研究報告

# 高等学校における情報と数学の横断的学習についての考察

鈴木 瞭太朗

学生課学生企画係

**概要**：高等学校における科目としての重要性が高まっている情報と，既存科目である数学の横断的な教育について論じる。特に高校数学の「整数の性質」の情報セキュリティ理論への応用について，私の高校教諭時代の経験も踏まえながら高校生への授業題材となり得るか考察する。

**キーワード**：共通鍵暗号方式，公開鍵暗号方式，Fermat の小定理，RSA 信号，Python

## 1．高等学校教育課程における情報

我が国における情報教育を巡っては，特に高等学校において平成15年に教科として新設されて以降その「地位」を確立してきた。平成25年度から施行されている学習指導要領では科目の再編がなされ，令和４年度から施行される次期学習指導要領［３］では，プログラミングを含む必修科目「情報Ⅰ」及び発展的内容を学習する選択科目としての「情報Ⅱ」に整備されることが明記されている。さらに国立大学協会は，令和７年度の大学入学共通テストにおいて，国立大学受験志願者には原則として「情報」を受験させる意向を示している[1]。

情報を扱う技術や情報モラルを扱う上で重要な事項を学ぶことは昨今において重要視されて当然といえよう。しかし一方で，情報を専任として担当できる教師を育成することが急務とされるが，令和３年度現在においては少なくとも追いついていないとされる。この社会的ニーズに対し，情報の教員免許取得可能な体制整備の拡充が急がれるとともに，将来教師になることを目標とする高校生のうち，情報を担当する意思をもつ生徒の割合が多くなることが期待されなければならない[2]。

## 2．高校数学における整数論の修得

平成21年度より，数学Ａにおいて「整数の性質」が追加された。令和４年度から施行される学習指導要領では，数学Ａの「数学と人間の活動」に内包されることとなるが整数の性質についての学習は継続して行われる。

純粋数学において初等整数論は長く深い歴史を持ち，現代においてもなお魅力的な研究対象であるにもかかわらず，苦手意識を抱いたり，半ば「毛嫌い」したりする高校生は少なくない。筆者は，平成28年度より２年間，稚拙ながら高校の数学教師として勤務した経験があるが，「整数の性質」の指導にあたっては他の分野より生徒の気持ちが乗らなかったような印象であった。生徒たちからは「他の分野との関係がない」，「入試対策においては解法パターンが多すぎる」といった声が聞かれた。さらには、何の役に立つのか不明といった，教科としての数学そのものに対する疑念も，この分野に対してはより一層抱かれやすい。

学習する内容は約数・倍数の概念から始まり，Euclid の互除法や一次不定方程式の解法，$n$進数などである。初等整数論において扱われる内容は，一般的な情報理論において特にセキュリティに関わる部分に関する応用が深い。

そこで，高校での科目指導において数学と情報の横断的な教育が達成できれば，高校生にとっては，情報セキュリティに関する理論及び整数論の応用に対する理解が深まるものと考える。

## 3．情報セキュリティに関する事項

### 3.1　共通鍵暗号方式

情報セキュリティにおいて基礎となる暗号化方式のうち，最も基本的なものは共通鍵暗号方式である。送信者は，暗号化の方法$E$及び共通鍵$k$を用いて平文$P$を暗号化した暗号文$E(P,k)$を送信する。受信者は，受信した暗号文$E(P,k)$について$E$と$k$から平文$P$を

復号[3]する。この方式では，暗号化及び復号の処理を高速で済ませられるとい長所がある一方，暗号化の方法及び鍵を送信者と受信者で予め共有しておく必要があり，その両方がハッキング等により知られてしまった場合は誰でも復号可能である点が短所となりうる。

### 3.2　公開鍵暗号方式

共通鍵暗号方式の短所を一部補正した暗号方式として用いられる手段が公開鍵暗号方式であることはよく知られている。受信者は予め２つの鍵$k_1$，$k_2$を準備しておき，$k_1$は公開鍵として公開し，$k_2$は秘密鍵として保管する。送信者から送信された暗号文$E(P,k_1)$から，受信者は$k_2$を用いて平文$P$を復号する，というものである。セキュリティの強化という観点からは，この手段において「暗号文$E(P,k_1)$と鍵$k_1$では平文$P$を復号できないこと」が達成されなければならない。それを体現するのが有名なRSA信号であり，ここの初等整数論の応用がある。

## 4．初等整数論からの準備

ここでは特に断らない限り，$a, b, c$などのアルファベット小文字は整数を表すものとし，とりわけ$p$，$q$については奇素数（２以外の素数）を表すものとする。また，$d$が$a$と$b$の最大公約数であるとき，

$$d=(a,b)$$

と記し，特に$(a,b)=1$であるとき$a$と$b$は互いに素であるという。

$a$と$b$の差が$m$の倍数となるとき，$a$と$b$は$m$を法として合同であるといい，

$$a\equiv b \pmod m$$

と記す。このような表記は合同式と呼ばれるものである[4]。

ここではまず，Fermatの小定理について述べる。

**補題１．**素数$p$に対し，

$$(m+n)^p\equiv m^p+n^p \pmod p$$

が成立する。

証明

$$(m+n)^p=\sum_{0\le i\le p}\binom{p}{i}m^{p-i}n^i$$

であり，$1\le i\le p-1$においては，

$$\binom{p}{i}\equiv 0 \pmod p$$

であるから，

$$(m+n)^p=\sum_{0\le i\le p}\binom{p}{i}m^{p-i}n^i \equiv m^p+n^p \pmod p$$

（証明終）

**定理１．**（Fermatの小定理）$(a,p)=1$である$a$と$p$に対し，

$$a^{p-1}\equiv 1 \pmod p$$

が成り立つ。

証明　定理の主張と同値な

$$a^p\equiv a \pmod p$$

を[5]，aに関する数学的帰納法で示す。

$a=1$のとき成立することは自明である。

$a=k$で成立を仮定すると，$a=k+1$のとき，補題１を用いて，

$$(k+1)^p\equiv k^p+1^p\equiv k+1 \pmod p$$

が成立する。

（証明終）

Fermatの小定理に加えて重要となる定理をもう一つ証明する。

**定理２．**$(a,b)=1$に対し，合同方程式

$$ax\equiv 1 \pmod b$$

において，$1\le x\le b-1$なる解はただ１つ存在する。

証明　一般に，ある整数を$b$で割った余りは

$$0, 1, 2, \cdots, (b-1)$$

のb通りであるから，b個の整数

$$0a, a, 2a, \cdots, (b-1)a$$

について，$b$で割った余りがすべて異なることを示せばよい。上の$b$個の整数のうちで$b$で割った余りが等しい２つの整数が存在したとする。すなわち，

$$0\le i<j\le b-1$$

であるような$i, j$が存在して，

$$ia\equiv ja \pmod b$$

が成立したとすると，$(i-j)a$は$b$の倍数である。$a$と$b$は互いに素だから，$(i-j)$が$b$の倍数でなければな

らない。ところが，

$$1 \leq i-j \leq b-1$$

よりこれは矛盾である。したがって，上にあげた $b$ 個の整数は，$b$ で割った余りがすべて異なる。

（証明終）

## ５．RSA信号の仕組み

RSA信号とは次のような手順で暗号化及び復号化を行うプロセスである。

①なるべく大きな２つの素数 $p, q$ をとり、

$$N=pq$$

とする。

② $(p-1)(q-1)$ と互いに素な整数を１つ選び $k_1$ とし，これを公開鍵とする。

③ $k_2$ を，

$$k_1 k_2 \equiv 1 \pmod{(p-1)(q-1)}$$

を満たすようにとる。これを秘密鍵とする。

④送信者は、送りたい平文 $m$ を

$$E(m, k_1) = m^{k_1} \pmod{N}$$

と暗号化する。

⑤受信者は

$$\{E(m,k_1)\}^{k_2} = m^{k_1 k_2} \pmod{N}$$

を計算することで平文 $m$ を復号できる。

上記手順についていくつか補足する。①において「なるべく大きな」と記したが，現在のコンピュータではある整数の素因数分解を求めることが難しく，とりわけその整数が大きいほど天文学的な時間を要するため，理論上セキュリティ高度が増すこととなる。③における $k_2$ は，定理２によってその存在は保証され，さらに $N$ 及び $k_1$ より一意に定まる。⑤によって復号がうまくいくことについては以下で証明する。

証明　示すべきは

$$m^{k_1 k_2} \equiv m \pmod{N}$$

であるが，対称性により，

$$m^{k1\,k2} \equiv m \pmod{p}$$

を証明すれば十分である。

まず，$m$ が $p$ の倍数であれば自明である。$m$ が $p$ の倍数でないとき，$(k_1 k_2-1)$ が $(p-1)(q-1)$ の倍数となるように $k_1$ 及び $k_2$ を選んだことにより，

$$k_1 k_2 = a(p-1)+1$$

と書けるから，Fermat の小定理を用いて，

$$m^{k_1 k_2} = \{m^{(p-1)}\}^a \times m \equiv m \pmod{p}$$

が成り立つ。

（証明終）

なお、RSA信号の名称の由来については、その開発に携わったリヴェスト(Rivest)氏、シャミル(Shamir)氏、エイドルマン（Adelman）氏の頭文字を順にとったものである。

ここまでで，初等整数論と RSA信号について述べたが，実用上は $p$ と $q$ にはこのほかに様々な条件が付けられる[6]。あくまで，高校での科目指導にあたるための準備として必要最低限にとどめた。

## ６．横断的授業を行う上での留意事項

平成30年告示の高等学校学習指導要領においては，指導計画の作成に当たっての配慮事項として第一に「主体的･対話的で深い学び」の実現が要請されている。この内容は当年度の高等学校学習指導要領改訂における「目玉」の１つとされているが，この内容が登場することとなった経緯については本書では割愛する。

「情報」においては，「第３章各科目にわたる指導計画の作成と内容の取扱い」の１節において，（２）情報活用能力を更に高めるとともに他の各教科・科目等との連携を図ること，とされ学習指導要領解説には次のように記されている。

> （２）学習の基盤となる情報活用能力が，中学校までの各教科等において，教科等横断的な視点から育成されてきたことを踏まえ，情報科の学習を通して生徒の情報活用能力を更に高めるようにすること。また，他の各教科・科目等の学習において情報活用能力を生かし高めることができるよう，他の各教科・科目等との連携を図ること。

さらに，続く（４）他教科等との関連においては，

> （４）公民科及び数学科などの内容との関連を図るとともに，教科の目標に即した調和のとれた指導が行われるよう留意すること。

とある。情報に関する内容を指導するのは当然のことながら，やはり他教科との「連携」や「関連」，さらには「調和のとれた指導」が行われることが留意点として明示されている。

一方で数学に関しては，同じく学習指導要領解説第３章第１節における，３教科内の科目相互・他教科等

との関連，において，

（４）各科目を履修させるに当たっては，当該科目や数学科に属する他の科目の内容及び理科，家庭科，情報科，この章に示す理数科等の内容を踏まえ，相互の関連を図るとともに，学習内容の系統性に留意すること。

とあり，情報等との強化と相互の関連を図ることが盛り込まれている。さらに，同章第２節においては，４数学的活動の取組に関わる配慮事項，として下の図１のような「イメージ」とともに，数学的活動を行う意図や目的について記述がある。

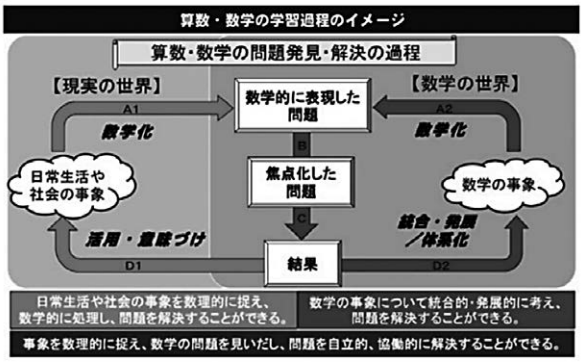


図１

ここでいうところの，【現実の世界】から【数学の世界】というプロセスで行われる授業計画はしばしば目にするが，一方で，【数学の世界】から【現実の世界】へという数学的活動が行われる授業計画は，少なくとも筆者の感覚ではそう多くはない。

前節までの議論を踏まえた授業実践例の１つを次節で論じるが，数学の応用として整備された体系があってこそなしえるものである。その意味では情報における情報理論が最も親和的なものの１つである。

## ７．実践的内容についての考察

ここでは実践例としての授業づくりの具体例をのべる。数学Ａの「整数の性質」の高校生を対象とし，45分ないし50分授業１回で行うことを想定する。同じような先行研究として［１］や［２］があるが、本実践内容では情報の新学習指導要領の内容を踏まえプログラミングの実習も兼ねる内容とした。

メッセージと番号
おはようございます　：１１
調子はいかがですか　：２２
そちらへ伺います　：３３
こちらへ来てください　：４４
助けてください　：５５

図２

（１）異なる２つの素数を決めよう
$p=\square, q=\square$
（２）$p$ と $q$ の積 $N$ を求めておこう
$N=pq=\square$
（３）$(p-1)(q-1)$ を求めておこう
$(p-1)(q-1)=\square$
（４）公開鍵 $k_1$ を生成しよう
$(p-1)(q-1)$ と互いに素な整数を適当に１つ選んで $k_1$ とすればよい。$k_1=\square$。

図３

まず，「主体的・対話的で深い学び」の実践として２人１組でのグループワークとすることを設定する。双方向での通信を想定し，お互いがそれぞれ秘密鍵と公開鍵を設定して暗号を解読し合うといった流れで行う。送信する内容については，教師による準備としては図２のようにメッセージと数字の対応を数字化したものをプリントアウトし配付する。[7]

グループワークに入る前に，教師は全生徒に等しく手順を説明する。説明すべきは，まず適当な素数を２つ用意させその積を計算すること，$(p-1)(q-1)$ と互いに素な数を１つ取り「公開鍵」とすること，公開鍵をもとに秘密鍵を求めておくことが最低限必要な内容となる。また，これらの内容が誰にも（特にグループワークを行う相手の生徒には）知られないように行うことも語り掛けておきたい。ここでも，図３のようなワークシートがあると授業進行の大きな助けになる。

秘密鍵については，生徒それぞれが勝手に選んだ $p$ 及び $q$，$k_1$ によって、求めるための時間に差がでることとなろうから，この部分については５～10分程度時間を要することには留意されたい。

グループワークでは，互いに公開鍵を伝え合った後，それぞれ送りたいメッセージを決めて暗号化し，その数値を伝え合う。あとは互いに復号作業を行い，答え合わせをする。この一連で，簡単ではあるが，ネットワークセキュリティの原理を体験できるとともに，整数の性質がどのように応用されているかを体験的に認

識することが出来る。

この内容で授業を行う場合，教師側は次の点に配慮しておかなければならない。

（１）$p$ と $q$ の積はある程度大きくなければならないので，両方２桁以上とさせるのが良い。これは必然的に奇素数を選ばせることを意図するものである。

（２）煩雑な数値を正しく計算することが本授業の狙いではなく，さらに情報という教科の性質を考慮すれば，表計算ソフトを使用するのが効果的であると思われるだろう[8]。Microsoft 社の Excel では合同式に関する計算式もプログラミングされており，暗号化及び復号に多大な時間を割かずに済む。参考までに，図４はメッセージを送信する側が Excel を使用した例である。

ここで１つ問題が生じる。Microsoft 社の Excel はセル内での数値計算の最大桁数に制限があるため，暗号文と秘密鍵の数値が大きいと，計算結果はエラーとして返される。実際，図４の図中にある設定で復号する側が同様に Excel を利用すれば図５のようになってしまう。

この問題点を解決するために，プログラミングが情報の教育内容となった点を最大限活用する。ここではプログラミング言語として Python を使用する。これは文部科学省による教員研修用教材［６］においても第一に取り上げられる言語として記載があるとともに，数値計算においては桁数が無数に扱える点が最大の利点である。演算子について注意さえすれば，プログラミングの履修を終えた生徒に対しては特段の指導は不要であろう。図６は実際に Python を使用した例であるが，コマンドにも大きな難点はないため，もっと実践的に暗号化を行ったとしても（例えば柱脚７で述べたような，［１］や［７］にある方法で暗号を作成させたとしても，暗号鍵や秘密鍵となる素数が３桁以上となっても[9]），あるいはこの授業実践を情報が選任ではない数学教師が行うにしても，とりわけ問題は生じないものと思われる。

（３）合同式の取り扱いについては現在多くの教科書で「発展」として扱われており，必修事項ではない。生徒たちの学力レベルに合わせて適宜解説が必要となる。

（４）授業時間としてもう１回分確保することができるのなら，先に述べたような「仕組み」を授業することも考えられる。合同式の取り扱いには前述の通り注

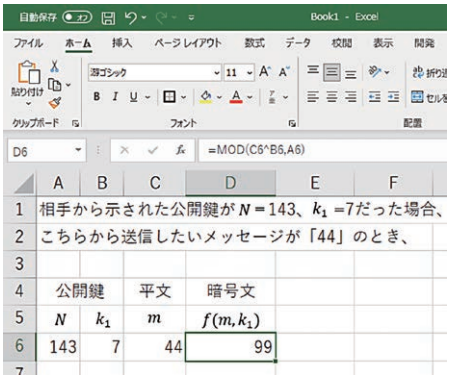


図４

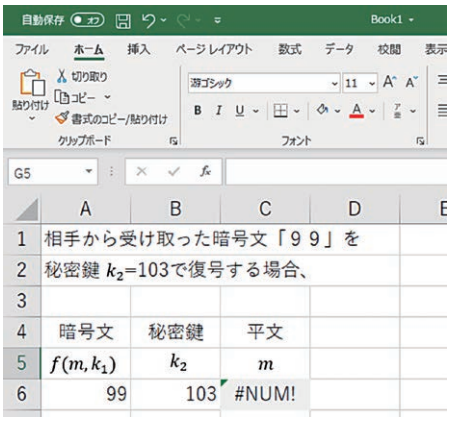


図５

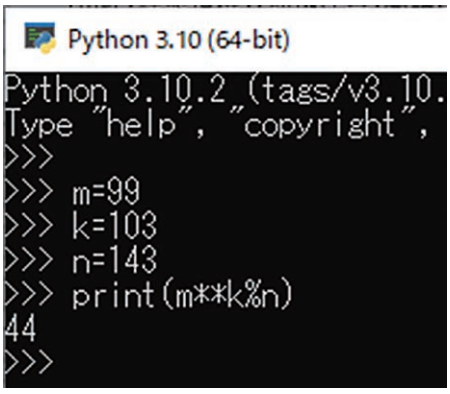


図６

意を要するほか，補題１を説明するにあたっては二項定理の理解が必要となるため，生徒が数学Ⅱの該当箇所を履修済みであることが求められる。

（５）授業計画を立てる上では評価にかかる点についても十分に検討しておくことが必要であることは言うまでもない。ただし，仮にこのような授業が高校で行われることを想定した場合に，情報の授業として行われるのか，あるいは数学の授業として行われるのかの違いで，評価のポイントのニュアンスは微妙に異なっ

てくる。そのためこの点については，本書を読まれる方の構想にお任せすることとし，本書で述べるのはあくまで暗号理論を題材とした数学と情報の横断的な学習についての考察というだけにとどめておきたい。なお，中学校の数学における授業実践例の一例として［1］があり，評価の方法についても考察されているので，読者の必要に応じて参照されたい。

## 8．最後に（プログラミング教育の意義）

前節（2）でPythonでの計算について述べた。プログラミングの基礎的な事項で取り扱うことは十分に可能である。

ところで，先行事例［2］では，Microsoft社のExcelを用いてFermatの定理を確認させるなどの教材開発を行っており，そのExcelシートには平文や公開鍵，暗号鍵について「あまり大きな数にならないように」入力させることで，Excelの桁数における限度を回避しているほか，復号を行うにあたっては合同式の性質を駆使した計算の工夫を行うことを教材としてのPowerPointファイルの中で提示している。後者については，令和4年度から施行される数学の学習指導要領における数学Aの「数学と人間の活動」の趣旨には必ずしも含まれない事項であるため，高校生が当計算方法にある程度習熟するまでには，あらかじめ一定程度の時間を有してしまう可能性は否定できない。

情報という教科の「骨格」が定められ，プログラミングが正式に題材化されたことで，その学び自体の簡単な応用によって，Excelの限界や合同式のやや高度な取り扱いという点を回避できることは非常大きな意味があることと思われる。プログラミングは，システムの構築だけなく数値計算についても存分に活用できるという魅力を，これからの高校生が実感できるのなら「情報Ⅰ」や「情報Ⅱ」の教科としての存在意義は確固たるものとなろう。また，そのような思いを携えて教壇に立たれる先生方にとって，本考察を参考としていただける機会があれば幸いである。

### 後注

1　国立大学協会は令和4年1月28日の総会で，その方針を決めた。

2　［5］によれば，令和2年度時点で，全国に数ある教員養成系学部のうち高等学校教諭第一種免許状（情報）を取得できるのは17ほどであり，国立教員養成系単科大学においては11大学中わずか5大学にとどまっている。

3　「復元」と呼ぶこともある（例えば［7］など）。

4　高校数学では必ずしも必修事項ではないが，記法の簡略化を図るために導入する。

5　(a,p)=1という条件のもとでは同値である。実際，この式は任意の整数aで成立する。

6　例えば，「300桁くらいの非常に大きな素数とする」など。

7　実際の暗号の用いられ方については［1］や［7］により詳細な記述があるが，そこまでを述べるのは本書の趣旨に特段の必要はないためここでは割愛する

8　実際［2］では，Fermatの定理を確認させるためにそのようなExcelファイルを準備している。

9　当然ながら扱うPCシステムのメモリ等に依存して計算速度や扱える桁数には一定の限度がある点には留意されたい。

### ［引用文献］

［1］大澤弘典（2001）「暗号の教材化についての一考察」『日本数学教育学会誌』83巻7号pp.10-17

［2］滋賀県総合教育センター（2008）「高等学校情報　暗号（公開鍵と秘密鍵）」，https://www.shiga-ec.ed.jp/www/contents/1436927714369/index.html（2022年1月31日）

［3］文部科学省（2018）『高等学校学習指導要領（平成30年告示）解説情報編』開隆堂出版pp.60-64

［4］文部科学省（2018）『高等学校学習指導要領（平成30年告示）解説数学編理数編』学校図書pp.129-135

［5］文部科学省（2020）通学課程（1）一種免許状（大学卒業程度）高等学校教員（情報）の免許資格を取得することのできる大学,https://www.mext.go.jp/a_menu/shotou/kyoin/daigaku/detail/1287078.htm（2021年12月10日）

［6］文部科学省（2020）高等学校情報科「情報Ⅰ」教員研修用教材（本編）第3章　コンピュータとプログラミング,https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1416756.htm

［7］雪江明彦（2013）『整数論1初等整数論からp進数へ』日本評論社,pp.35-46