的部品とはどういうことかを説明します。

さて、暗号…戦争やスパイ映画には不可欠です。時代劇だと、「ヤマ」,「カワ」と言い合って味方どうし確認するやつですね。昔の暗号として、ローマ時代にシーザーが使ったと言われるシーザー暗号があります。これは、アルファベットを適当な数だけずらすんですね。円筒の上部と下部が別々に回転するようにして、上部と下部に同じアルファベットを書き、上部と下部を適当にずらして、上部のそれぞれの文字を、同じ場所にある下部の文字に対応させるんです。そうすると、たとえばこのスライドのように、『あいうえおかきくけこさし…』を『ナニヌネノハヒフヘホマミ…』に対応させると、「あいしてる」という文は「ナニミヌス」に変換されます。これを見た敵が「ナニモミエナイス」と返事をすれば成功ですね。



これはもう少し複雑な暗号です (上図)。図を見れば暗号化が大体わかると思いますが、第 1 段では文章を小さな部分に分割し、各部分で一定の規則で文字を置き換えています。第 1、第 2、第 3、第 4 の文字がそれぞれ 第 2、第 4、第 1、第 3 へ移ってますね。第 2 段では、変換された文字を数文字づつ、ここでは 2 文字ですが、まとめて一塊りとし、それらの塊りどうしを置き換えます。必要なら、同じことを繰返します。この仕組みは複雑そうですが、数学的に見れば、単なる線形変換というやつです…ゴメンね、中学生や高校生諸君の知らない言葉を使って。それぞれの段の組換えが線形変換で、3 段の組換えをすることは、三つの線形変換を順に行なうことに対応します。線形変換は何回行っても全体として線形変換で、元に戻す変換、逆変換と言いますが、それも簡単に計算できます。このような暗号は、数学的に見れば極めて単純で、簡単に破られてしまいます。

では、数学的に見ても絶対に破れないと保証できるような暗号を作りたくなりますね。それが現代暗号ですが、ここで「絶対に破れない」というのは少し説明が必要です。実は、理論的には破ることはできるのだが、破るためには途方もない量の計算が必要で、現在の最高速のコンピュータを持ってしても、たとえば 1 億年かかる、そういうものなんですね。これはきちんと頭に入れておく必要があります。そのような暗号の一つが、1978 年に発表された RSA 暗号です。RSA というのは三人の暗号学者、Rivest, Shamir, Adleman という人の頭文字です。この暗号の中で数学がどう使われているか、安全性がどう担保されているか、見ていきましょう。

その前に簡単な数学の復習です。素数、これは誰も知ってますね。1 と自分自身でしか割り切れない整数で、3 や 5 や 11 や 13 などですね。任意の自然数は素数の積で表わされ、それを素因数分解といいます。今、二つの大きな素数を掛けて一つの整数を作り、次にその整数を素因数分解してみましょう。もちろん、掛けた人はどんな素数の積になるかを知っていますが、それを知らないとして、一般的な方法で計算するのです。コンピュータを使って実験してみます。最初は 20 桁の素数を二つ掛けて 40 桁の整数を作った場合です。…アッという間に分解しましたね、1.34 秒ですか。次は 25 桁の素数の積の場合です。これは少し時間がかかりそうですね。コンピュータが計算している間に、コンピュータを操作してくれている人を紹介します。私の研究室の院生の稲葉君です。彼は今日のためにいい服装をしてきたそうです。…やっと答が出ましたね、今度は約 30 秒ですか。最後は 30 桁の素数の積です。今、コンピュータに go の命令を出しましたが、答が出るまでには約 10 分かかるので、別の話をしておきましょう。

$$\begin{cases} 1 \div 4 \equiv 4 & (\Leftarrow 4 \times 4 = 15 + 1 \equiv 1) \\ 2 \div 3 \equiv 4 & (\Leftarrow 3 \times 4 = 10 + 2 \equiv 2) \end{cases}$$

乗算表 ($p = 5$)

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

素数のことを英語で prime というので、数学では素数のことを p という記号で表わすのが慣例です。そこで、ある素数、3 でも 5 でも 11 でも何でもいいですが、を p とします。そして、『素数 p で割った余りを答』とする計算を考えましょう。このスライドは $p = 5$ の場合を示しています。$2 + 3 = 5 = 5 + 0$ だから、答は 0 ですよね。それで、このことを記号 $\equiv$ を使って $5 + 0 \equiv 0$ と表わします。同じように、$3 \times 4 = 12$ で、$12 = 10 + 2$ だから、答は 2 となります。これは誰だって分りますよね。実は、この計算法は面白い性質を持っています。「整数を整数で割った答が整数になる」という性質です。…そんなバカな、2 を 3 で割ると 2/3 で、整数にはならない、と思うでしょうが、仕組みはこうです。たとえば、$4 \times 4 = 15 + 1 \equiv 1$ だから、両辺を 4 で割ってやると $4 \equiv 1 \div 4$ となりますよね。同じように、$3 \times 4 = 10 + 2 \equiv 2$ だから、$4 \equiv 2 \div 3$ となります。この表は、縦列の $1, 2, 3, 4$ と横列の $1, 2, 3, 4$ を掛けた一覧表です。どの行にも、どの列にも $1, 2, 3, 4$ が一個づつ出ていますね。この表は $p = 5$ の場合ですが、このことはどんな p にも成立します。証明は簡単ですから、意欲ある中学生や高校生諸君はやってみるといいですよ。

こんなオタクっぽいことが一体、何の役に立つの？、と思われるでしょうが、実はコンピュータには非常に役に立つんですね。理由の一つは、コンピュータのメモリというやつは、たとえば電球を 32 個並べて、どの電球がついているかで数を表しているものなので、一つのメモリで表せる数が限られているのです。先程の計算では、素数 p より大きな数は現れないので、その計算法はコンピュータにはとても便利です。でも、もっと重要なのは、その計算法には通常の計算法にはない種々の性質があって、それが役に立つんです。しかし、…数学者というのは、確かにオタクっぽいことをやってますね。

性質の第一はフェルマーの小定理です。フェルマーの定理といえば、有名な「$x^n+y^n=z^n$ となる整数 x, y, z は？」、というやつで、それと区別するために小定理と呼んでいます。約 350 年前の定理です。p を素数、どんな素数でもよいですが、h を任意の整数とするとき、h を $p-1$ 乗すると、先ほどの計算法では答は 1 になる、式で表すと $h^{p-1} \equiv 1$ というものです。たとえば $p=7$ の場合、このようになり、確かに 1 ですよね。実は、このスライドには 1ヶ所ミスがありまして、どこか分りますか？ …h が 0 の場合は困るんですね。0 は何乗しても 0 ですからね。だから、$h \neq 0$ という条件をつける必要があります。さて、この式の両辺に h を掛けてやると、$h^p \equiv h$ という式が得られますね。そうです、p 乗すると元の数に戻るんです。この性質が RSA 暗号では決定的な役割を果たします。

次の定理はユークリッドの拡張互除法で、これは何と紀元前の定理です。正確に言えば、ユークリッドの方法は最大公約数を計算する互除法で、拡張互除法はずっと後に発見された方法です。u と v を互いに素な、ということは同じ素数を含まない整数とするとき、$au+bv=1$ となる整数 a と b が存在する、というもので、この a と b を計算する方法が拡張互除法です。ここで、$\equiv 1$ ではなく、$=1$ であることに注意してください。たとえば $u=29$, $v=23$ の場合、$4\times 29-5\times 23=1$ なので、$a=5, b=-4$ となります。ユークリッドの互除法は実に速い方法で、現在でも使われています。紀元前の計算法が現代でもスピードを競うコンピュータで使われているなんて、驚異的ですね。

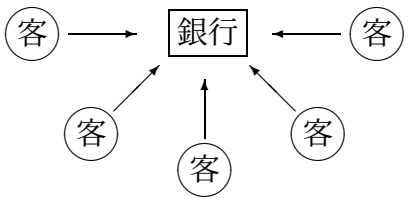
アッ、先ほどの計算がようやく終了したようです。計算時間は約 519 秒、9 分弱ですね。このように、素因数分解は中学生でも知っている計算ですが、桁数が増えるにしたがい、急速に時間がかかる計算なんですね。この簡単な事実が、RSA 暗号の基礎になっているのです。本当に、こんな簡単なことが国家機密がからむ暗号の基礎になっているなんて、驚くべきことですよね。

さて、RSA 暗号の仕組みを説明します。私の説明はいつも簡単で、こんなに簡単な説明でいいの、というくらい簡単です。まず、整数 a と e を、任意の整数 h に対して $h^{ea} \equiv h$ となるように決めます。この式はフェルマーの小定理みたいなものですね。次に暗号化ですが、まず暗号にしたい文を簡単な規則で整数 h に変換します。そして、h を e 乗した η を暗号にします：$h^e \equiv \eta$。ついでながら、この文字はギリシャ文字で「エータ」と発音しますが、ちょうど h をひっくり返した形をしていますね … この字「平文」は何と読むんでしょうね。「タイラブン」か「ヒラブン」か、「ヘイブン」さんか、「ペーブン」か、という訳ですが、分りますか？ ヒラブンと読むらしいんですが、今のジョークは 50 年以上前の落語が出典です。さて、復号化ですが、今度は η を a 乗してやります。すると、$\eta^a = h^{ea} \equiv h$ ですから、元の数 h に戻りますね。ちょうど時計の針のように、h を 2 乗、3 乗、4 乗としていくと、上にあった針がだんだん回転していきますね。真下に来たところで、そのときの数を暗号にします。平文を記号 h で表し、h を 180 度回転した形の η で

暗号を表すとは、芸が細かいでしょう。数をたとえば 1000 乗して余りをとると、元の数とは似ても似つかぬ数になりますよね。ですから、この暗号 η から元の数 h を見つけ出すのは、たとえ e の値が分っても絶望的に難しいのです。しかし、η を a 乗すると、ピタリと元の数 h に戻るんですね。…どうです、うまく出来ているでしょう。

実は、暗号化の仕組みはもう少し複雑です。フェルマーの小定理では割る数は素数で、何乗かして元に戻すための指数も同じ素数でしたが、RSA の暗号化では、元に戻すための指数は $e \times a$ で、素数ではないですね。割る数、それを m とすると、m も素数ではなく、異なる素数 p と q の積です：$m = p \times q$。しかし、用いる定理はフェルマーの小定理を少し拡張したもので、e と a の計算にはユークリッドの互除法と拡張互助法を用います。素数 p と q は 100 桁程度に選びます。e は $\gcd(p-1, e) = \gcd(q-1, e) = 1$ を満たすように決め、ここで gcd は最大公約数を表わしますが、最後に a と b を $a \times e + b \times (p-1)(q-1) = 1$ を満たすように決めます。この仕組みはやや複雑なので、説明は省きますが、いずれも大昔の定理が使われていることだけを強調しておきます。数学の定理は永遠に真理ですから、時代を越えて使えるんですね。

RSA 暗号をコンピュータで実演してみましょう。「Tateaki Sasaki」という文を暗号にしてみます。まず、文字を数字化する規則ですが、文字 1 は 1 に、文字 2 は 2 に、文字 a は 11 に、文字 b は 12 に、文字 A は 41 に、文字 B は 42 に、等として、アルファベットやその他の文字を 99 以下の 2 桁の数字で表します。この規則では、「Tateaki Sasaki」という文は整数 601130151121193759112911 2119 に変換されます。次に素数 p と q として、$p = 347304951386502593301 7097$、$q = 962884287636615482625 2291$ を選びます。すると、p と q の積 m は、$m = 33441448070846192022001779927542856064726938419227$ と、50 桁の整数になります。次に e を計算します、…アッという間ですね。条件を満たす e は非常に多く存在しますので、ここでは最も小さい数を選びました。e が決ると、暗号 η が $\eta = 80862526023468016661705293404055088344172858940 13$ と計算できます。…元の数とは似ても似つかない数ですね。そして、a を計算すると、…これもアッという間に計算できましたね：$a = -11147149356948730674000588941883488611182059716613$。最後に復号化として、整数 η を a 乗してやると、…ほら、元の数に戻りました。確認のため数字を文字に戻してみましょう…目出度く「Tateaki Sasaki」が得られましたね。



RSA 暗号の有用性を見てみましょう (上図)。RSA 暗号では素数 p と q が決定的に重要ですが、これらは完全秘密です。実際、p と q は m, e, a を計算したら消してもいいんです。p と q は暗号化にも復号化にも必要ないんです。次に、m と e は公開します。公開と言っても、新聞に載せる訳ではなく、暗号を作成するユーザのコンピュータに入れるんですね。このスライドで説明しましょう。銀行には顧客が何百万人もいます。顧客は ATM でお金を引き出したり入金したりしますが、その際、パスワードがバレると大変ですよね。そこで、パスワードを暗号化して銀行本店のコンピュータに送るとします。もしも、この暗号化を、あの将軍様の国のように、秘密の暗号表による方法で行うならば、何百万もの

お客の中には必ず多くのスパイがいるはずで、暗号表がバレバレになって、秘密が保たれるなんて有り得ないですよね。でも、RSA 暗号では、m と e が知られても、a さえ知られなければいいんです。a は銀行本店が厳重に管理して、秘密にする訳ですね。どうです、うまく出来ていると思いませんか？

RSA 暗号の安全性ですが、式 $\eta \equiv h^e$ から h を決めることは、e が大きいときは絶望的に大量の計算が必要なことが分っています。式 $\eta^a \equiv h$ から計算しようとすると a が必要で、a を計算するには素数 p と q が必要で、そのためには公開された数 m の素因数分解が必要ですね。でも、60 桁程度の数でさえ、さっき見たように、分解するのは大変だったですよね。だから、100 桁程度の数では非常に大変な訳です。10 年くらい前までは、m として、50 桁 $\times$ 50 桁で、100 桁の整数をもってくれば十分だと思われていました。現在では、素因数分解の方法もいろいろ研究されて、いい方法も見つかっています。そのため、100 桁では危ないぞ、200 桁なら当分は絶対に大丈夫だ、という訳で、200 桁程度にしているんですね。

これまでの話をまとめましょう。これまでの説明で、理論的部品とはどういうことか、大体お解りであろうと思います。ハイテク製品の多くはコンピュータで制御されていますが、その中にあるプログラムは数学の理論に基づいて作られていることが多いのですね。そういう形の部品として、数学が入っている訳ですね。

人類が３千年をかけて創り出した
最高の知的資産・最高の芸術作品

♠ 科学技術を記述する共通の言語
♢ 科学技術を探求する最強の武器
♣ 人間の神秘的な頭脳活動の結晶

これは数学の講演としては最後のスライドです。最近、新聞やテレビで知的資産という言葉をよく見ます。資源の少ない日本は、科学技術で生きるしかない、そのためには知的資産を保護し、活用しなければならない、と言われていますね。そういう観点から数学を観ると、数学とは、その時代時代の最高の頭脳が、脳味噌を絞り尽くし、３千年をかけて栄栄と築きあげてきた、最高の知的資産であると言えます。数学とは、世界の誰もが自由に使える知的資産です。これを活用しない手はないですね。アメリカなど先進国は、そのことをよく知っていて、数学を戦略的に活用しています。

と同時に、数学を勉強すればするほど、その見事さ、美しさに驚嘆します。数学とは、人間が創り出したものです。そういう意味で芸術みたいなものですね。そこに現れる定理の多くは見事な論法で証明され、理論は想像を絶するほどの美しさで構成されています。何十万、何百万という人が参加して創り出した、最高の芸術作品だと思います。

最後に、少し時間が残ってますので、筑波大学の校風ともいうべき「文武両道」の話をさせてください。　≪ この部分は割愛する ≫

どうも、御静聴、ありがとうございました。