ＰＤＡと手書き数式インターフェースを用いた実践授業について

藤本 光史
福岡教育大学 教育学部 情報教育講座
〒811-4192 福岡県宗像市赤間文教町 1-1
e-mail: fujimoto@fukuoka-edu.ac.jp

鈴木 昌和
九州大学大学院 数理学研究院
〒812-8581 福岡市東区箱崎 6-10-1
e-mail: suzuki@math.kyushu-u.ac.jp

金堀 利洋
筑波技術大学 障害者高等教育研究支援センター
〒305-0821 茨城県つくば市春日 4-12-7
e-mail: kanahori@k.tsukuba-tech.ac.jp

概要

普通教室でコンピュータを文房具のように手軽に扱うことは難しい。パソコンは起動に時間がかかり、ノート型であっても机を占有する。多機能電卓は場所を取らず起動も速いが、解像度が低く、キー操作が複雑である。これらの欠点を埋める候補として PDA が挙げられる。我々は、PDA の手書き入力に数式入力を新たにサポートし、入力された数式を数式処理ソフトで処理し、結果を GUI 表示するシステム AsirPad を開発した。さらに、中学生・高校生向けに RSA 暗号を題材にした教材を作成し、このシステムを用いた実践授業を行った。本稿は、この実践授業についての報告である。

１．はじめに

近年の教育現場におけるコンピュータの普及に伴い、国語や数学などの普通教科の授業におけるコンピュータ利用の実践事例が数多く報告されるようになってきた。しかし、その多くは、授業の最初から最後までコンピュータを積極的に使うような大掛かりなものであり、5 分あるいは 10 分といった短時間利用のものは見られない。

これは、現在の教育現場で導入されているコンピュータが、定規やコンパスのように手軽に利用できる状態ではないことを意味している。パソコン教室での普通教科の授業は、教科書やノートを開くスペースがなく、児童・生徒の関心がパソコンに集中してしまう、という問題がある。普通教室においても、パソコンの起動に時間が取られ授業が中断してしまう、一人一台のパソコンを置くスペースがない、という問題がある。グラフ電卓を利用する事例もあるが、解像度が低く、キー操作は複雑である。これらの欠点を埋める候補として PDA(Personal Digital Assistants)が挙げられる。PDA は場所も取らず、起動が速く、解像度も高い。何よりも手書きで文字が入力できる。これだけでも小・中学校での総合学習の時間における「調べ学習」に利用可能である。

また、手書き数式インターフェースを用いれば、複雑なコマンドを知らなくとも、数式を入力し、計算を実行することが可能であると考えられる。中学校及び高等学校の数学の授業において、この手書き数式インターフェースを備えた PDA が有効であることを検証することが本研究の目的である。そのために、我々が開発した手書き数式インターフェースを有する数式処理システム AsirPad が利用可能な場面を調査し、授業設計を行い、教材を作成し、実践授業を実施した。

２．これまでの研究の経緯

我々は、1998 年より数式 OCR・手書き数式インターフェース・e ラーニングシステム・Web アクセシビリティに関するアルゴリズムとシステムについて研究を行ってきた。

1999 年に、オフライン数式認識の研究からオンライン手書き数式認識の必要性を認識し、効率的なアルゴリズムの研究を行い、手書き数式インターフェースを備えた Windows 用の数式文書作成ソフト InftyEditor（図１）を開発した。2002 年に、InftyEditor に OpenXM プロトコルを利用して、様々な数式処理システムと通信し、数式の計算を行う機能を実現した。また、動作が軽快で非常に高性能な計算エンジンを有するオープンソースの数式処理ソフト Risa/Asir を Linux OS

On a classroom experiment using PDA and handwriting interface.
M.Fujimoto
Department of Information Education, Fukuoka University of Education.
M.Suzuki
Faculty of Mathematics, Kyushu University.
T.Kanahori
Research and Support Center on Higher Education for the Hearing and Visually Impaired, Tsukuba University of Technology.

搭載の PDA である Zaurus に移植した。

さらに、2003 年、福岡県産業・科学技術振興財団より助成を受けて、PDA の手書き入力に、数式入力を新たにサポートし、入力された数式を数式処理ソフトで処理し、結果を表示するシステム AsirPad（図２）を開発した。

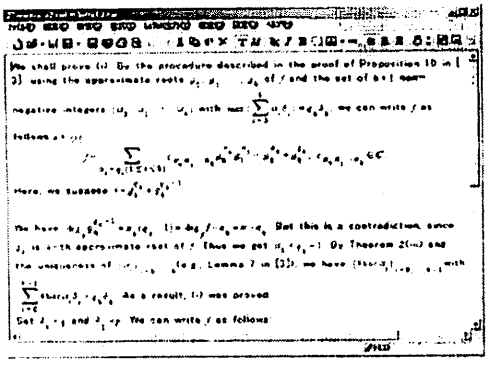


図 1　InftyEditor

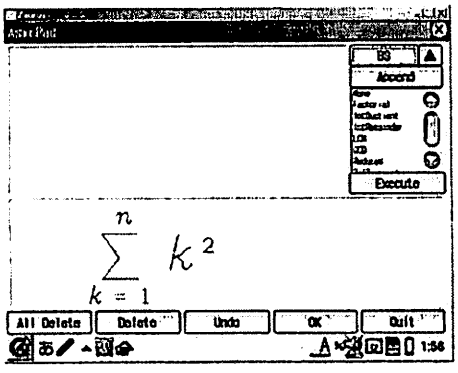


図 2　AsirPad (English version)

３．システム概要

○ハードウェア

本研究で使用した PDA は、シャープ社製の Linux OS 搭載した Zaurus SL-C700 シリーズである。選定理由は、(i)現時点で PDA としては最も高速な CPU を搭載している (ii)画面の解像度が VGA(640x480)である (iii)OS が Linux である、の３点である。これらは、利用する数式処理ソフト Risa/Asir が UNIX 系の OS 用に開発されていること、手書き数式入力の際にできるだけ滑らかな線で描画すること、そして、数式認識にはある程度の CPU パワーを必要とすること、が求められるからである。

○ソフトウェア

AsirPad のインターフェースは手書き数式入力部、数式表示部、そして、計算実行部の３つの部分から構成されている（図３）。手書き数式入力部は、PDA の画面のほぼ下半分を占め、そのエリア内であれば、どこに数式を書いてもよいようになっている。スタイラスを離す毎に、それまでに書かれた文字が認識され、きれいなストロークで適切な大きさに再描画される。いくつかの文字については、スタイラスを離しても直ちには認識されない。別の位置に次の文字を書き始めるか、何も書かずに１秒以上たつと、認識が行われる。強制的に認識させたい場合は、数式をクリックする。認識結果を次候補に変更する場合も、その数式をクリックする。「OK」で画面上方の数式表示部に認識結果が反映される。そこには、数式の計算結果も表示される。縦及び横スクロールに対応しており、必要な場合に、スクロールバーが出現する。数式表示部に表示されている数式に対して計算を実行するには、画面右上の計算関数一覧から関数を選択後、「実行」を押す。すると、計算結果が数式表示部に表示される。

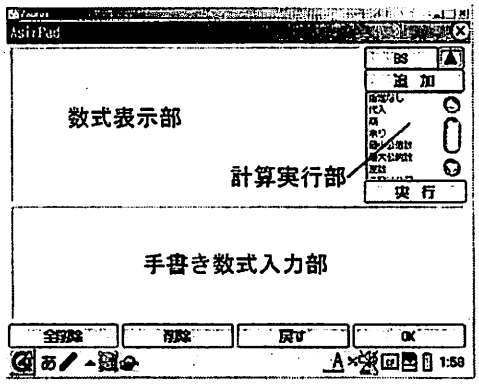


図 3　AsirPad（中学校バージョン）

４．教材について

福岡県田川市立弓削田中学校にご協力いただき、公開形式で実践授業を行うこととした。実施時期は平成１７年３月となった。当初は数学教科書にある単元から教材を選択することを考え、「分数計算」、「連立一次方程式」、「正多面体が５種類あることの証明」などを教材候補にしていた。しかし、実施時期が年度末ということもあり、検討の末、教科書にない RSA 暗号を教材に選んだ。

AsirPad を用いて RSA 暗号を効果的に学習するために、以下のようにインターフェースの改良

を行った。

・整数のかけ算　４７×６１のように積演算子×も含めて手書きで入力するようにした。

・最大公約数の計算　AsirPad では、引数を２個以上必要とする計算のために、「追加」ボタンを用意しているが、縦に２つの数が並ぶのは、生徒達に見慣れていないと判断し、カンマ","で区切って横方法に並べるようにした。

・n を法とする e の逆数計算　この計算については、意味を理解することが困難と思われたので、「ed÷n の余りが１となる数 d」とだけ説明し、n,e を入力後、逆数計算を実行する関数を選択するだけで計算できるようにした。

・べき乗計算　「31^21」ではなく、31 の右上に 21 を手書きで入力できるようにした。

・割り算の余りの計算　「a÷b」のように除演算子÷も含めて手書きで入力するようにした。結果の表示については、「c...d」という商と余りを同時表示することも検討したが、今回のケースでは、商が非常に大きくなるため、見づらくなることがわかった。そこで、余りのみを求める関数を用意し、それを選択するようにした。

・素因数分解計算　素因数分解は中学３年生で学習する内容であるため、素因数分解を行う関数名は「素数に分解」と表現した。

また、暗号化したり復号化するとき、何度も同じ数を入力しなくてもよいように、変数への数の代入機能も用意した。その他にも、過去の入力をできるだけ再利用できるように引数の順序を工夫し、手書き文字の辞書も使用する文字だけに変更した。

５．実践授業実施計画

○実施期日　平成１７年３月１０日（木）５時限 13:20～14:40　（８０分間）

○実施学級　田川市立弓削田中学校　２年１組　毛利学級（３５名）

○授業者　藤本光史

○授業補助　藤本研究室所属学生５名

○授業内容　「RSA 暗号について」

○授業形態　普通教室での６班による班別学習，補助プリントを使用

○使用機器

・PDA　生徒用６台，教師用１台，予備用３台

・ノートパソコン　１台（教師用）

・プロジェクター　１台

・デジタルビデオカメラ　１台（記録用）

・デジタルカメラ　１台（記録用）

○授業評価　授業終了後にアンケート（生徒・見学者・授業補助者）を行う

○授業の進行予定

①授業者の紹介（２分）

②割り算の余りに関する簡単なトリック（５分）

生年月日を９で割った余りを暗算で求める方法（各桁の数を足したものを９で割って余りを求める）を紹介することで、普段見過ごしがちな割り算の「余り」に注目させる。

③共通鍵暗号の仕組み（５分）

パワーポイントのアニメーションにより、共通鍵暗号の仕組みと問題点を解説する。

④公開鍵暗号・RSA 暗号の仕組み（５分）

共通鍵暗号の解説と同様に、パワーポイントのアニメーションにより、公開鍵暗号の仕組みを解説し、共通鍵暗号との違いを気付かせる。

⑤PDA を利用した鍵の生成（１５分）

班毎に PDA を１台配布し、簡単に使用方法を紹介した後、手書きで数式を入力させ、鍵を生成させる。

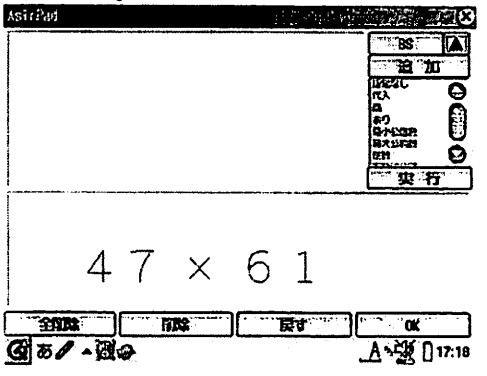


図 4　まずは掛け算で練習

⑥暗号文を作成（１５分）

メッセージを変換表により数字に変換させ、送信相手の班の公開鍵を用いて、暗号化させる。

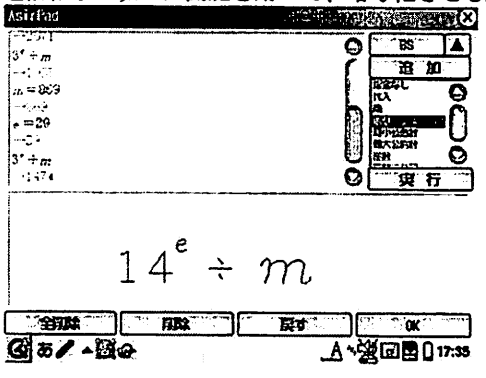


図 5　暗号化のための入力例

⑦暗号文からの復号（１０分）

別の班から渡された暗号文を自分達の班の

秘密鍵を用いて、複合化させる。

⑧暗号破り（１０分）

公開鍵から秘密鍵を見つけるには、何がわかればよいか考えてもらい、「素数に分解する」ことが重要であることに気付かせる。

⑨なぜRSA暗号は安全か？（３分）

最新の RSA 解読結果を示し、素数に分解するには、どれくらい時間がかかるのか解説する。そして、現実的な時間で解くことができないことが、暗号としての保証になっていることに気付かせる。

⑩まとめ（２分）

⑪アンケートの記入（８分）

６．授業の様子

授業の最初の 20 分間は、プロジェクターを用いての一斉授業の形態をとった（写真１）。

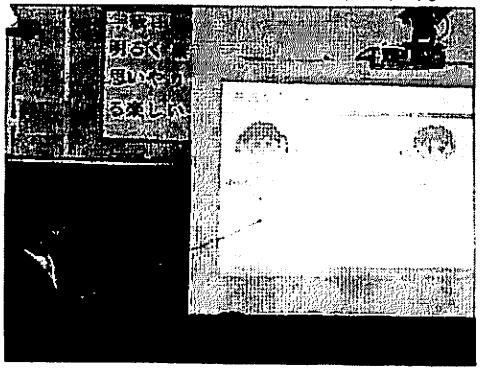


写真 1　公開鍵暗号の仕組み

割り算の余りに関する簡単なトリックを紹介し、「余り」に興味を持ってもらった後で、RSA 暗号の仕組みを簡単に解説した。その後、６班に分かれての班別学習に移行した。各班に１台の PDA を渡し、RSA 暗号を体験する作業を行った（写真２）。

写真 2　各班に１個のＰＤＡ

数式の手書き入力の方法はあえて説明しなかったが、ほとんどの生徒が使いこなし、驚くべき速さで数式を入力していった（写真３）。

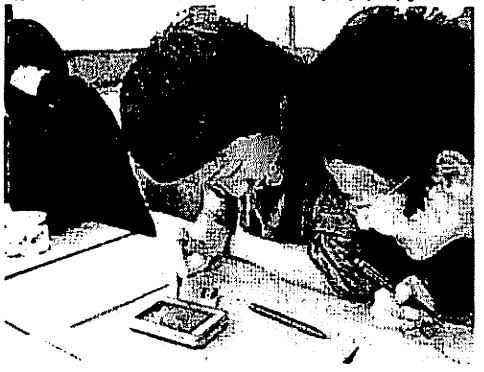


写真 3　手書き数式入力中

各班で PDA を用いて公開鍵を作成し、その公開鍵を発表してもらった（写真４）。この公開鍵を用いて、別の班に送る暗号文を作成した。

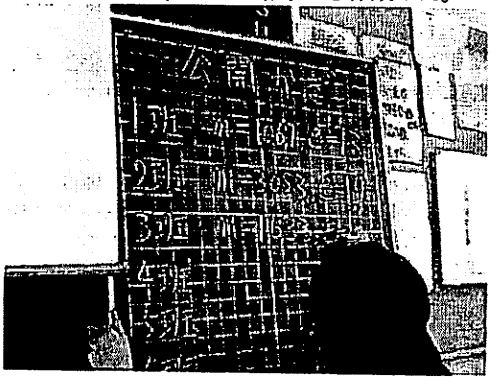


写真 4　公開鍵の発表

机の上にプリントを広げた状態でも PDA は利用可能であった（写真５）。

写真 5　ノートの上でＰＤＡを利用

暗号メッセージの変換については、すべての班がメッセージの暗号化及び暗号の復号化に成功した。実際の授業は、予定を 10 分オーバーし、全体で 90 分間になった。ほぼ予定通りの進行であったが、手書きインターフェースを利用した鍵の生成の部分で、24 分間かかった。これは、生徒達がはじめて PDA に触れて、使い方に慣れるまで少し時間を要したことによる。

生徒達は素数についてまだ習っていなかったが、簡単な説明をしたところ、大きな混乱はなかった。6 台中 2 台の PDA が授業中数回ハングアップしたため、予備機に切り替えて対応した。

7．授業の考察

RSA 暗号については、大学の授業でもなかなか理解してくれない内容なので、中学生がどこまで理解できるか心配したが、アンケートの設問 1 及び 2 から、概ね理解できたとの回答が得られた。理解度を測るための試験は行わなかったため、どの程度理解しているかは不明であるが、少なくとも公開鍵暗号の仕組みと RSA 暗号の概要は理解できたようである。今回の授業では、RSA 暗号の暗号化と復号化を実際に体験し、概要をつかむことができればよいと考えていたが、ここまでは達成できたようだ。さらに、秘密鍵を用いて暗号文から平文を復号できることに疑問を持って欲しいと期待し、そのような生徒が自分で学べるように参考になる Web ページの URL を補助プリントの最後に挙げておいたが、アンケートの感想や授業中の様子から、そこまでは到達していなかったようである。

手書き数式インターフェースの有効性を検証するために、生徒達には使用法について、ほとんど説明しなかった。しかし、設問 9 の結果を見ると、説明は十分だったという回答がほとんどであり、そして、見学者の「初めて PDA を使ったのにも関わらず、上手に使いこなせていた」という感想から、問題なく利用できたようである。ただし、設問１０の結果から、多くの生徒が自分の意と異なる認識結果に遭遇したことがわかる。この部分については、ある程度の慣れが必要かもしれない。研究室の学生に対して行った予行演習では、メッセージの暗号化と復号化に非常に時間がかかっていたが、授業では、非常にスムーズに作業を行うことができた。これは、同じ数を何度も入力しなくてもよいように導入した代入機能が大きく貢献した。授業中、手書き文字を修正する際に、思わず消しゴムを手に取った生徒がいた。これは、手書き入力が違和感なく生徒達に受け入れられた証拠といえる。

「また PDA を使ってみたい」という感想が多く、PDA に対する生徒の関心は、非常に高いことがわかった。設問 5 からは、PDA は普通教室で机の上にノートやプリントを広げた状態でも邪魔にならず利用可能なことが明らかになった。設問 8 の回答として、半数以上が普通教室での使用に適したコンピュータとして PDA を選んでいるが、その理由として「邪魔にならない」,「使っていて面白い」という意見が多かった。

見学者の教師の感想「授業がありましたので、60 分を過ぎた頃に参観させていただきましたが、生徒達が思っていた以上に授業に意欲的に取り組んでいたのに少し驚きました。」や生徒の感想「難しかったけどけっこうがんばれた。」が示すように、中学生には未経験の９０分近くの授業に関わらず、最後まで彼らの集中力は切れなかった。このように、PDA と手書き数式インターフェースの活用によって、生徒の興味を持続させ、学習意欲を高めることができた。

8．おわりに

以下に今回の実践授業で明らかになった点をまとめる。

① 机の上にノートやプリントを広げた状態でも、PDA は問題なく利用可能である。
② 手書きによる数式入力は、特別な訓練を必要としない。
③ 手書き数式インターフェースを用いれば、数式の計算実行に複雑なコマンドは不要である。

反省点は、PDA の台数が少なかった点である。5 人または 6 人に 1 台の PDA では、PDA に触れる時間が限られてしまう。3 人に 1 台あれば、一人で試行錯誤する時間も長くなり、作業効率ももっと上がると考えられる。

最後に、今後の課題として、以下を挙げる。

・PDA 上での手書き入力と紙上での鉛筆との書き心地の違いについて調査を行う。
・PDA のハングアップのないように改良する。
・下添え字は中学では使用しないので、これもオフにできるように仕様変更する。
・引数のカンマの入力をしやすくする。

参考文献

1) T.Kanahori, M.Fujimoto, M.Suzuki: Authoring Tool for Mathematical Documents − Infty −, Proceedings of the Workshop on Mathematical User Interfaces, online, (2004) 9 pages.

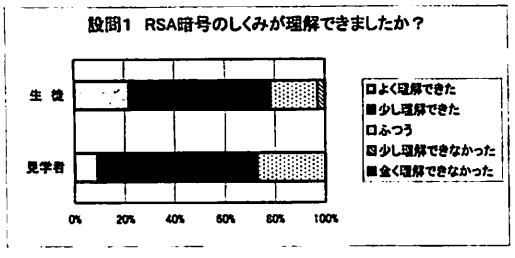
http://www.activemath.org/%7Epaul/MathUI/proceedings/Authoring_Infty.html

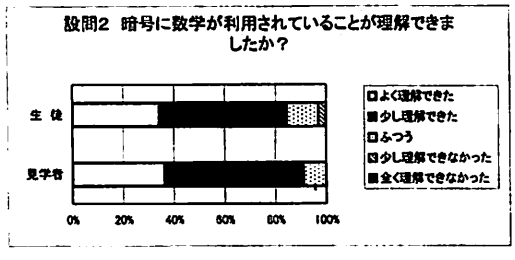
2) M.Fujimoto, M.Suzuki: AsirPad － A Computer Algebra System with a Pen-based Interface on PDA, Proceedings of the Seventh Asian Symposium on Computer Mathematics, Korea Institute for Advanced Study, (2005) 259 - 262.

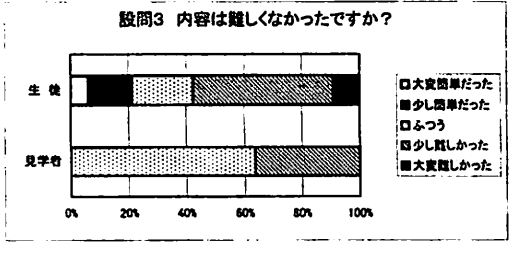
付録１　アンケート結果

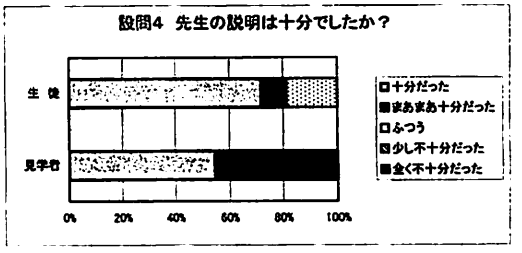
授業終了後に生徒と見学者に対してアンケート調査を行った。以下はその結果である。なお、記述されている設問項目は、すべて生徒用のアンケート用紙に書かれていたもので、見学者用のアンケート用紙には、「生徒は・・・理解できたと思いますか？」と若干変更してある。

○授業内容について

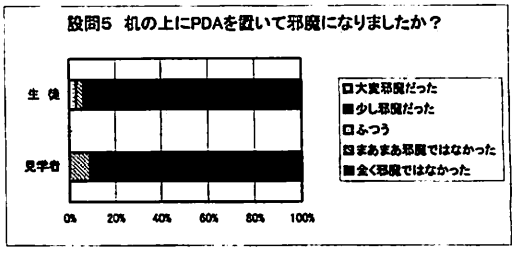


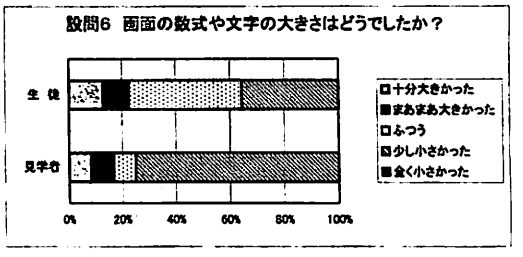


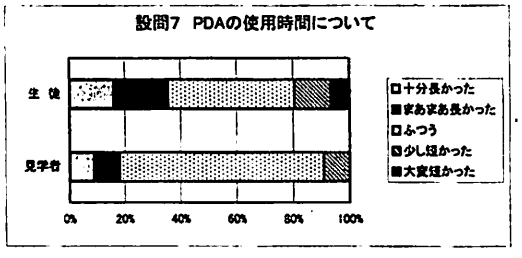


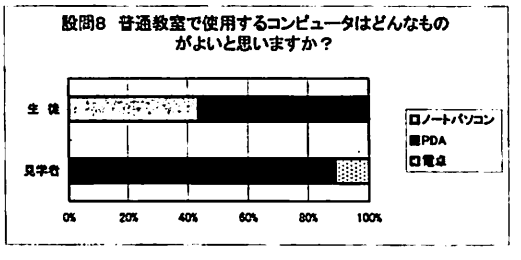


○PDAについて

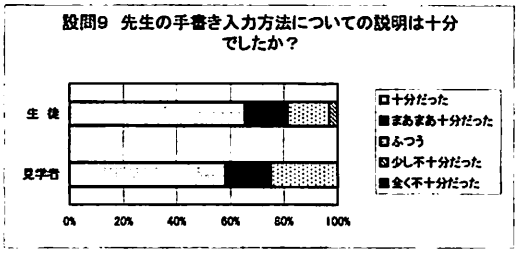


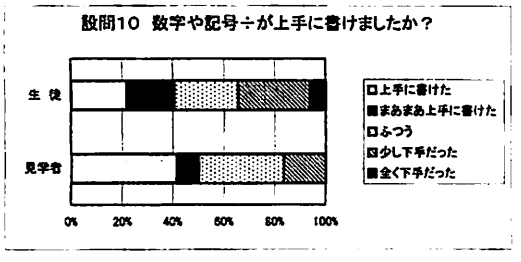


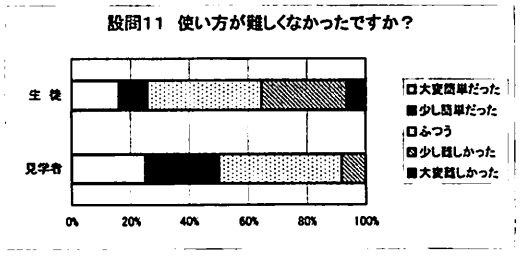




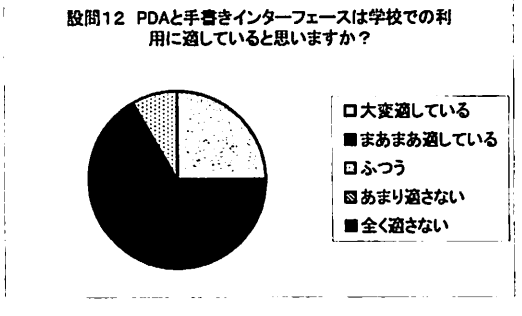
○ 手書き入力について







○見学者のみに対する質問



○生徒の感想（複数回答）

・とても楽しい授業だった（13名）
・とても面白かった（9名）
・わかりやすい授業だった（11名）
・またPDAを使ってみたい（10名）
・簡単に計算できて便利（4名）
・暗号を解いていくのがわくわくした（4名）

○見学者の感想

・初めてPDAを使ったのにも関わらず、上手に使いこなせていた（5名）
・ふだんより長い授業だったが、生徒は大変興味を持って意欲的に取り組んでいた（4名）

付録2　授業プリント「RSA暗号に挑戦」

1　かぎを作ろう

1. 2桁の2つの素数 $p=$ □, $q=$ □ を選びます。
2. $pq=$ □ … この数を m とします。
3. $(p-1)(q-1)=$ □ … この数を n とします。
4. n との最大公約数が1になる数 e を見つけよう！
   → $e=$ □
5. $ed \div n$ の余りが1となる数 d（n についての e の逆数）を見つけよう！
   → $d=$ □

これで暗号の「かぎ」の準備ができました。あなたの班の公開かぎと秘密かぎは次の数です。

公開かぎ：$m=$ □, $e=$ □　　秘密かぎ：$d=$ □

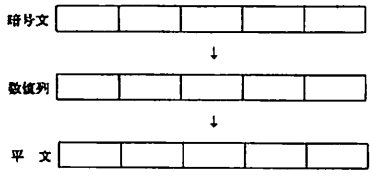
2　暗号文を作ろう

では、第□班にメッセージを暗号化して送りましょう。第□班の公開かぎは $m=$ □, $e=$ □ です。5文字以内のメッセージ（平文）をみんなで考え、それを3ページ目の変換表を使って数位列にして下さい。次に、M をある文字を変換した数とします。$M^e \div m$ を計算し、その余りを暗号と考えます。

平文					
	↓				
数位列					
	↓				
暗号文					

3　暗号文を平文に戻そう

では、もらった暗号文から元のメッセージ(平文)を復元しましょう。私たちの班の m と秘密かぎ d は $m =$ [　　], $d =$ [　　] です。C をある数(暗号)とします。次に $C^d \div m$ を計算し、その余りが平文になります。



4　暗号破りに挑戦

2. で作った暗号文は自分で作ったものなのに、元の平文に戻すことができません。送り先の相手の秘密かぎ d がわからないからです。では、送り先の公開かぎ m と e から秘密かぎ d を見つけるにはどうすればよいでしょうか?

方針：　暗号を解読するためには

[　　]

を求めればよい。

では、上の方針に従って、暗号を破ってみましょう。

第[　]班の秘密かぎは[　　]だ!

■2桁の素数達

11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

■変換表

	0	1	2	3	4	5	6	7	8	9
0	a	b	c	d	e	f	g	h	i	j
1	k	m	n	l	o	p	q	r	s	t
2	u	v	w	x	y	z	あ	い	う	え
3	お	か	き	く	け	こ	さ	し	す	せ
4	そ	た	ち	つ	て	と	な	に	ぬ	ね
5	の	は	ひ	ふ	へ	ほ	ま	み	む	め
6	も	や	ゃ	ゆ	ゅ	よ	ょ	ら	り	る
7	れ	ろ	わ	を	ん	゛	゜	、	。	,
8	.	・	!	#	$	¥	%	&	(	)
9	@	?	〜	<	>	／	*	+	−	=

(例) 「d」→「03」→「3」,「あ」→「26」,「！」→「82」

■参考になるかもしれないWebページ

- サルにもわかるRSA暗号
  http://www.maitou.gr.jp/rsa/
- 高校生のための暗号論入門
  http://www.nikonet.or.jp/spring/sanae/report/angou/angou.htm