教科横断的な授業作り

-RSA 公開鍵暗号を題材にして-

芝浦工業大学柏中学高等学校　清水真光

1　はじめに

本稿は、前任校の流山高等学校での実践である。流山高等学校は, 商業科, 情報処理科, 園芸科からなる職業高校である。 数学 I, 数学 A が必修科目であり, 第 3 学年では選択科目として数学探究を履修することができる。本稿は, 第 2 学年の情報処理科で行った数学 A の授業実践報告である。

2　授業実践の内容

(1) 授業実践の目的・方法

ア　目的

新学習指導要領において, 数学と人間の関わりや数学の社会的有用性について, 数学的活動を充実させることが重要になった。本校の情報処理科の生徒は公開鍵や秘密鍵についての知識を 2 年次の情報処理の授業において学習している。そこで, より深く暗号の原理を理解し, 現実の世界で数学がどのように使われているのかを深く理解することに焦点を当てる。

イ　方法

対話的な学習の中で最後に個人で振り返り, 今日の授業で何を学んだかをまとめさせる時間を与える。その際に, R80[1)]を用いることで思考力や論理的な記述能力を育成できると考えた。また, Wolfram |Alpha を用いることで合同式の計算技術に重きをおかず, 計算時間の短縮をした。「算数・数学の問題解決の過程」(中央教育審議会, 2016) を参考に, 現実の世界での思考のサイクルを取り入れた。

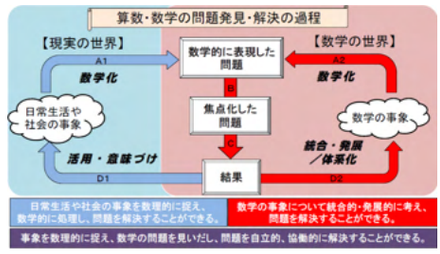


図 1　算数・数学の問題解決の過程

(2) 授業実践計画

科目：数学 A

単元：合同式の利用

教材：授業プリント (穴埋め形式のもの)

　　Wolfram |Alpha

授業形態：グループワーク・BYOD・R80

本授業実践は 3 時間の構成で実施した。

[1 時間目]

合同式についての定義の理解と定理や性質の説明を行い, それらの練習問題を解く。また，RSA 暗号で必要になるフェルマーの小定理[2)]やオイラー関数[3)]に関しては説明のみ行う。

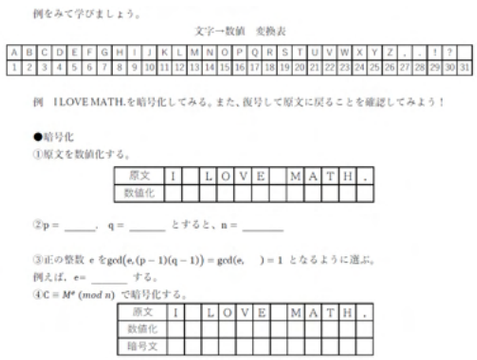
[2 時間目]

[1)] 茨城県立並木中等教育学校校長の中島博司氏が開発した。授業の最後に内容を振り返り, 80 字以内で書くというものである。

[2)] p を素数とし, a を p の倍数でない整数（a と p は互いに素）とするとき, $a^p \equiv a \pmod{p}$ が成り立つ。

[3)] 正の整数 n に対して, n と互いに素である 1 以上 n 以下の自然数の個数を $\varphi(n)$ と表す。

シーザー式暗号 (平文の各文字を辞書順で 3 文字分ずらして暗号文とする暗号である) について理解し, その暗号の脆弱性について考える。そこで, 現在利用されている RSA 公開鍵暗号の原理 (公開鍵と秘密鍵) を理解する。この原理のみを説明するため, 理解することは難しい。そこで, Wolfram |Alpha を活用し平文を数値化し暗号文にする練習を行う。問題は穴埋め練習問題 (図 2 を参照) に設定する。この活動はグループワークで行い, 生徒同士で結果を共有する。


例をみて学びましょう。

文字→数値　変換表

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	,	.	!	?
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

例　I LOVE MATH.を暗号化してみる。また、復号して原文に戻ることを確認してみよう！

●暗号化

①原文を数値化する。

原文	I		L	O	V	E		M	A	T	H	.
数値化												

②p＝ ＿＿＿，　q＝ ＿＿＿ とすると、n＝ ＿＿＿

③正の整数 e を $\gcd(e,(p-1)(q-1)) = \gcd(e,\ \ ) = 1$ となるように選ぶ。

例えば、e＝ ＿＿＿ する。

④$C \equiv M^e \pmod{n}$ で暗号化する。

原文	I		L	O	V	E		M	A	T	H	.
数値化												
暗号文												

図 2　授業プリント

[3 時間目]

暗号文を復号化し, 暗号文が平文に戻ることを確認する。また, RSA 公開鍵暗号がなぜ安全なのかを理解する。その後, R80 を用いて授業の振り返りを行う。特に, この 3 時間目では以下の 3 つについて理解や体験できるようにする。

ア 素因数分解を見つけることが困難である。
イ 秘密鍵を教える必要がないこと。
ウ 2 つの素数の積という簡単な計算で公開鍵を生成できる。

3　成果と課題

(1) 生徒が書いた R80

・公開鍵暗号がどれだけ安全かわかった。なぜなら簡単に作れるのに, 秘密鍵を教えなければほぼ解読できないのですごいと思いました。

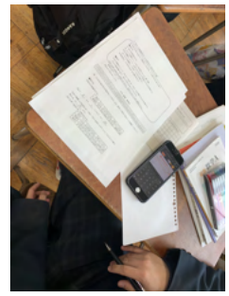


図 3　生徒の様子

・今回の授業では前よりも理解して取り組むことができた。また, 改めて暗号のすごさと作った人がとんでもない人だなと実感することができた。

・今まで情報処理の授業でよく公開鍵について学んでいたが, ここまで詳細に知るとなぜ安全なのかがわかった。また, ハッカーなどはどのように解けるのか気になった。

(2) 学校数学と現実の世界との課題

本授業では Wolfram |Alpha を用いて計算させた際に, 現実のデータを扱うことが困難であるため, 簡略化したデータを扱ったが, 計算が困難になってしまった。また, アプリを使うことで, 自力で解いた実感は薄く, 時間の余った生徒に手計算で確認するように指示をしたが, 自力で解ける生徒は少なく感じた。一方で, 生徒の中には懸命に計算した答えが, Wolfram |Alpha と一致し, 喜ぶ姿も見られた。

参考文献

[1] 中学数学からはじめる暗号入門: 現代の暗号はどのようにして作られたのか, 関根章道, 知りたい!サイエンス , 2019

[2] 中央教育審議会,「算数・数学ワーキンググループにおける審議の取りまとめ」, 2016