1 RSA暗号の解読

前回は「RSA暗号」と呼ばれる公開鍵暗号の仕組みを解説した。今回は，RSA暗号を解読することによって，理解を深めることを目的とする。

1.1 整数に関連するMathematicaの命令 (復習)

前回解説した命令のうち，今回も使うものを再掲しておく。

[整数の剰余] (小学生割り算)

`Mod[m, n]` は，`m` を `n` で割った余りを与える。

[整数のベキの剰余]

`PowerMod[a, b, n]` は，a^b を `n` で割った余りを与える。

(`PowerMod[a, b, n]` は，`Mod[a^b, n]` と同じ答を与えるが，効率がよくなる。)

[m を法とする逆数]

`PowerMod` を用いると，ある数 m を法とする a の逆数 (すなわち,「$ax \equiv 1 \mod m$」を満たす x) を，`PowerMod[a,-1,m]` として求めることができる。

[最小公倍数] (Least Common Multiple)

`LCM[m, n, ... ]` は，整数 `m`, `n`, ... の最小公倍数を返す。

[素因数分解]

`FactorInteger[n]` は，整数 `n` の素因数をこれらの指数とともにリストとして返す。

例：$2434500 = 2^2 \cdot 3^2 \cdot 5^3 \cdot 541^1$ を `FactorInteger` を用いて計算すると，次のように出力される。

`FactorInteger[2434500]` ⇒ `{{2,2},{3,2},{5,3},{541,1}}`

[n を法とする方程式]

`Solve` では，自然数 n に対して，mod n での方程式を解くこともできる。

例：$5x \equiv 6 \mod 7$ を満たす $x \in \{0,1,2,3,4,5,6\}$ を求める。

```
Solve[{5 x == 6, Modulus == 7}, x, Mode -> Modular]
    ⇒ {{Modulus -> 7, x -> 4}}
```

解がない場合には，“`x -> **`” という部分が出てこない。

また，`Modulus` が指定してあれば，“`Mode -> Modular`” の部分は省略可能。

1.2 RSA暗号の仕組み (復習)

「RSA暗号」とは，次のようにして作られる整数の組 (m, k_1, k_2) を用いて，暗号化・復号化を行うことであった。

RSA 暗号の仕組み

下準備 ：

1. 2 つの素数 p, q をとり, $m = pq$ とおく。
2. $p-1$ と $q-1$ の最小公倍数 $L = LCM(p-1, q-1)$ を計算しておく。
3. $L = LCM(p-1, q-1)$ と互いに素な自然数 k_1 (すなわち，L との最大公約数が 1 となるような k_1) を定め,

$$k_1 k_2 \equiv 1 \bmod L$$

となる自然数 k_2 を計算しておく。(すなわち，k_2 は $\bmod L$ での k_1 の逆数。)

暗号化鍵（公開） m, k_1： 暗号化関数 $f : i \longmapsto i^{k_1} \bmod m$.

復号化鍵（秘匿） k_2： 復号化関数 $g : c \longmapsto c^{k_2} \bmod m$.

例 1: $p = 3$, $q = 7$

このときは，次のようにして $(m, k_1, k_2) = (21, 5, 5)$ が得られる。

$$m = pq = 21, \quad L = LCM(p-1, q-1) = LCM(2, 6) = 6,$$
$L = 6$ と互いに素である整数として $k_1 = 5$ を選ぶ。
$\Rightarrow$ $L = 6$ を法とする $k_1 = 5$ の逆数を求めて,$k_2 = 5$

これが実際に暗号として働くことを見るために，$\bmod 21$ のべき乗の表を書いておく。(a^n で，$1 \le a \le 20, 1 \le n \le 20$ としてある。)

$a\backslash n$	**1**	2	3	4	5	6	**7**	8	9	10	11	12	**13**	14	15	16	17	18	**19**	20
1	**1**	1	1	1	1	1	**1**	1	1	1	1	1	**1**	1	1	1	1	1	**1**	1
2	**2**	4	8	16	11	1	**2**	4	8	16	11	1	**2**	4	8	16	11	1	**2**	4
3	**3**	9	6	18	12	15	**3**	9	6	18	12	15	**3**	9	6	18	12	15	**3**	9
4	**4**	16	1	4	16	1	**4**	16	1	4	16	1	**4**	16	1	4	16	1	**4**	16
5	**5**	4	20	16	17	1	**5**	4	20	16	17	1	**5**	4	20	16	17	1	**5**	4
6	**6**	15	6	15	6	15	**6**	15	6	15	6	15	**6**	15	6	15	6	15	**6**	15
7	**7**	7	7	7	7	7	**7**	7	7	7	7	7	**7**	7	7	7	7	7	**7**	7
8	**8**	1	8	1	8	1	**8**	1	8	1	8	1	**8**	1	8	1	8	1	**8**	1
9	**9**	18	15	9	18	15	**9**	18	15	9	18	15	**9**	18	15	9	18	15	**9**	18
10	**10**	16	13	4	19	1	**10**	16	13	4	19	1	**10**	16	13	4	19	1	**10**	16
11	**11**	16	8	4	2	1	**11**	16	8	4	2	1	**11**	16	8	4	2	1	**11**	16
12	**12**	18	6	9	3	15	**12**	18	6	9	3	15	**12**	18	6	9	3	15	**12**	18
13	**13**	1	13	1	13	1	**13**	1	13	1	13	1	**13**	1	13	1	13	1	**13**	1
14	**14**	7	14	7	14	7	**14**	7	14	7	14	7	**14**	7	14	7	14	7	**14**	7
15	**15**	15	15	15	15	15	**15**	15	15	15	15	15	**15**	15	15	15	15	15	**15**	15
16	**16**	4	1	16	4	1	**16**	4	1	16	4	1	**16**	4	1	16	4	1	**16**	4
17	**17**	16	20	4	5	1	**17**	16	20	4	5	1	**17**	16	20	4	5	1	**17**	16
18	**18**	9	15	18	9	15	**18**	9	15	18	9	15	**18**	9	15	18	9	15	**18**	9
19	**19**	4	13	16	10	1	**19**	4	13	16	10	1	**19**	4	13	16	10	1	**19**	4
20	**20**	1	20	1	20	1	**20**	1	20	1	20	1	**20**	1	20	1	20	1	**20**	1

表から分かるように，べきが $n = 1, 6, 13, 19, ...$ と，6 $(= L)$ 周期でもとに戻っていることが分かる。また，$n = 5$ のところでは，$1 \sim 20$ の数字が，順番が入れ替わってすべて現れていることが分かる。RSA 暗号では，このことを利用して次のように暗号化する。

1. 暗号化したい文章を，$1 \sim 20$ の数字で置き換える。(この処理を**「符号化」**という。)
   例として，次のように符号化されたとする。
   `a = {10, 11, 12, 13, 14}`
2. $1 \sim 20$ を並べた列のそれぞれを，21 $(= m)$ を法として 5 $(= k_1)$ 乗する。
   `b = PowerMod[a,5,21]` ⇒ `{19, 2, 3, 13, 14}` (これが暗号文)
3. 暗号文を復号化するには，21 $(= m)$ を法として 5 $(= k_2)$ 乗する。
   `PowerMod[b,5,21]` ⇒ `{10, 11, 12, 13, 14}` (もとに戻った)

(今の場合はたまたま $k_1 = k_2$ となっているので，やや紛らわしい。)

例 2: $p = 409$, $q = 463$

この場合は，前回のプリントにあるように $(m, k_1, k_2) = (189367, 7919, 24287)$ と選ぶことができる。

[暗号化・復号化の例]

もとの文： `a = {3001, 3002, 3003, 3004, 3005}`
暗号化: `b = PowerMod[a,7919,189367]` ⇒ `{8198, 120109, 54064, 32358, 86427}`
復号化： `PowerMod[b,24287,189367]` ⇒ `{3001, 3002, 3003, 3004, 3005}`

1.3 RSA 暗号の解読 I

前節での計算では，暗号化・復号化に用いられる整数の組 (m, k_1, k_2) がすべて分かっているとして計算した。実際の利用の際には，

公開鍵 (m, k_1) のみが公開されていて，秘密鍵 k_2 は作った本人しか知らない

という点が重要である。k_2 を使えば容易に解読できることは前節で見たとおりだが，それを知らない場合に解読できるかどうかを試してみよう。

実は，前節の例くらいの，比較的小さな公開鍵では，k_2 を知らなくてもすぐに解読できてしまう。前節の「例 2」で試してみよう。すなわち，

公開鍵： `(m, k1) = (189367, 7919)`
暗号文： `b = {8198, 120109, 54064, 32358, 86427}`

のみを使ってもとの文を取り出すことができるかどうかを試してみる。

今，暗号文の最初の数 8198 ともとの数字 x との関係は

$$x^{7919} \equiv 8198 \mod 189367$$

であるので，これを Mathematica で解いてみる。

入力： `Solve[{x^7919 == 8198, Modulus == 189367}, x]`
出力： `{Modulus → 189367, x → 3001}`

このようにあっさり解けて，秘密鍵なしでも復号化ができてしまう。

暗号文の 5 個のデータをまとめて解いて，計算にかかる時間を計ってみよう。

入力：
```
b = {8198, 120109, 54064, 32358, 86427};
Timing[
    Solve[{x^7919 == b[[1]], Modulus == 189367}, x]
    Solve[{x^7919 == b[[2]], Modulus == 189367}, x]
    Solve[{x^7919 == b[[3]], Modulus == 189367}, x]
    Solve[{x^7919 == b[[4]], Modulus == 189367}, x]
    Solve[{x^7919 == b[[5]], Modulus == 189367}, x]
]
```
出力：`{0.031 Second, {{(Modulus → 189367)^5, (x → 3001), ...(略)...}}}`

ここで，`Timing[ ... ]` は，命令の実行時間を測るものである。5 個合わせても，0.031 秒で解読できていることが分かる。これでは暗号としては使い物にはならない。

1.4 RSA 暗号の解読 II

それでは，もう少し大きな素数に対する暗号を考える。

`p = Prime[50000]`	⇒	$p = 611953$
`q = Prime[51000]`	⇒	$q = 625187$
`m = p*q`	⇒	$m = 382585060211$
`L = LCM[p-1, q-1]`	⇒	$L = 191291911536$

この L と互いに素である自然数としては，

`k1 = Prime[52000]` ⇒ $k_1 = 638977$

を選ぶことにする。この k_1 の $L = 191291911536$ を法とする逆元は，

`k2 = PowerMod[k1, -1, L]` ⇒ $k_2 = 93144551857$

こうして，公開鍵 (暗号化鍵) $(m, k_1) = (382585060211, 638977)$，秘密鍵 (復号鍵) $k_2 = 93144551857$ が得られた。

公開鍵を使って暗号化を行ってみよう。

1. 暗号化する数字を用意する。ここでは，$a = 1234567890$ としよう。
2. $a^{k_1} \mod m$ を計算して暗号化する。得られた結果は b とおくことにする。
   今の場合は，

$$b = a^{k_1} = 1234567890^{638977} \equiv \underline{311589097182} \pmod{382585060211}$$

   という暗号文が得られる。

次に，暗号文 $b = 311589097182$ と公開鍵 $(m, k_1) = (382585060211, 638977)$ のみから，もとの a を計算してみよう。数学的には，

$$x^{638977} \equiv 311589097182 \mod 382585060211$$

という方程式を，x について解けばよいことになる。対応する Mathematica の命令は，

```
Solve[{x^638977 == 311589097182, Modulus == 382585060211}, x]
```

である。しかし，この命令を入力すると，次のようなエラーメッセージが帰ってくる。

```
Roots::badmod: 入力法 382585060211 を押出できません.
```

これは，今用いた $m = 382585060211$ が，計算機には大きすぎたためである。

さて，今の例では，`Solve` 命令のみを用いて暗号を解読することは難しいことが分かった。そこで，次の解読の手順を試してみよう。

素因数分解による解読

[手順 1] m を素因数分解して，p, q を作り出す。

[手順 2] 得られた p, q から $L = LCM(p-1, q-1)$ を計算する。

[手順 3] 得られた L を法として k_1 の逆数を計算し，k_2 とおく。

[手順 4] 得られた k_2 を用いて $b^{k_2} \mod m$ を求める。

上述の [手順 1]〜[手順 4] のうち，[手順 2] 以降は RSA 暗号の秘密鍵 (復号鍵) k_2 を作り出す手順に他ならない。計算機からすると，最も計算時間がかかるのは [手順 1] の素因数分解であり，他はそれと比べると短時間で終わる。

先ほどの例の $m = 382585060211$ を Mathematica の `FactorInteger` で素因数分解して，計算に要する時間を計測してみよう。

```
In[1]:= Timing[FactorInteger[m]]
Out[1]= {0. Second, {{611953, 1}, {625187, 1}}}
```

このように，正しい p, q がすぐに得られることが分かる。この p, q をもとに [手順 2]〜[手順 4] を実行すれば，暗号文 b が解読できてしまう。このことから分かるように，RSA 暗号を実際に利用する際には，素因数分解がすぐには実行できないように，十分大きな m を作り出す必要がある。

現時点の RSA 暗号では，1024 ビットの暗号鍵 (10 進で約 310 桁) が主流となっているが，素因数分解の理論とコンピュータの能力が発展すれば，従来安全であったものでも危険になってしまうので，技術の進歩に合わせて，暗号鍵そのものをより安全性の高いものへと取り替えていく必要がある。

素因数分解を計算機で実行するための手法は色々あるが,「数体ふるい法」と呼ばれる手法についてのノートが，木田先生の Web ページ

```
http://www.rkmath.rikkyo.ac.jp/~kida/bunkai.htm
```

にある。

1.5 相手を認証（確認）する

ネットワーク上のショップで買い物をするとしよう。支払いは通常の銀行振り込みということもあるが，その場でクレジット・カード決済をすることが多い。その際，利用者名,

カード番号，有効期限などを相手に知らせるが，本当にそこが amazon なり楽天なりのサイトであることを，どうすれば確認できるのだろうか。それができなければネット上での買い物なんてできるわけがない。ましてや，ネット上の銀行や証券会社なんて誰も利用しないだろう。こういう相手の認証も RSA 暗号の仕組みで行えるのである。

amazon の公開鍵が m と k_1 だったとしよう。amazon のサイトと思われるところに，こちらから問い合わせをする。それに対する返答 c を m と k_1 で変換したところ正しいメッセージ d になったとする。これは返答 c が，正しいメッセージ d を，公開鍵の m と秘密鍵 k_2 とで変換されていることを示す。相手は秘密鍵を知っているのだから，amazon の正しいサイトであるということになる。

さて，この仕組みが正しく機能するためには amazon の公開鍵が m と k_1 であることが確認できなければいけない。それは認証局というサイトが行う。では認証局の認証はどうするのか。実は，認証局の公開鍵はインターネット・イクスプローラーなどのブラウザに最初から登録されているのである。

ツール → インターネットオプション → コンテンツ → 証明書

でそれらを見ることができる[1]。

1.6 参考文献

今回までに扱ったように，Mathematica を用いると様々な整数の性質を実験的に調べることができる。興味を持った方は，以下の文献を見るとよい。

ジョセフ・H・シルヴァーマン 「はじめての数論」(原著第 3 版，鈴木治郎 訳)，ピアソン・エデュケーション，2007 年，3570 円 (税込)

著者が (文系を含む) 学生に対して行った入門的講義のテキスト。計算機を用いる課題も多数用意されている。

木田祐司・牧野潔夫 「UBASIC によるコンピュータ整数論」

書籍版： 日本評論社，1994 年，3500 円+税 [絶版]

電子版： `http://www.rkmath.rikkyo.ac.jp/~kida/kima.htm`

現在では電子版が木田先生のホームページより無料で手に入るので，ぜひ眺めていただきたい。UBASIC という言語で書かれているが，それを Mathematica のプログラムに書き直すことは，大変良い勉強になる。

木田祐司 「初等整数論」(講座 数学の考え方 **16**)，朝倉書店，2001 年，3990 円 (税込)

整数論に対する入門書。計算機でプログラムを組むことを念頭においた説明がなされているので，実際にプログラムを書いて動かしてみると良い。

2 今日の課題

【課題 1】(RSA 暗号の解読 1)

公開鍵 $(m, k_1) = (1471719773, 46447)$ の RSA 暗号を考える。このとき，暗号文 $b = 1397724479$ を 2 通りの方法で解読し，かかる時間を比較してみよう。

[1] 認証局のレベルではすでに 2048-bit の RSA 暗号が使われている。

(1) Solve で解くときにかかる時間を測定するには,

```
m = 1471719773
k1 = 46447
b = 1397724479
```

を入力しておいてから，次の命令を入力すればよい。

```
Timing[Solve[{x^k1 == b, Modulus == m}, x]]
```

結果として出力される計算時間と，x の値 (すなわち暗号化前の数字) を記せ。

(2) 素因数分解によって解読する場合には，素因数分解の部分に一番時間がかかる。Mathematica の命令

```
Timing[FactorInteger[m]]
```

によって，素因数分解にかかる時間を調べ，結果として出力される計算時間と，2 つの素数を記せ。

【課題 2】 (RSA 暗号の解読 2)

この課題では，以下の表に従ってひらがなを 1 文字ずつ数字に直し，それらを並べて大きな整数を作る。(たとえば,「**すうがく**」ならば 23136618 になる。)

あ 11	い 12	う 13	え 14	お 15	か 16	き 17	く 18	け 19	こ 20
さ 21	し 22	す 23	せ 24	そ 25	た 26	ち 27	つ 28	て 29	と 30
な 31	に 32	ぬ 33	ね 34	の 35	は 36	ひ 37	ふ 38	へ 39	ほ 40
ま 41	み 42	む 43	め 44	も 45	や 46		ゆ 48		よ 50
ら 51	り 52	る 53	れ 54	ろ 55	わ 56	ゐ 57		ゑ 59	を 60
ん 61	空白 62				が 66	ぎ 67	ぐ 68	げ 69	ご 70
ざ 71	じ 72	ず 73	ぜ 74	ぞ 75	だ 76	ぢ 77	づ 78	で 79	ど 80
ば 81	び 82	ぶ 83	べ 84	ぼ 85	ぱ 86	ぴ 87	ぷ 88	ぺ 89	ぽ 90

各自の学籍番号に応じて，RSA 暗号を解読してみよう。Web ページ

http://www.rkmath.rikkyo.ac.jp/~kakei/kadai10.html

に，各自の学籍番号に対応した問題が用意してある。

(1) 公開鍵 m を素因数分解して，要する時間を測定せよ。(要する時間は問題によって異なるし，使用する計算機によっても異なってくる。)

(2) (1) の結果として，2 つの素数 p，q が得られる。これらを元に，1.4 節の手順に従って秘密鍵 k2 を作成し，暗号文 b の復号化を行え。

(3) 復号化の結果として得られる数字を 2 桁ごとに区切り，上の表によってひらがなに直すと，有名な和歌の上の句が得られる。その下の句と作者の名前を答えよ。

《参考》「ゐ」「ゑ」をローマ字入力するには，それぞれ「wi」「we」とタイプして変換すればよい。

これらの課題に対して，次のような出力が得られるように LaTeX で記述し，PDF ファイルを作成して CHORUS で提出せよ。ただし，枠で囲まれた部分については，該当する Mathematica の計算結果を記入すること。

計算機１・２ 第10回 課題

学籍番号: ******** 氏名: ********

平成19年6月26日

課題１ RSA暗号の解読 1

(1) 計算に要した時間： Mathematica で得られた結果を記す

得られた x の値： Mathematica で得られた結果を記す

(2) 計算に要した時間： Mathematica で得られた結果を記す

得られた素数の組： Mathematica で得られた結果を記す

課題２ RSA暗号の解読 2

(1) 計算に要した時間： Mathematica で得られた結果を記す

(2) $p =$ Mathematica で得られた結果

$q =$ Mathematica で得られた結果

秘密鍵 $k_2 =$ Mathematica で得られた結果を記す

復号化の結果： Mathematica で得られた結果 (数字) を記す

(3) 得られた上の句： ひらがなに直した結果

対応する下の句： 調べて得られた結果

作者： 調べて得られた結果