RSA暗号の教材化についての一考察

福井大学教育実践研究　2010，第35号，pp.87－95

教育実践報告

RSA暗号の教材化についての一考察

福井大学大学院教育学研究科　岡　本　理　生
福井大学教育地域科学部　伊　禮　三　之

「数学はいろいろなところで役に立っているにもかかわらず，国内外の諸調査でそのことについての生徒の意識が低いことが明らかになっている。日常事象を数学の眼でとらえたり学んだ数学を日常生活で生かしたりする学習を通して，数学が役に立つことを生徒に実感できるようにすることが重要である」（平成15年度教育課程実施状況調査教科別分析と改善点）と指摘されて久しい。今日の中･高校の数学教育は，受験プレッシャーもあるが，ほぼ学問的体系としての数学の学習に重点が置かれすぎ，学習者にとってその実用的な意義が見えにくいものになっている。

本稿では，現在の情報化社会において大きな役割を担っているRSA暗号を取り上げ，その中にある数学を考えることによって，数学が日常生活に生かされていることや役に立っていることなど数学の有用性の実感を促していくような教材開発をおこなうとともに，その実践の考察を通して，数学的問題解決の図式の「確認」の活動の意義を確認した。

キーワード：有用性，数学的問題解決，フェルマーの小定理，RSA暗号

1．はじめに

伏見・麻柄（1993）によれば，社会的な有用情報は，生徒の学習に関する興味・関心を高め，さらに認知面の定着についても良好であることが明らかにされている。そして，平成20年度全国学力・学習状況調査の教師に対する質問調査によると，多くの中学校教師は数学と実生活とを関連させて授業を行っていると回答しており，生徒たちに数学の有用性を伝えようとしていることがわかる。残念ながら，それに反して多くの生徒は，数学は現実には役に立たないと考えているのが実情である（表1）。

表１　平成20年度全国学力・学習状況調査より

	当てはまる
数学の授業で学習したことを普段の生活の中で活用できないか考えますか	10.9（%）
数学で学習したことは，将来，社会に出たときに役に立つと思いますか	30.9（%）

つまり，教師の方は数学と実生活を関連させることでその有用性を伝えようと努力しているのにもかかわらず，生徒たちにはそれがうまく伝わらず，教師と生徒の意識が乖離しているのである。

では，数学の有用性を生徒たちに実感させるためには，どうしたらよいのだろうか。

銀林（1987）は，数学的問題解決の過程を図1のように，①現実世界の課題を数学の問題に定式化し，②これを数学的技法を用いて解を求め，③この解を現実世界で解釈し直してもとの課題の解決とする，と整理した。

つまり，④現実の課題をそのレベルで直接解決するのではなく，一度数学の世界を通す《まわり道》を経て解決するところにその特徴があるというわけである。この図式を参考にすると，数学の有用性を生徒たちに実感させるためには，問題解決の成否が直ちにフィードバックされ，数学による解が現実問題の適切な解決となっていることを「確認」する④の過程こそ重要だということがわかる。これまでの数学教育では，④の過程が不足していたのではないか。

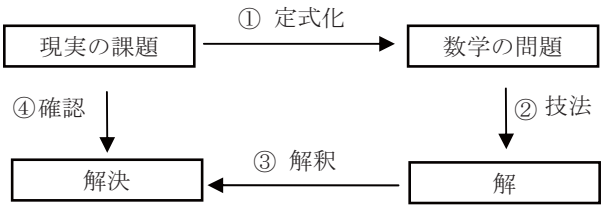


図１　数学的問題解決の図式

本稿では，以上のようなことを踏まえ，生徒が数学の有用性を実感することができるような教材について考察していく。

2．ＲＳＡ暗号と，その数学的内容

情報社会と呼ばれている現代において，暗号技術はとても重要なものとして考えられている。その現代暗号は大まかに共通鍵暗号と公開鍵暗号に分けられる。共通鍵暗号では，相手へメッセージを暗号化して伝えたい場合，その暗号化に使う鍵を周囲の人に秘密にして，相手だけに伝えなければいけない。つまり，相手にメッセージを

暗号化して伝えられていたとしても，鍵を相手に伝えることができなければ，相手はメッセージを解読することができないのである。そこで，鍵はどのようにして周囲の人に秘密にして相手に伝えればいいのか，という問題が浮上する。しかし，この問題は共通鍵暗号では，仕方のないことと考えられてきた。

この問題を見事に解決したのが，公開鍵暗号なのである。公開鍵暗号では，この問題を解決するために，鍵を公開鍵と秘密鍵の2種類用意する。つまり，公開鍵を全体に公開し，どの人にも，その公開鍵を使って自分宛の暗号文を作成してもらえるようにする。そして，届いた暗号文を，自分だけが秘密に持っている秘密鍵によって元の文章に復元するのである。このとき，公開鍵と秘密鍵は無関係ではなく，互いに関係をもち作成されている。

そして，この公開鍵暗号の代表とされるのがRSA暗号である。ちなみに，このRSAとは開発者3人Rivest−Shamir−Adlemanの名前の頭文字を取って付けたものである。RSA暗号は，素因数分解の限界を基として考えられており，その内容には，ユークリッドの互除法や二項係数といった，高等学校学習指導要領の整数の性質の内容が含まれている。そして，それらの内容と同様にRSA暗号の中心的内容をなしているのがフェルマーの小定理である。フェルマーの小定理は

$x^{(n-1)} \equiv 1 \pmod{n}$（nは素数，xとnは互いに素）

といった内容である。これは，ある数xとnが互いに素であり，nが素数である場合，xをn−1乗して，それをnで割った余りは必ず1になる，という内容である。これを初めて知る生徒にとっては不思議な性質であり，生徒の興味を引くことが期待できる内容である。このときのmodとは，モジュラ計算（modular arithmetic）のことで，自然数あるいは整数をある特定の自然数で割ったときの剰余に注目して解決していく方法である。

3．授業計画

(1) 授業の構想

本実践では，高等学校第1学年を対象に2時間分（1時間は50分間）授業を行う。高等学校数学科（2009）の目標に「数学のよさを認識し」という文言がある。そして，高等学校学習指導要領解説（2009）には，次のように述べられている。

「数学のよさ」には，数学的な見方や考え方のよさ以外に，数学の概念や原理・法則のよさ，数学的な表現や処理の仕方のよさが含まれ，さらに高等学校では，数学の実用性や汎用性などの数学の特長や，数学的活動や思索することの楽しさなども含まれる。

そこで，本実践を行う上では，①整数の性質の不思議さを感じ，その性質を理解すること，②整数の性質を用いて，課題を解決する「確認」の活動を行い，数学の有用性を実感すること，の2点を重要視した。そして，RSA暗号は先にも述べたとおり，数学的内容を数多く含んだ題材である。そのため本実践では，2時間扱いと少ない時数のため，上の2点に絞って授業を展開する必要がある。

まず，①についてだが，RSA暗号に含まれている数学的内容から，本実践においては，フェルマーの小定理を中心に扱うことにする。その理由は，「整数の性質の不思議さを感じ」という本実践のねらいを重視するためである。「不思議さを感じる」ことは，生徒の数学に対する肯定的な意識につながると考えられる。そして，それは数学に対する興味・関心・意欲にもつながるものであり，数学の授業において重要視されなければならないものである。そして，フェルマーの小定理には，

$$x^{(n-1)} \equiv 1 \pmod{n}$$

というように，1が並ぶ美しさがある。さらに，すべてのnにおいて成り立つのではなく“nは素数，xとnは互いに素”という条件がある。生徒が自分で計算したときに，法則を発見しようとしたり，成り立たなかったときの条件を探そうとするなど，教師がうまく課題を設定してあげれば，生徒の興味・関心を引き出し，整数の不思議さを伝えることができるかっこうの材料である。

そして，整数の性質を活用し，課題を解決するために，しっかりとそれを理解する必要がある。フェルマーの小定理には，“≡”と“mod”という，生徒がまだ学習したことのない内容が含まれている。そのため，初めから

$$x^{(n-1)} \equiv 1 \pmod{n}$$

という式を出すのではなく，自分たちでこの定理を導き出し言葉で言語化した後に，それを数学的な表現に移すという段階を踏む。なお，“≡”と“mod”を説明するために，カレンダーの日付を利用することにする。

次に，②についてだが，前述したように，多くの生徒は，数学は現実には役に立たないと考えている。そこで，世界で使われているRSA暗号の中に，数学が活用されていることを実感するような，授業展開を考える。ここでは，RSA暗号の中の数学を，フェルマーの小定理とする。そこで，学習したフェルマーの小定理が，実際生活で利用されているRSA暗号に活用されていることを知ることはもちろん重要なのであるが，それだけでは，有用性の実感までには至らない。その後に，実際に生徒間でRSA暗号を使った「確認」の活動を行う必要がある。これによって，生徒の数学の有用性に対する実感は，より深いものになると考える。

以上の①，②を主なねらいとし，授業実践の概要を考える。

(2) 指導案

1．日時　　平成21年11月4日（水）第4時
　　6日（金）第6時
2．学級　　1年3組（33名）

3. 単元名　　「RSA暗号とフェルマーの小定理」

4. 本時について

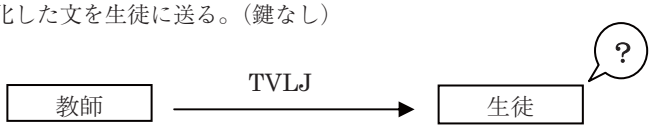
（1）教材名 「RSA暗号とフェルマーの小定理」

（2）本時の目標

RSA暗号，フェルマーの小定理を学ぶこと

を通して，整数の性質の不思議さ，数学の社会的有用性を実感することができる。

（3）学習過程

形態・時間	教師の働きかけ・学習者の反応	留意点
0分	フェルマーの小定理の不思議 ①クラス全員に1～6の好きな数字を思い浮かべてもらう。 ②その数字を6乗してもらう。 ③6乗した数を7で割る。そのときの余りをだしてもらう。 ④それぞれの数に対して，余りが何になったか全体で確認する。 ⑤1～6を1～6乗した数を表で見せ，6乗した時のみ1～6のすべての数の余りが1になっていることを確認する。 ⑥他の例として，1～ 12の数を12乗し，その数を13で割ったときの余りの数を表にまとめて見せる。(mod13) ⑦法則を探す。 ⑧素数でないと成り立たないことを予測させるため，1～7の数を7乗し，その数を8で割ったときの余りの数についても表で表す。(mod8) ⑨7，13と8との違いを考える。 ⑩「奇数か偶数か」という意見が出たら，さらに素数でないと成り立たないことを予測させるため，mod9 でも成り立たないことを確認する。 ⑪7，13と8, 9との違いを考える。 ⑫フェルマーの小定理を定義する。	・フェルマーの小定理を利用する。 ・計算機を使う。 ・「余りを出す」ということを強調する。 ・パワーポイントを利用する。 (ゆっくり説明) ・すべての数において余りが1になっていることを強調する。 ・12乗は計算機では出来ないが，できるところまで計算してもらう。(残りはパワーポイントで説明)
30分 (現実の課題)	・フェルマーの小定理の名前の由来や証明が簡単に行えることを説明する。 ・現実の課題を考える。 他の誰にも知られることなくメッセージを伝える ・紙にメッセージ（文）を書き，生徒とやり取りをする。(非暗号化)  ・第三者にやりとりの途中に盗聴させ，このまま（非暗号化）ではまずいことを確認する。 ・どのような手段があるか生徒に発言を促す。「暗号」 ・暗号化した文を生徒に送る。(鍵なし)  ・暗号化してメッセージを伝えるためには暗号化する鍵，復元する鍵が必要であることを確認する。  ・共通鍵暗号の弱点を説明する。 →盗聴者が解き方を知っていたら解読されてしまう。 ・共通鍵暗号を説明する。 共通鍵暗号 暗号化するための鍵と復元するための鍵が同一である。 ・公開鍵暗号を説明する。 公開鍵暗号 暗号化するための鍵と復元するための鍵が別々である。	・modの説明を行う。 ・生徒一人を指名し，教師が生徒にメッセージを伝える設定とする。(ロープとハンガーを活用) ・受信した文はみんなに見せるように受信者に促す。 ・平文，暗号文を説明する。 ・受信した鍵で解読してもらう。(みんなには鍵を見せない) ・パワーポイントを利用する。 ・共通鍵暗号の弱点を克服できることを強調する。
45分		

〔2時間目〕 （数学の問題） 【技法】 0分	・公開鍵暗号の代表がRSA暗号で，RSA暗号にフェルマーの小定理が活用されていることを説明する。 ・実際にRSA暗号を説明する。 RSA暗号の説明 〈公開鍵を作る〉 ①二つの素数を考える。ここではp＝3，q＝11とする。 ②pとqの積N＝pqを計算する。pq＝3×11＝33 ③L＝(p－1)(q－1) を計算する。 L＝(3－1)(11－1)＝20 ④ある数eを決める。(eはLと互いに素) ここではe＝7 N＝33，e＝7が公開鍵となる。 〈秘密鍵を作る〉 ⑤e×dをLで割った余りが1となる数dを求める。 つまり7×d≡1(mod20) を求める。このときd＝3 d＝3が秘密鍵となる。 〈暗号化する〉 ⑥平文（伝えたい文）Mをe乗し，Nで割った余りを求める。このときの余りをCとし，これを暗号文とする。ここではM＝5とする。 $M^e=5^7=78125\equiv14\pmod{33}$ C＝14が暗号文となる。 〈復号化する〉 ⑦暗号文Cを秘密鍵d乗し，Nで割った余りを求める。 $C^d=14^3=2744\equiv5\pmod{33}$ 5が復元した文となる。	・資料を配布する。 ・パワーポイントを利用する。 ・ワークシートを配布し，生徒と一緒に進める。
（解） 【解釈】 （解決）	・復号化のからくりを説明する 復号化のからくり C＝14≡5(mod33) なので $C^3=14^3=(5^3)^7\pmod{33}$ $=5^{21}\pmod{33}=5^{1+20}\pmod{33}$ $=5^1\cdot5^{20}\pmod{33}$ $=5^1\cdot5^{(3-1)(11-1)}\pmod{33}$ $=5^1\cdot1=5$	・波線の部分を詳しく説明する。
30分 【確認】	・暗号ゲームを行う。	・班になり，班の中で2グループを作り，送信者・受信者を決めて行う。 ・ワークシートを配布する。 ・簡単な数を選んで行う。（p，q，e，M）

4．授業実践の分析と考察

(1) 授業実践の記録と考察

1) 授業の流れ

①フェルマーの小定理（第1時）

本時は，フェルマーの小定理を実感することから授業に入る。フェルマーの小定理はほとんどの生徒は初めて聞く定理であると考えられるため，いきなり紹介したりするのではなく，生徒自身に法則や条件を見つけてもらうことで，より整数の不思議さを実感できるように促した。

まず，1～6の数を思い浮かべてもらい，それを，電卓を用いて6乗してもらった。そして，6乗した数を電卓ではなく筆算を使って，7で割った余りを出してもらう。そしてパワーポイントを用いて，全員で，6乗した数と，それを7で割った余りの2つを確認していく。そして，余りがすべて1になることを確認したら，n＝13の場合も同様に全員で計算してやってみる。

n＝13でも，余りがすべて1になることを確認したところで，法則を探す時間を与える。このとき，周りの人と相談してもよいことを伝えた。多くの生徒は，「aをn－1乗してnで割ったときの余りが1になる」ということに気づいていたように感じるが，条件まで考えていた生徒はいなかった。5分程度をとった後に，横の生徒と相談していた生徒に聞いてみた。

T ；どうですか？ 何か法則が見つかりました？
S_1；…。
T ；見つからなかったんですか？
S_1；見つかったんですけど…全部確かめようと思ったら，普通に当てはまらないものがでてきてしまったので…。
T ；そうですか，じゃあ，その当てはまらないのを除いて，その考えた法則を教えてください。
S_1；aに○乗して，それを，○に1足した数で割ると，1余る。

T ；おぉ，他の人もこのような感じでいいですかね。まとめるとこうなりますね。

そして，「ある数をn－1乗して，それをnで割ると，余りは1になるようだ」として，他の数で再度計算してみた。そこで次は，n＝8で計算してもらった。すると，余りには1の他に，0，3，5，7が出てきてしまい，S_1が言うように法則に当てはまらない数があることが分かった。そこで，これまでに実際に計算して法則が成り立った（7，13）と，成り立たなかった（8）の間にどのような違いがあるかを考えさせた。

T ；7と13，8何か違いはありますか？
S_2；奇数と偶数。
T ；つまり，奇数では？
S_2；奇数では法則に当てはまるが，偶数では当てはまらない。

そこで，再度，n＝9の場合で計算をしてもらった。すると，n＝9も法則には当てはまらないことが分かった。

T ；ということは，nが9のときも法則には当てはまらないということですね。じゃあもう一回探しましょう。ここにはどんな違いがあると思いますか？
S_3；素数か素数じゃないか。

S_3の発言を聞いた後，パワーポイントを使って，フェルマーの小定理の説明を始めた。ここで，

$x^{(n-1)} \equiv 1 \pmod{n}$（nは素数，xとnは互いに素）

という式が登場するのだが，生徒にとって初めて見る「≡とmod」を説明するために，カレンダーを用いた。

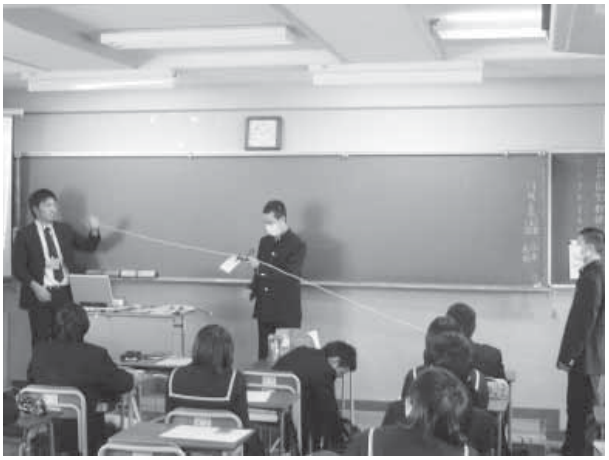
最後に，時間の都合で省略したフェルマーの小定理の証明は，高校生の知識で十分にできるものだから，是非チャレンジして欲しいと伝え，1時間目の授業を終了した。

②復習（第2時）

第1時から2日後に第2時を行ったが，まず，フェルマーの小定理の復習から授業に入った。予定より第1時のフェルマーの小定理に，時間をかけてしまったため，復習はパワーポイントで，「フェルマーの小定理，≡とmod」について口頭で説明するだけにした。

③共通鍵暗号と公開鍵暗号（第2時）

前回学習したフェルマーの小定理と関連のある話で，誰にも知られることなく，ある人にメッセージを伝えたい，という状況での話をすることを伝えた。そして，生徒一人に前に出てきてもらい，私のメッセージを受け取る，受信者役をやってもらった。そしてもう一人生徒に前に出てきてもらい，盗聴者役をやってもらうこととした。このとき，送信者と受信者が1本のロープの両端を持ち，その間に盗聴者がいるようにする。そして，メッセージを送る際には，クリップ付きハンガーにメッセージを挟み，ロープに引っ掛けて送る。そのようにして，まず，共通鍵暗号について説明した。



共通鍵暗号の弱点は，前述したように，暗号文とそれを解読するための鍵を，一緒に送らなければならないことである。そのことを，盗聴者役の生徒に実際に解読してもらうことで，明らかにした。そして，この共通鍵暗号の問題点を改善する方法として公開鍵暗号を，同じように生徒に前に出てもらい，ハンガーとロープを使って紹介する。このとき，公開鍵暗号には，「公開鍵」と「秘密鍵」の2つの鍵があることを強調して説明をした。

④RSA暗号（第2時）

公開鍵暗号の概要を説明した後に，その代表となっているRSA暗号の話をすることを伝えた。そして，最後には，このRSA暗号を使って，隣の席の人と暗号通信をしてもらうことも伝えた。時間の制約のためRSA暗号の説明は，「公開鍵を作る過程，秘密鍵を作る過程，暗号化する過程，復号化する過程」に分けて，すべてパワーポイントで行い，生徒は配布されたプリントの空欄の部分を埋めるだけの活動にした。そして，最後に，復号化のからくりを簡単に説明した。

⑤RSA暗号通信（第2時）

暗号通信は隣の席の人と送信者役，受信者役に別れて行った。このとき，注意として，受信者が任意で決定する数p，q，e，そして送信者が任意で決定するM（学習指導案参照）は，なるべく計算しやすいように簡単な数にするよう伝えた。

⑥複号化のからくり

授業の最後に，復号化のからくりを，板書しながら詳しく説明した。そして，その中には，フェルマーの小定理が利用されていることを強調した。

2）授業実践の考察

本実践は，生徒にとって初めて聞くような内容であるとともに，時間の制約のために教師が説明する時間がど

うしても多くなってしまったが，ここでは，本実践のねらいである以下の2点について，主として検討していくこととする。

①整数の性質の不思議さを感じ，その性質を理解する
②整数の性質を用いて，課題を解決する確認の活動を行い，数学の有用性を実感する

①整数の性質の不思議さを感じ，その性質を理解すること

生徒は，初めて聞くフェルマーの小定理に対して，意欲的に取り組んでいた。それは，nを変える度に行う計算の態度や，法則を探す際の相談の様子などからも分かる。しかし，整数の性質の不思議さを実感できたかには疑問が残る。フェルマーの小定理の中で扱ったのはn＝7，8，9，13の4つのみである。つまり，不思議さを伝えるというよりも，フェルマーの小定理の条件を見つけることを目指した紹介になってしまった可能性があるのだ。不思議さを伝えるのであれば，扱った7，13以外にも大きい数の素数なども扱い，1がよりたくさん並んでいるのを見せると，より伝わったのではないかと考える。

また，フェルマーの小定理，RSA暗号，ともに重要な役割を担っているのが素数である。今回の実践では，フェルマーの小定理，RSA暗号の流れを紹介することが主となってしまったが，素数や素因数分解などにも授業中に触れることができたら，生徒はより実践内容に興味を示していたと考えられる。

そして，その性質の理解度については，アンケート結果の考察で述べることにする。

②整数の性質を用いて，課題を解決する確認の活動を行い，数学の有用性を実感する

「確認」の活動は，隣の人と受信者，送信者に役割分担してRSA暗号通信を行った。しかし，活動の前の説明が疎かになってしまったこともあり，うまく生徒が活動を始めることが出来ず，実質活動したのは5分程度になってしまった。そのため，クラスのほとんどのペアが暗号通信の最後，つまり復号化まで行うことができなかった。さらに活動中，受信者が計算をしている時間がほとんどになってしまい，送信者が時間を持て余す状況が多くみられた。そのため，受信者，送信者に役割分担するのではなく，お互いがメッセージを送信しあうように設定する配慮が必要であったと考える。そして，短い時間でも，暗号通信を行えるように，配布プリントを工夫する必要があった。

最後に，短い時間で復号化のからくりについて説明をした。これは，フェルマーの小定理がRSA暗号の中に活用されていることを示す大切な説明である。しかし，時間が足りなかったため，暗号通信の後に行ってしまった。このからくりを生徒が理解し，さらに暗号通信を実際にやることで有用性の実感はさらに深まると考えるため，生徒のことを考えた展開ではなかったように感じる。それでも，からくりの説明に対して生徒は意欲的に説明を聞き，積極的に理解に努め，納得の表情もみられた。

「確認」の活動をしっかり行うことによって，フェルマーの小定理やRSA暗号の難しい説明に少し苦戦してしまっていた生徒も，暗号通信に成功したときの喜びや楽しさ，そして何より数学の有用性を実感することができるのではないかと考える。そのため，この「確認」の活動に対してさらなる検討が必要である。

(2) アンケートの分析と考察

ここでは，本実践の直後に実施したアンケートの調査結果を分析し，考察する。

1) アンケートについて

アンケートをとる最大の目的は，本実践において生徒がどの程度「数学の有用性」について実感を持つことができたかを調査することである。そこで，比較検討するために，平成20年度全国学力・学習状況調査と同じ質問内容を含むようにした（質問4, 5)。そして，本実践の内容，指導方法について検討を行うために，実践内容の生徒の理解度も，併せて調査することにする。

【質問1】
フェルマーの小定理について理解できましたか。

【質問2】
RSA暗号について理解できましたか。

【質問3】
RSA暗号の中にフェルマーの小定理が利用されていることが理解できましたか。

【質問4】
数学が現実世界の中で活用されていると感じましたか。

【質問5】
この授業で扱った内容を，普段の生活の中で活用できないか考えてみようと思いますか。

また，この5つの内容とは別に，自由に感想を書く欄を設けた。

2) アンケートの結果と分析

【質問1】

①よくできた	②できた	③あまりできなかった	④できなかった
1人	18人	11人	3人
3%	54.5%	33.3%	9.1%

【質問2】

①よくできた	②できた	③あまりできなかった	④できなかった
6人	13人	9人	5人
18.2%	39.4%	27.3%	15.6%

【質問3】

①よくできた	②できた	③あまりできなかった	④できなかった
3人	14人	10人	16人
9.1%	42.4%	30.3%	18.2%

【質問4】

①強く感じた	②感じた	③あまり感じなかった	④感じなかった
9人	18人	5人	1人
27.3%	54.5%	15.6%	3%

【質問4】

強くそう思う	②そう思う	③あまり思わない	④思わない
2人	13人	12人	5人
6.1%	39.4%	36.4%	15.6%

【分析】

質問1については，ほとんどの生徒が始めて聞く内容である「フェルマーの小定理」を約6割の生徒が「よく理解できた・理解できた」と回答している。しかし，4割強の生徒が「あまり理解できなかった･理解できなかった」と回答していることから，授業の進め方に改善の余地がありそうである。

次に，質問2についてだが，6割弱の生徒がRSA暗号について「よく理解できた・理解できた」と回答している一方で，「あまり理解できなかった」が27.3%，「できなかった」が15.6%と，RSA暗号を理解することができず，疑問を感じている生徒も多くいたことが分かる。

また，質問3についても，RSA暗号の中にフェルマーの小定理が利用されていることが「あまり理解できなかった・理解できなかった」と回答している生徒が48.2%もおり，フェルマーの小定理の有用性を理解できない生徒が多くいたことが分かる。

そして，質問4についてだが，数学が現実世界の中で活用されていると回答している生徒数が81.8%という結果であった。

しかし，質問5において，本実践の内容を，普段の生活の中で活用できないか考えてみようと「強く思う・思う」と回答した生徒数は半数以下の45.5%であった。

最後に，自由に感想を書く欄には，おもに次のような感想が書かれていた。

・暗号化するのがすごく楽しかった。
・暗号通信がうまくいったので，うれしかった。
・数学が情報の保護のために，こういった形で利用されていることを知って，すごいなあと思った。
・難しいけど，学校で習うことを，初めから役に立たないと決めつけずに関心を持っていこうと思う。
・フェルマーの小定理がこんなに奥が深いとは驚きました。
・計算は難しかったけど，パソコンはこれをパッと計算してしまうかと思うと，すごいなあと思ったし，それを考えた人はもっと尊敬します。

3）アンケート結果の考察

質問1において，「あまり理解できなかった・理解できなかった」と回答している生徒の数が多くなってしまった原因は，“≡”と“mod”の理解が難しかったのであろうと考えられる。本来であれば，高校では学習しない内容である“≡”と“mod”に対して，もっと時間をかけて理解を深める必要があるのであろう。今回は，練習問題などは全く行わなかったが，第2時の最初の復習で，口頭で説明する時間を省き，簡単な練習問題を扱うことで，生徒の理解をより深めることができたのではないかと考える。さらに，生徒の理解を深めるために，各自で法則を探す時間をもっと長く取る必要がある。ほとんどの生徒は，

$$x^{(n-1)} \equiv 1 \pmod{n}$$

ということに気づいていた。そして，発表をしてくれたS_1のように，当てはまらない数が存在することに気づいていた生徒も少なからずいたはずである。今回は，n＝8，n＝9を教師と一緒に確認するなかで，“nは素数，xとnは互いに素”という条件を求めた。しかし，各自の追求時間を多く設定することで，クラスの何人かは条件を求めることができたのではないか。そうすれば，教師主体の授業ではなく，生徒主体の授業となり，クラスメイトが発見した法則とその条件に対して，興味を抱き，理解を深めることができると考える。

次に質問2についてだが，RSA暗号自体は計算が多く，教師が一方的に，計算を行う手順を説明するという授業であった。しかし，それでも6割弱の生徒が「よく理解できた・理解できた」と回答している理由は，公開鍵暗号を理解することができたからであろう。授業ではRSA暗号の前に，ハンガーとロープを使って共通鍵暗号と公開鍵暗号を丁寧に説明した。このときに公開鍵暗号を理解することができていたため，RSA暗号をある程度スムーズに考えることができたのではないかと考える。しかし，より生徒の理解を深めるためには，公開鍵暗号を学習するときと，RSA暗号を学習するときのギャップを埋める必要がある。公開鍵暗号の場合は，前述したように，生徒と一緒にハンガーとロープを使って説明を行う教授活動である。しかし，RSA暗号になると，パワーポイントを使って一方的に教師が説明を行うという教授活動であった。その2つの活動のギャップに，生徒の中にRSA暗号に対しての否定的な意識が生まれたのではないか，と考える。これを改善するために，RSA暗号に対しての教授活動を工夫し，検討していかなければならない。

そして質問3については，「あまり理解できなかった・理解できなかった」と回答している生徒が約半数いた。

これは前述したように，確認の活動であるRSA暗号通信を，時間をかけて行うことができなかったことに原因があると考えられる。さらに，フェルマーの小定理が活用されている復号化のからくりの説明を，授業の最後に短時間で行ってしまったことも原因の1つであろう。

最後に，質問4，質問5についてだが，質問4において「強く感じた･感じた」と回答した生徒数が，81.8%であったのに対して，質問5で「強く思う・思う」と回答したのはたった45.5%の生徒であった。また，全国学力・学習状況調査においても「数学の授業で学習したことを普段の生活の中で活用できないか考えますか」，「数学の授業で学習したことは，将来，社会に出たときに役に立つと思いますか」という2つの質問に対して，「当てはまる･どちらかといえば，当てはまる」という回答数は後者の方が30%以上多かった。これらから生徒は，数学は現実世界で活用されているとは感じているが，どこか自分とは関係のない世界で使われている，と感じているのではないか。自分とはあまり直接関係がない世界で，数学が活用されていると感じることももちろん大切である。しかし，より身近なところで数学が活用されていることを実感した方が，より強く数学の有用性を実感できるのではないか，と考える。したがって，数学の有用性を伝えるためには，その題材を生徒にとってより身近で現実性のあるものとして感じられるよう構成して伝える工夫が必要である。そのため，本実践の授業構成にも課題の余地があるといえるであろう。

5．今後の課題

授業実践の考察やアンケート結果の考察から，RSA暗号の教材化について改善するべき点を以下の3点とした。

ア．整数の不思議さを実感することにさらに重点を置く。
イ．数学の有用性を実感するために，「確認」の活動に重点を置く。
ウ．RSA暗号の教授活動の工夫。

まずアについてだが，前述したように，初めからフェルマーの小定理が成り立つ条件を見つけようとすると，扱うnの数も少なくなってしまい，フェルマーの小定理の不思議さ，美しさを生徒に実感してもらうことは難しい。そこで，今回のような小さい素数の他に大きい素数の場合も扱い，フェルマーの小定理の不思議さを実感してもらう。そしてその後に，各自で法則を見つける時間をとる。すると，成り立たない場合もあることに気がつき，条件探しを始める。このように，教師が誘導して授業を進めるだけでなく，生徒が自ら活動を展開していくことで，より興味・関心，そして理解が深まるのではないかと考える。

そして前述したように，RSA暗号は，素因数分解の限界を基として考えられているため，本実践では行うことが出来なかったが，RSA暗号を扱う際に素因数分解の難しさを生徒に体験してもらうと，よりRSA暗号しくみを理解しやすくなり，さらに整数に対して興味を抱くのではないか，と考える。

次にイについてだが，「確認」の活動を十分に行うことができる時間配分が必要である。そして，活動中に生徒がスムーズに成功体験を行うことができるように工夫をしなければならない。そこで，配布プリントを工夫し活動手順が分かりやすいようにし，一人が受信者と送信者の二役を担うことによって，成功体験を増やすこととする。

最後にウについてであるが，先にも述べたが，RSA暗号を学習するときと，それまでの内容を学習するときとで教授活動にギャップが生まれてしまっていた。そこで，このギャップを埋めるためにRSA暗号の教授活動を工夫することにする。今回のように，RSA暗号をパワーポイントで説明するのではなく，授業プリントを作成してその流れにそって進めていく。そうすることで，生徒は授業プリントに集中することができ，RSA暗号のより深い理解にもつながるのではないかと考える。そして，これらの改善点に注意して再度授業実践を行い，RSA暗号の教材化についてさらに追究していく必要がある。

6．おわりに

数学の有用性を実感できるような教材というのはまだまだ少なく，実際の授業でそのような教材の活用が少ないように感じる。それは，テストや入試などが強い存在感を示す現代社会において，情意面ではなく認知面での不安が大きいためであろう。したがって，今後さらに多くの数学の有用性を実感できる教材を開発し，有用性の実感が情意面だけでなく，認知面についても高い達成につながることを示していく必要があるだろう。

最後に，今回授業実践に協力していただいた藤島高等学校の中田政晴教諭には大変御世話になり感謝を申し上げます。

【主要参考文献】

伊禮三之（2001）『数学と現実との関連を重視した教材の工夫』（研修報告集録第29集）沖縄県立教育センター，pp.109−114
銀林浩（1987）『人間行動からみた数学』（教育の方法6）岩波書店，pp.110−138
四方義啓・下田好行・岩田修一・鈴木貴（2006）『数あてマジックと暗号づくり』（学力向上につながる数学の題材）東京法令出版，pp.50−53
辻井重男（1996）『暗号』講談社

伏見陽児・麻柄啓一（1993）『授業づくりの心理学』国
　土社，pp.179−191
結城浩（2003）『暗号技術入門』ソフトバンククリエイ
　ティブ株式会社

A Study on Teaching Materials of RSA

Michio OKAMOTO, Mitsuyuki IREI

Key words：usefulness, mathematical problem solving, Fermat's little theorem, RSA