RSA 暗号の仕組み

— 実感する数学を目指して —

磯辺高等学校　氏家 悟

1　はじめに

自分は日ごろ，数を感覚的，体験的に捉えさせたいと考えている。

インターネットで使われている RSA 暗号の原理は，数式で書けば数行で書けてしまうが，それを高校生に見せても意味がない。実際に小さな数で計算させ，暗号化と復号ができることを情報の授業で体験させてみた。

2　mod 7 の計算

はじめに，商と余りの関係を確認した[1)]。

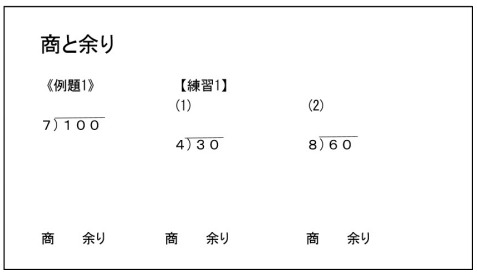
《例題 1》100 ÷ 7 の 商 14 余り 2 より，商と余りの関係

$100 = 7 \times \square + \square$

が成り立つ。

【練習 1】 次の割り算を行い商と余りの関係に表せ。

(1) 30 ÷ 4　　(2) 60 ÷ 8



問題プリントとは別に，すべての例題と練習に，右のような「計算用紙」も配り実際に計算させ，プリントを完成させた。

続いて，7 で割る計算。

【練習 2】$a = 110$，$b = 80$ とする。このとき，次の数を 7 で割った余りを求めよ。

(1) a　　(2) b　　(3) $a + b$　　(4) $5 + 3$

(5) $a - b$　　(6) $5 - 3$　　(7) ab　　(8) 5×3

(9) $b^3 = 80 \times 80 \times 80 = 512000$　　(10) $3^3 = 3 \times 3 \times 3 =$

mod 7 にしたのは，単に「曜日の計算」ができるからである。そして，計算の性質を考えさせる。

[1)] mod の導入までは数学 A の教科書を参考に教材を作成した。

このことから次のことがわかる。
（和 $a+b$ を 7 で割ったときの余り）＝（余りの和 $5+3=$__ を 7 で割ったときの余り）
（差 $a-b$ を 7 で割ったときの余り）＝（余りの差 $5-3=$__ を 7 で割ったときの余り）
（積 ab を 7 で割ったときの余り）＝（余りの積 $5\times 3=$__ を 7 で割ったときの余り）
（3 乗 b^3 を 7 で割ったときの余り）＝（余りの 3 乗 $3^3=$__ を 7 で割ったときの余り）
割り算はできません。このことが暗号化の逆操作で復号できない原理につながります。

【練習 3】今日は，____ 曜日である。明日は，____ 曜日，明後日は，____ 曜日，3 日後は，____ 曜日，4 日後は，____ 曜日，5 日後は，____ 曜日，6 日後は，____ 曜日，7 日後は，____ 曜日，8 日後は，____ 曜日。
80 日後は，____ 曜日，110 日後は，____ 曜日，$110+80=190$ 日後は，____ 曜日，$110\times 80=8800$ 日後は，____ 曜日，$80^3=512000$ 日後は，____ 曜日。

累乗計算で，数が繰り返すことを発見させる。[2)]

《例題 2》2^{100} を 7 で割った余りを求めよ。
$2^1\equiv 2\ (\mathrm{mod}\ 7)$　　$2^2\equiv 4\ (\mathrm{mod}\ 7)$
$2^3=2^2\times 2\equiv$ ____ $\times 2\equiv$ ____ $(\mathrm{mod}\ 7)$
$2^4=2^3\times 2\equiv$ ____ $\times 2\equiv$ ____ $(\mathrm{mod}\ 7)$
(中略)
$2^9=2^8\times 2\equiv$ ____ $\times 2\equiv$ ____ $(\mathrm{mod}\ 7)$
と繰り返すので，
$2^{99}=(2^3)^{33}\equiv$ ____ $\equiv$ ____ $(\mathrm{mod}\ 7)$
$2^{100}=2^{99}\times 2\equiv$ ____ $\times 2\equiv$ ____ $(\mathrm{mod}\ 7)$　　2^{100} 日後は _____ 曜日。

例題で実演し，3 の累乗で練習させる。

【練習 4】3^{2017} を 7 で割った余りを求めよ。
$3^1\equiv 3\ (\mathrm{mod}\ 7)$　　$3^2=$ ____ $\equiv$ ____ $(\mathrm{mod}\ 7)$
$3^3=3^2\times 3\equiv$ ____ $\times 3\equiv$ ____ $(\mathrm{mod}\ 7)$
(中略)
$3^9=3^8\times 3\equiv$ ____ $\times 3\equiv$ ____ $(\mathrm{mod}\ 7)$
と繰り返すので，$3^{2017}\equiv$ ____ $(\mathrm{mod}\ 7)$　　3^{2017} 日後は _____ 曜日。

順に掛けて割る数 7 を超えたら，すぐに余り 1〜6 に小さくでき，そのうえ，出てくる数は同じ数を繰り返すという規則性があるので，どんな巨大な累乗でも簡単に求まることを体験させる[3)]。これは，暗号化と復号の計算が高速で行えることを示している。

[2)] プリントでは「7 で割ったときの余り」を毎回書くのが大変だという理由で， mod 記号を導入する。そして，計算のルールも 「$a+b\equiv 5+3=8\equiv 1\ (\mathrm{mod}\ 7)$ のように」mod の式で書き直す。
[3)] $2^{100}=1267650600228229401496703205376$ 日後は約 3.5×10^{27} 年後。3^{2017} 日後は 10^{959} 年後。

【練習 4】表の一番左の数を累乗し，7 で割った余りの一覧を求めよ。

1 乗	2 乗	3 乗	4 乗	5 乗	6 乗	7 乗	8 乗	9 乗	10 乗	11 乗	12 乗	13 乗	14 乗
1													
2													
3													
4													
5													
6													

1 の累乗は明らか。2，3 の累乗は，9 乗までは例題 2，練習 4 から写し，10 乗以上は規則性から類推する。4,5,6 の累乗は自分で計算する。

【問 1】すべての数が 1 に戻るのは何乗か。
【問 2】すべての数が元の数と同じに戻るのは何乗か。

この問いで「フェルマーの小定理[4)]」の性質を見つけさせる。そして，「元に戻る」性質を暗号化と復号に使うのである。プリントで次のように説明した。

55 乗で元の数に戻る。$\Rightarrow 55 = 5 \times 11 \Rightarrow$ 5 乗して ＿＿ 乗すると元に戻る。
「0, 1, 2, 3, 4, 5, 6」 を 5 乗すると数がそれぞれ「0, 1, 4, 5, 2, 3, 6」に置き換わる。（暗号化）
「0, 1, 4, 5, 2, 3, 6」を 11 乗すれば，元の「0, 1, 2, 3, 4, 5, 6」に戻る（復号）
この場合，暗号化が ＿＿ 乗，復号が ＿＿ 乗となり，暗号化と復号の鍵が異なることになる。
さらに，合同式の計算では，割り算ができないので，5 乗の逆算ができない。つまり，「＿＿ 乗で暗号化」を公開しても，「＿＿ 乗で復号」を秘密にすれば，暗号は守られる。
これが公開鍵暗号の原理である。

3 RSA 暗号

割る数 (mod) が 1 つの素数 (例は 7 だけ) では，暗号化の鍵（5 乗）と mod の数 7 から，復号の鍵（11 乗）が計算でき，解読される。そこで RSA では 2 つの素数の積を mod に使う。

1 乗	2 乗	3 乗	4 乗	5 乗	6 乗	7 乗	8 乗	9 乗	10 乗	11 乗	12 乗	···	41 乗
1	1	1	1	1	1	1	1	1	1	1	1		1
2	4	8	16	32	31	29	25	17	1	2	4		2
3	9	27	15	12	3	9	27	15	12	3	9		3
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮		⋮
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮		⋮
9	15	3	27	12	9	15	3	27	12	9	15		9
10													
11	22	11	22	11	22	11	22	11	22	11	22		11
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮		⋮
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮		⋮
32	1	32	1	32	1	32	1	32	1	32	1		32

授業では，2 つの素数を 3 と 11 にし，33 を mod にした一覧表をエクセルで作成し配布。一

[4)] p を素数とし，a を p は互いに素とするときに，$a^{p-1} \equiv 1 \pmod{p}$．つまり，$p-1$ 乗で 1 になり，p 乗で元に戻る．

覧表の一部は消してあり，生徒に計算させて完成させる。1 つの数の累乗を見ると，一定の周期で繰り返しており，さらに。すべての数が元に戻る累乗があり，それを暗号化と復号に使うのである。

【問 3】一覧表では，10 の累乗と，22 の累乗が消されています。簡単なので計算してみよう。

$10^1 \equiv 10 \pmod{33}$　　$10^2 = \_\_\_\_ \equiv \_\_\_\_ \pmod{33}$

$10^3 = 10^2 \times 10 \equiv \_\_\_\_ \times 10 \equiv \_\_\_\_ \pmod{33}$

【問 4】すべての数が元の数と同じに戻るのは何乗か。

11 乗，21 乗，31 乗，41 乗 で元に戻ることは，一覧を見れば一目でわかる。理屈の上では，2 つの素数の積 $pq = 33$ を mod にしたとき，$p - 1 = 2$, $q - 1 = 10$ の公倍数 10 の倍数 10, 20, 30, $\cdots$ に 1 を加えた 11, 21, 31, $\cdots$ で元に戻ることが，わかっている。しかし，高校生に理屈から入っても無理があるので，実際の数で体験してもらうことを主眼としたのである。[5)]

（例）21 乗で元の数に戻る。$\Rightarrow 21 = 3 \times 7 \Rightarrow$ 3 乗して ____ 乗すると元に戻る。

「3 乗して 33 で割った余りで暗号化」として公開鍵にすれば，「____ 乗して 33 で割った余りが復号」を秘密鍵とする。

mod 33 ならば，アルファベット 26 文字を超えるので，文字を対応させて，自分の名前を暗号化したり，暗号化した文字列を復号したりさせた。

4　実際の桁数の計算

mod 33 では $33 = 3 \times 11$ と素因数分解でき，暗号化の鍵 3 乗から，簡単に復号鍵 7 乗が計算されるため，実際は p, q とも 1024 ビット（10 進数で 308 桁以上）の素数を使っている。つまり mod pq は 2048 ビット（10 進数で 617 桁以上）の数となる。

図は，ある銀行のディジタル証明書で，フィールド「公開キー」の値の画面を見ると「RSA(2048 Bits)」となっている。下の窓には，おそらく 16 進数で 2048 ビット分の公開キーや暗号化の累乗が書かれている。

最後に Mathematica での巨大数を実演した。まず 2 つの素数 p, q は次の通り。

[5)] 一応理屈はプリントに掲載したが，説明はしなかった。

素数 $p =$
898846567431157953864652595394512366808988489471153286367150405788663379027504815663542386612037680105600569399356966788293948844072083112464237153197370621888839467124327426381511098004705972654147604250288441907534117123144073695655527041361858167525534229314911062399736229692398581524176781648121120704 71

素数 $q =$
179769313486231590772930519078902473361797697894230657273430081157732675805500963132708477322407536021120113879871393357658789768814416622492847430639474124377767893424865485276302219601246094119453082952085005768838150682342462881473913110540827237163350510684586298239947245938479716304835356329624224135819

これらの積 pq を mod にする。[6)]

mod $pq =$
161585030356555036503574383443349759802220513348577420160651727137623275694339454465986007057614567318443589804609490974705779575245460547544076193224141560315438683650498045875098875194826053398028819192033784138396109321309878080919047169238085235290822926018152521443787945770532904303776199561965192970298532249550858665420076860664214977241507215494761423948232337845214071860101725114151138375664254957344414969468493672459861360538979845122681786284261453524274735611267709116513276514542263837954368993317566779549468221974524795479579807988036344493470759917359102741227134662105711077550372652938803300749

公開鍵（暗号化の累乗）e を

$e = 3571$

とし，mod pq とともに公開する。暗号化する文字列「磯辺」の文字コード (Unicode)「78EF 8FBA」を 10 進数に直したものが次の M。

平文 $M = 2028965818$

これを 3571 乗[7)]して「pq」で割った余りが次の暗号文 C.

$C = M^e = 2028965818^{3571} \equiv$
123090888097601069308548713328328154273673587050719243414263417283286391241181278922716598849000211185708410759913882550697458969549712690888749356715238269910858207386849756541456685420512940946797627316331573418050934865224880024548827031643231433587995248691375931719160163403105837604510755939244326019673147153731323092590739607432957496183618594763457458071027930877281960919614006656576640976967061145518125051466861648558436802045991375131271373588630112143268523485700108707747086849070664804595610510350549331160607337051270352050593515765948245114832089473572596967011570086379763332985748743679893561124 05 mod pq

2028965818^{3571} は 33237 桁になるが，累乗してから余りを求めるのではなく，2028965818 倍して，pq を超えたら pq の倍数を引くという手順で高速に計算されるのは，手作業で体験したとおりである。

「$e = 3571$ 乗」の暗号化とペアになる秘密鍵（復号の累乗）は $p-1$ と $q-1$ の公倍数 を l として，次の d のように決める。

[6)] 2 つの素数を見つけるには Mathematica を使った。

[7)] 5 乗や 7 乗くらいでいいのだが，平文が漢字 2 文字 (32 ビット) 程度だと暗号文が pq を超えないから，逆算できてしまう。パスワードにある程度の長さが必要な理由にもなる。

$$d = (1192l + 1) \div 3571 =$$
$$269685460914328764368889197793997358841006513457720925275128617681387488977390968529060935890053996420589133361935749364582683523574525188640052349794499814336264392479857094240872554735819555525769397262348141566689557019196322804150875164179946760017735381235139145975370977756349415036825836318648312937836382286599709345349744215203005693510234980636164536574368523685262799626393244668927266864902367929198988785023752354159594492230779712326645554232252309132084661038994282016141913427027532374814610690586762101463740586678315736826327394139943156294989448791899352411292594074198099619873906848010850472929 1 乗

これで暗号文を累乗計算すると

$$C^d \equiv 2028965818 \bmod pq$$

と復号する。桁数が膨大でも，「余りの累乗の余り」は非常に高速に計算できる。実際にパスワードなどの入力画面で時間がかかることはない。

5　安全性

この 617 桁（2048 ビット）の pq を素因数分解できれば暗号が解読されるが，スーパーコンピューターでも生きている間には終わらない。

308 桁の素数は 700 個に 1 個程度の 10^{305} 個くらいあることがわかっているから，2 つの素数の組み合わせが不足することはない。[8)]

RSA 暗号解読コンテストが 1991 年から行われていて，現在 768 ビットの RSA までが解読に成功している。コンピュータの性能が上がれば桁数を増やし，常に「生きている間には解読できない桁数」にしておけばよい。当初は 1024 ビットで始まったが，現在は 2048 ビットや 4096 ビットが使われている。

また，RSA と比べて，同レベルの安全性をより短い鍵で実現でき，処理速度も速い楕円曲線暗号（ECC）も使われ始めている。

しかし，RSA や ECC のような「計算の手間」を安全性の根拠とする暗号は，今は安全でも，巨大数の素因数分解を高速で行える手順[9)]が，量子コンピュータに実装されれば，その時点でこれらの暗号方式は使えなくなってしまう。したがって，量子暗号など「計算の手間」を安全性の根拠としない，新しい暗号技術が研究されている。

6　数学の話題として

暗号技術は，ネットショッピングをはじめ，現代の便利な生活を支えている重要な技術である。授業では，フェルマーについても触れて，「350 年前，フェルマーはこうした理論が実生活に役立つとは思いもしなかったろう。」と，数学と人間の生活とのかかわりについて，話すことができてよかったと思う。

8) 実際の素数は，厳重に管理され，不定期に交換している。
9) Shor のアルゴリズム