高校生のための現代数学講座
「素数」
講義 (3)　寺杣　友秀

東京大学
玉原国際セミナーハウス
2012 年 7 月 28 日

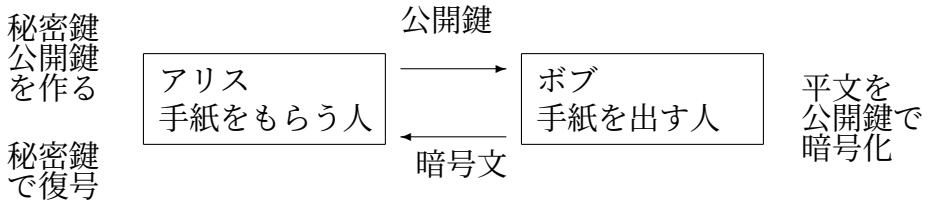
「計算機による実験」

1　暗号化と復号の手順

ＲＳＡ暗号は、素因数分解には現在のところ時間がかかることを安全性の根拠に使い、一方、素数に関係した数学の定理を用いて、暗号化し復号する方法であり、現在のコンピュータ・ネットワークに非常に多く用いられている。

- 情報を受け取る人が鍵をつくる。鍵は公開鍵と秘密鍵をワンセットとして作る。
- 秘密鍵は誰にも教えない。秘密情報を暗号化する人にも教えない。
- 暗号化する人は公に公開されている鍵を用いて秘密情報を暗号化する。暗号化したものを暗号分という。
- 暗号文を秘密鍵を用いて復号する。

公開鍵＝暗号化のための鍵
秘密鍵＝暗号解読（復号）のための鍵



（1）公開鍵と秘密鍵をつくる。

- 暗号を受け取る方の人をアリスと呼ぼう。アリスは素数を 2 つ用意する (最後の表を参考にせよ。なるべくランダムに選ぶ。）ここでは説明のため、小さい素数、例えば、$p = 13, q = 17$ を選んだとする。
- $n = pq$ を計算する。上の例では $n = pq = 221$ である。

  この n の桁数が十分大きいと、約数を見つけるのに今の計算機の方法では長い時間がかかる。例えば、10000 年以上かかるという桁数の n を作っておく。例えば 100 桁の p, q の積として 10000 桁の n を作っておく。

- アリスは $(p-1)(q-1)$ と互いに素となる f を適当にとり、合同式

$$fd = 1 \bmod (p-1)(q-1)$$

  を下のやり方でユークリッドの互除法を用いて解いて、解 d を秘密鍵として保管する。

- 例えば、上の例では $(p-1)(q-1)=192$ となるが、$f=7$ とすると $GCD(7,192)=1$ なので $7d+192k=1$ を満たす整数 d,k を求めることができる。

$$7\times 55+192\times(-2)=1$$

となるので、$7d=1 \bmod 192$ の解のひとつが $d=55$ となる。これが秘密鍵である。

桁数が 10000 桁でも、この合同式の計算は短い時間でできる。

- 一日目のアルゴリズムで d は求まる。homepage の http://gauss.ms.u-tokyo.ac.jp/gcd.html でも求められる。

$$\left[\ f\ \right]\times\left[\quad\right]+\left[\ (p-1)(q-1)\ \right]\times\left[\quad\right]=\left[\quad\right]$$

を入力して $\left[\ =\ \right]$ のボタンを押すと

$$\left[\ f\ \right]\times\left[\ d\ \right]+\left[\ (p-1)(q-1)\ \right]\times\left[\ k\ \right]=\left[\text{最大公約数}\right]$$

と答えが帰ってくる。

- この計算は筆算するときに、ひとつ注意が必要である。

$$f\times d+(p-1)(q-1)\times k=1$$

となる d,k を求めたとき d が負の数になることもある。このとき d に $(p-1)(q-1)$ の何倍かを加えることにより正の数に取り換えることにする。

（2）公開鍵を公開する。

- 公開鍵である $n=pq=221$, $f=7$ をだれにでも読める場所に公開する。今回は秘密の数字を送ってくれる人に教えよう。これはこの数字を解読しようとする、悪意の第三者に知られてもかまわない。ただし秘密鍵である d は誰にも知られないように自分で保管する。秘密の情報を送ってくれる人にも秘密鍵は教えない。（暗号化するのに秘密鍵は必要ない。）

実際には、コンピュータ同士が、桁数が 100 桁位の n と、f をやり取りする。

（3）ボブは公開鍵を使って情報を暗号化してアリスに伝える。

- 秘密の数字を送るひと（仮にボブと呼ぼう）はアリスにだけ教えたい数字 a をもとに、アリスにだけ解読できるような数字 b に公開鍵 n,f を用いて暗号化する。平文 a から暗号文 b をつくる規則は

$$b\equiv a^f \mod n,$$

である。暗号文つまり、この数字 b をアリスに送る。上の例を使うと、$a=76$ を暗号化して送りたいとすれば、76 の 7 乗 $\bmod 221$ を計算して

$$b=15$$

となる。秘密鍵である 55 を知らないと $b=15$ から $a=76$ を復元することはとても難しい。

- pq を法とした a の f 乗をしたものが暗号文である。homepage の http://gauss.ms.u-tokyo.ac.jp/power-modulo.html でも求められる。

$$\left[\ a\ \right]\text{の}\left[\ f\ \right]\text{乗}\ mod\left[\ n\ \right]\text{は}\left[\quad\right]$$

を入力して $\left[\text{は}\right]$ のボタンを押すと

$$\left[\ a\ \right]\text{の}\left[\ f\ \right]\text{乗}\ mod\left[\ n\ \right]\text{は}\left[\ b\ \right]$$

と答えが帰ってくる。

時間に余裕のある人は、次の章に書いてあるアルゴリズムを用いて pq を法とした a の f 乗を電卓でも効率的に求められるので、試してみよう。

（4）秘密鍵を用いて暗号文を平文に復号する。

- アリスは、この数字 b, に対し、他人に読まれないように保管してあった (n, d) を用いて、

$$c \equiv b^d \mod n,$$

を計算する。例について、15 の 55 乗 mod 221 を計算すると 76 となる。暗号文である 15 から暗号化される前の平文 76 を求めるのは秘密鍵を知らない人にとっては、大変時間がかかる。

d 乗 mod n の計算は、後で説明するように d を 2 進展開して、 mod n の d 倍の計算、 mod n の 2 乗の計算を繰り返して効率的におこなう。

- 通常はこれで終わりですが、今回は解読した値がボブの送りたかった数であることをボブに確認してみましょう。

「あなたの秘密の数字は**ですね？」

これが当たっていれば成功である。

2 累乗の計算と合同式と２進法（発展）

- 7 乗を計算するのは、3 桁の１００前後の数字の７乗は、１５桁でかろうじで電卓上に表せるくらいである。
- 55 乗を計算するのはそのままでは１００桁を超えて無理である。
- しかし、 mod 221 の計算は、常に 3 桁であるので、合同式として計算することに大きなメリットがある。
- ３桁同士の掛け算といっても５５回掛けるのは大変である。以下のように工夫できる。
- 55 を 2 で繰り返し割り算をして、あまりを書いていく。

$$\begin{aligned}
55 \div 2 = 27 \quad &\text{あまり} \quad 1 \\
27 \div 2 = 13 \quad &\text{あまり} \quad 1 \\
13 \div 2 = 6 \quad &\text{あまり} \quad 1 \\
6 \div 2 = 3 \quad &\text{あまり} \quad 0 \\
3 \div 2 = 1 \quad &\text{あまり} \quad 1 \\
1 \div 2 = 0 \quad &\text{あまり} \quad 1
\end{aligned}$$

従って「あまり」を下からよんでいくことにより、55 は 2 進数で $\overset{5\,4\,3\,2\,1\,0}{110111}$ と表わされる。（ふつうは下の数字は書かない。0 と 1 が並ぶと何桁目が見にくいので、参考までに小さく書いた。）すなわち、

$$55 = 2^5 + 2^4 + 2^2 + 2^1 + 2^0 = 32 + 16 + 4 + 2 + 1$$

である。

- これを使うと、

$$b^{55} = b^{32} \times b^{16} \times b^4 \times b^2 \times b$$

と 2 乗の計算と掛け算を用いて、効率的に計算できる。

$$\begin{aligned}
15^2 &\equiv 4 \quad (mod\ 221)\\
15^4 &\equiv 4^2 \equiv 16 \quad (mod\ 221)\\
15^8 &\equiv 16^2 \equiv 35 \quad (mod\ 221)\\
15^{16} &\equiv 35^2 \equiv 120 \quad (mod\ 221)\\
15^{32} &\equiv 120^2 \equiv 35 \quad (mod\ 221)
\end{aligned}$$

従って

$$15^{55} \equiv 35 \times 120 \times 16 \times 4 \times 15 \quad (mod\ 221)$$

となる。最後の掛け算もかけるたびに 221 で割った余りで置き換えることにより電卓でも十分効率よく計算できる。実はもう少しだけ効率がよく計算できる方法があるのだが、それは自由研究ということにしよう。

素数の表 (100 から 300)

$$\begin{aligned}
&101, 103, 107, 109, 113, 127, 131, 137, 139, 149,\\
&151, 157, 163, 167, 173, 179, 181, 191, 193, 197,\\
&199, 211, 223, 227, 229, 233, 239, 241, 251, 257,\\
&263, 269, 271, 277, 281, 283, 293
\end{aligned}$$

演習のためのメモ

(1) 鍵をつくるのためのメモ

(a) 3 桁の異なる素数（他人になるべく推測されないもの）を二つ選ぶ。

$$p = \boxed{}, \quad q = \boxed{}$$

(b) $n = pq$, $(p-1)(q-1)$ を計算する。

$$n = pq = \boxed{}, \quad (p-1)q-1) = \boxed{}$$

(c) $(p-1)(q-1)$ と f が互いに素になるように (2 桁位の)f を選び

f	$\times$	d	$+$	$(p-1)(q-1)$	$\times$	k	$=$	1
$\boxed{}$	$\times$	$\boxed{}$	$+$	$\boxed{}$	$\times$	$\boxed{}$	$=$	1

をみたす d と k を求める。

(d) これで自分の公開鍵と秘密鍵ができた。

公開鍵は $n = \boxed{}, \quad f = \boxed{}$

秘密鍵は $d = \boxed{}$.

(e) 次のページに公開鍵を書いて、暗号文を送る人に渡し、暗号文を送ってもらおう。

(2) 暗号化のためのメモ

(a) 送りたい 2 桁の数を平文として決める。

$$a = \boxed{}$$

(b) 送りたい相手の公開鍵を使って平文を暗号化する。

公開鍵は $N = \boxed{}, \quad F = \boxed{}$

暗号文 b は次の規則で求める。

a	の	F	乗	mod	N	$\equiv$	b
$\boxed{}$	の	$\boxed{}$	乗	mod	$\boxed{}$	$\equiv$	$\boxed{}$

この b を送りたい相手に伝える。（他人にみられても b から a を復元するのは難しい。）

(3) 復号化のためのメモ

秘密鍵を用いて暗号文を平文に復号する。暗号分 a から平文 b を求めるには次の規則を使う。

b	の	d	乗	mod	n	$\equiv$	a
$\boxed{}$	の	$\boxed{}$	乗	mod	$\boxed{}$	$\equiv$	$\boxed{}$

□様、

私の公開鍵

$$n = \square, \quad f = \square$$

を使って平文を暗号化したものを下の□に書いて、返送してください。

□

. . . . . .

□様、

私の公開鍵

$$n = \square, \quad f = \square$$

を使って平文を暗号化したものを下の□に書いて、返送してください。

□

. . . . . .

□様、

私の公開鍵

$$n = \square, \quad f = \square$$

を使って平文を暗号化したものを下の□に書いて、返送してください。

□