紹介

情報科学を体感的に学習する教材の開発

―モンテカルロ法と秘密鍵公開鍵―

静岡産業大学情報学部教授　高橋　等

1．はじめに

情報科学の事象を理解するためには，その前提となる概念が必要である。そして，情報科学に関する概念は，学校での学習から獲得するものとは別に，遊びや趣味，部活動，家事の手伝いなどの日常生活の体験から獲得するものも多い。

そこで，情報科学に関連する体験が乏しく，理論的，抽象的な内容を座学だけでは理解が難しい生徒に対して，実験を行い体感を伴う学習を行うことが有効であると考えた。

ここでは，体感を伴う教材として，モンテカルロ法により円周率を求める教材と，通信データの暗号化で使用される秘密鍵と公開鍵の教材を紹介する。

2．モンテカルロ法により円周率を求める教材

2.1　教材のねらい

モデル化とシミュレーションの学習として，モンテカルロ法により円周率を求める題材がよく取り上げられる。授業展開としては，コンピュータによるシミュレーションを行う前に，①正方形の中に四分円を紙に描き，その上から胡麻や大豆などの粒を一様に振りまき，②図形の面積と粒の数が比例すると仮定して，③正方形内と四分円内の粒の数から計算して円周率を求める実験を行う。個々の実験結果にはばらつきがあるので，真の値に近づくためには，④より多くの実験を行いその平均を求めるとよいことに気づく。より多くの実験を効率よく行う代替方法として⑤表計算ソフトを使用してシミュレーションのスプレッドシートを制作し，理論と結果を検証する。このように，円周率という生徒がよく知っている値を求める題材は，コンピュータによる問題解決方法を学習するのに適した題材である。

しかし，実際に教室で実験を行おうとすると，胡麻や大豆が散乱する可能性や，粒を計数する手間などが予想され，実験を諦める場合も出てきてしまう。円周率を求める理論を理解しないと，単なる表計算ソフトの操作方法の学習になってしまう恐れがある。

そこで，手軽に豆まきの実験が行え，モンテカルロ法の概念を理解できるように工夫した教材を開発した。

2.2　教材の構造

この教材の構造は図２のように，クリアケースの中にフェルトを貼り，その上に正方形と対角線の図形及び，正方形と四分円の図形に合わせて直

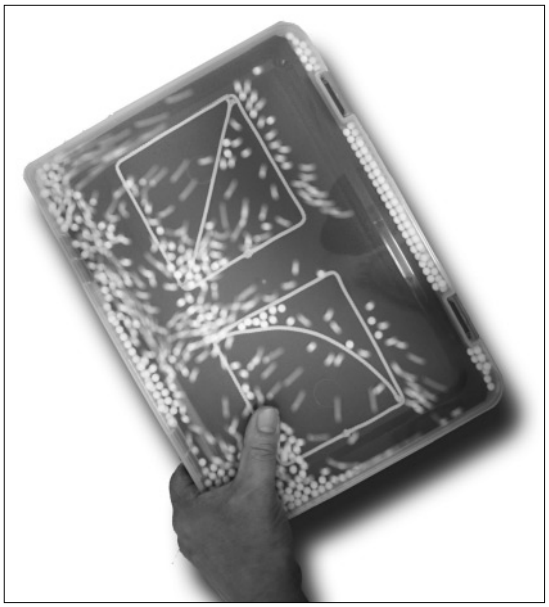

図１　円周率を求める実験

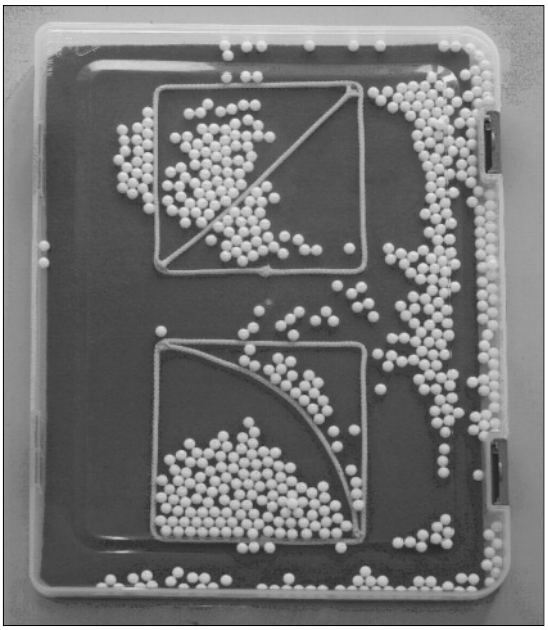

図２　円周率を求める実験教材

径約２mmの組紐を接着剤で貼り付け，玉（BB弾）を500個入れてふたをしたものである。費用は接着剤も含めて１組500円程度である。

2.3　実験方法

この実験では，①「ある図形の上に一様にばらまいた玉の数は，図形の面積と比例する」という幾何の概念と，②「ばらまいた玉は偶然にその図形の上に止まったもので，１回の実験では真の値から離れた結果がでるかもしれない。しかし，数多くの実験を繰り返せば真の値に近づく」という確率の概念の獲得が重要である。

そこで，この教材の実験では，まず，正方形と対角線に囲まれた２つの領域内に止まった玉を数える。２つの領域は同じ面積なのでほぼ同数の玉が入ることが確認でき，玉数と図形の面積が比例することが理解できる。しかし，図形の面積が等しくても，玉数が全く同数になることはまれである。何度も繰り返して得た値を平均すれば，玉数が等しい値に近づくことを理解させる。その後，正方形と四分円に玉をばらまき，玉数を数え，計算から円周率を求める。

2.4　教材の特長

この教材の特長をまとめると次のようになる。

・玉が散乱しないので片付けが楽である。
・玉数と図形の面積の関係を理解させやすい。
・組紐が玉の移動を止めるので数えやすい。
・ランダムや確率の概念が体感できる。
・生徒に作らせることも可能である。
・班（５～６人）に１個あれば実験できる。
・一度作れば何年も使える。

2.5　授業の様子

情報科担当教員の研修会と大学の授業でこの教材の製作及び実験を行い，その様子を観察した。

最初はクリアケースの振り方がわからず，玉の配置が極端に偏ってしまうが，そのうちに振り方が上手になり玉が均等に散らばるようになる。計数結果も予測どおりになり，モンテカルロ法で円周率を求める理論を理解することができた。

さらに，特筆する行動として，図形の中に玉を隙間なく並べようとする者が何人か現れた。図形の中に玉を並べて計数した方が正確な値が出るのではないかという探求心と，ただ図形の内側に玉を揃えるのが面白いという遊び心からの行動であると思われるが，いずれにせよ，「ランダムに玉をまく方法と，きれいに隙間なく玉を整列する方法ではどちらが正確な円周率を求めることができるか」というこの実験の本質に迫る疑問を生じさせることができた。この疑問を生徒に投げかける授業展開もよいと考える。

なお，疑問への解答例は次のようである。「ランダムに玉をまいた結果はばらつきがあるので，比較すると整列する結果の方が円周率に近いことが多い。しかし，それは真の値ではない。整列した玉にも隙間があるので，より真の値に近づくためには，玉をできるだけ小さくしなければならず，物理的に限界がある。ランダムにまく方法は時間はかかるが，数多く実験することでより真の値に近づくことができる。」

３．秘密鍵と公開鍵の教材

3.1　教材のねらい

通信データの暗号化について学習する場合，送信者と受信者が，互いに同じ秘密鍵を使用して暗

号化と復号化を行う共通鍵方式については容易に理解できる。しかし，送信者と受信者が異なる鍵を使用する公開鍵方式については理解に苦しむ生徒も多い。その理由として，①１つの鍵で錠を開け閉めできる鍵は現物（モノ）として身近にあり，その概念を持っている。しかし，閉めることだけ，あるいは開けることだけしかできない鍵は現物として身近にないので，その機能が想像できない。②公開が可能な鍵をどのように使用するのかわからない，が考えられる。そこで，秘密鍵と公開鍵の現物モデルを作り，秘密鍵と公開鍵による暗号化と，通信文と鍵の伝送をロールプレイで体験できる教材を開発した。

3.2　教材の構造

この教材は図３のように，平文に見立てたボタン状のフェルト，平文を入れる厚紙の箱，箱に平文を出し入れるために使う厚紙でできた秘密鍵と公開鍵からできている。

秘密鍵の使用法は，図４①のように平文（フェルト）を箱の右側から秘密鍵を使い箱の中へ押し込む。平文と箱には適度な摩擦があるので押し込んだ状態で静止している。この時，平文は外部から読めず，暗号化された状態となる。復号化するには，箱の上側から図４③のように秘密鍵を押し込み，図４④のように下方に平文が押し出された状態になれば復号化されたことになる。復号化できる鍵は，暗号化に使用したものと同じ形状の秘密鍵だけであり，図４②のように異なる鍵では復号化できない。

公開鍵の使用法は，図５①のように平文（フェルト）を箱の右側から公開鍵を使い箱の中へ押し込む。この時，平文は外部から読めず，暗号化された状態となる。復号化するには，箱の上側から図５③のように公開鍵とペアの秘密鍵を押し込み，図５④のように下方に平文が押し出された状態になれば復号化されたことになる。図５②のように暗号化で使用した公開鍵では復号化できない。

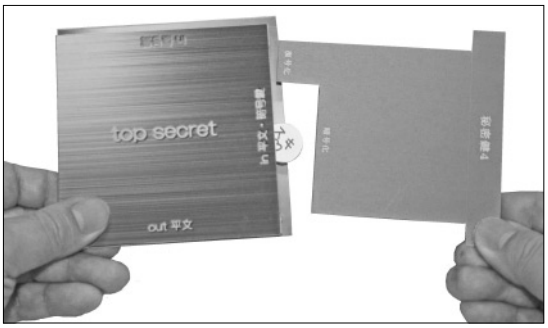

図３　秘密鍵と公開鍵の教材

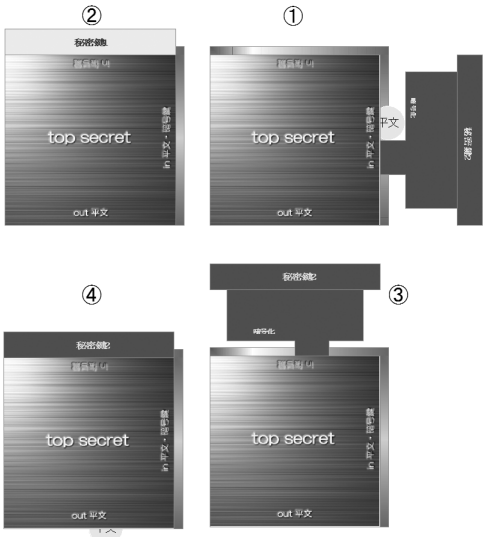

図４　秘密鍵の使用法

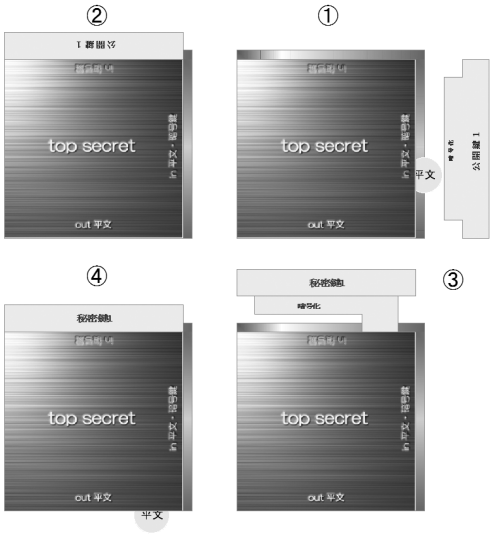

図５　公開鍵の使用法

3.3　実験方法

生徒は数人のグループになり，送信者，受信者，手渡し役（ネットワーク）の３つの役割に分かれてロールプレイを行う。実験はワークシートの指

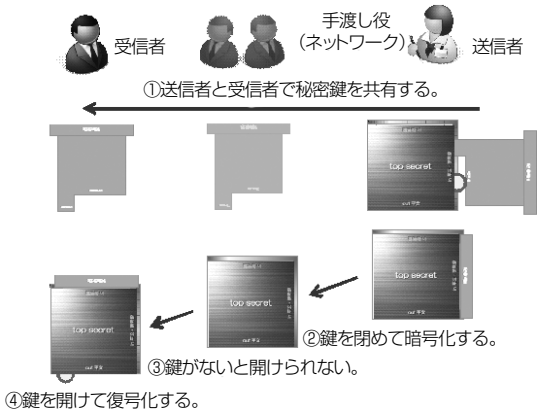

図6　秘密鍵による暗号化と復号化

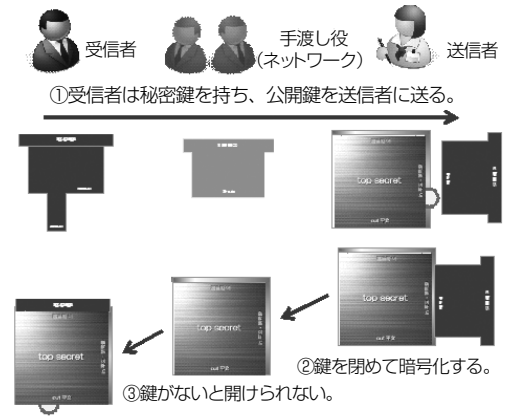

図7　公開鍵による暗号化と復号化

示に従って行われる。実験の中で，質問シートに解答させる。

実験 1　秘密鍵で暗号化した文章を送る（図 6）

①送信者は受信者に手渡し役を介して秘密鍵を送る。

②送信者は同種の秘密鍵で平文を箱に入れる。

③送信者は手渡し役を介して箱を送る。

④受信者は秘密鍵で平文を箱から出して読む。

質問

A　平文を手渡し役が読めないように暗号化できたといえるか。

B　手渡し役が悪意を持ったとき，箱を開ける方法はあるか。

C　１人の送信者が複数の受信者と交信する場合，鍵の数はどうなるか。

実験 2　公開鍵で暗号化した文章を送る（図 7）

①受信者は送信者に手渡し役を介して公開鍵を送る。

②送信者は送られた公開鍵で平文を箱に入れる。

③送信者は手渡し役を介して箱を送る。

④受信者は秘密鍵で平文を箱から出して読む。

質問

A　平文を手渡し役が読めないように暗号化できたといえるか。

B　手渡し役が悪意をもったとき何ができるか。

C　送信者と受信者が互いに交信する場合，秘密鍵と公開鍵をどのように所持すればよいか。

3.4　教材の特長

この教材の特長をまとめると次のようになる。

・公開鍵の機能を体験することができる。

・ネットワークの危険性について気づかせることができる。

・「なりすまし」に対応するためには，別途「認証」の仕組みを作らなければならない。

3.5　授業の様子

情報科担当教員の研修会と大学の授業でこの教材の製作及び実験を行い，その様子を観察した。

当初は公開鍵の構造に興味関心が集中するが，ロールプレイが進むと，公開鍵の使用法が理解できてくる。そして，手渡し役が秘密鍵を入手したり，送信者になりすまして別の平文を送るなどのいたずらをすることで，セキュリティの重要性を体感させることができた。

なお，実際は公開鍵の暗号化には時間がかかるため，長い平文を暗号化することはなく，秘密鍵の暗号化や認証に使用される。この教材をもとに，実際の暗号化について学習を展開する必要がある。

4．おわりに

今回紹介した教材を使用すると，「いたずら」や「あそび」「話し」をはじめる学習者がいる。このような行動は，「工夫」「応用」「やる気」の現れと考えられ，体感を伴う教材を使用することで，活気のある授業を行える。

教材資料提供

URL　http://www.ssu.ac.jp/home/~h-taka/