RSA 暗号を教える

大谷（おおたに）　茂（しげる）

§1. はじめに

整数の授業の締めに RSA 暗号の原理の証明はいかがでしょうか。合同式は既知とします。問題形式で逆元の存在，フェルマーの小定理，中国剰余定理，オイラー関数を学びます。最後に RSA 暗号の原理を証明します。

§2. RSA 暗号とは

RSA 暗号の手順を簡単に説明します。

⑴　好きなアルファベットを 1 つ選びなさい。
⑵　コード表を使ってその文字を数に直します。
⑶　その数を mod 33 で 13 乗しなさい。
　　（大変なのでべき乗表を使ってください）
⑷　さらに 17 乗しなさい。

すると，必ず元の数に戻ります。たとえば

$$\mathrm{A}\to\underline{2}\to 2^{13}\equiv 8\to 8^{17}\equiv\underline{2}$$

手順⑶を「暗号化」，手順⑷を「復号化」，$(N,\ e)=(33,\ 13)$ を「公開鍵」，$d=17$ を「秘密鍵」といいます。

コード表と公開鍵は皆が知っています。送信者はこれを使って伝えたい文を暗号化し，受信者に送ります。秘密鍵は受信者だけが知っています。受信者は秘密鍵を使って暗号文を解読します(復号化)。第三者が暗号文を傍受したとして，これを解読するには，公開鍵から秘密鍵を求めればよい。これは理論上は可能ですが，実はとんでもなく時間がかかってしまい，現実には不可能です。かくして RSA 暗号は安心して世界中で使われているわけです。

問題 1　（**RSA 暗号**）mod 33 とする。任意の整数 x に対し $(x^{13})^{17}\equiv x$ が成り立つことを示せ。
$x^{21}\equiv x$ は用いてよい。

解答

$(x^{13})^{17}=x^{221}\equiv x^{20\times 11+1}$
$\equiv x^{20}\cdots x^{20}\underline{x^{20}x}\equiv x^{20}\cdots x^{20}\underline{x}\equiv\cdots\equiv x$

次の疑問を解決します。

⑴　何故，$x^{21}\equiv x$ が成り立つのか。
⑵　17 はどうやって見つけるのか。

§3. 逆元の存在

$(Z/pZ)^{\times}$ における逆元の存在を証明します。写像を使う方法は生徒にとって初めてかもしれません。鳩の巣原理と同じ感覚です。

問題 2　（**逆元の存在**）

自然数 b，$S=\{0,\ 1,\ \cdots,\ b-1\}$ とする。以下，mod b とする。b と互いに素な自然数 a に対し，次の方程式を考える。

$$\boxed{ax\equiv 1 \bmod b\ (x\in S)}\quad\cdots①$$

⑴　$a=7$，$b=9$ のとき①を解け。
⑵　x，$y\in S$，$ax\equiv ay$ のとき $x=y$ を示せ。
⑶　①の解がただ 1 つ存在することを示せ。

解答

⑴　$7x\equiv 1 \bmod 9\ (0\leqq x\leqq 8)$
　$7\cdot 4=28\equiv 1$ から $x=4$　他は不適。
⑵　$x\geqq y$ としてよい。$a(x-y)\equiv 0$ ゆえ $a(x-y)$ は b の倍数。a は b と互いに素ゆえ $x-y$ が b の倍数。$0\leqq x-y\leqq b-1$ より $x-y=0$
　よって $x=y$
⑶　$f:S\to S$ を $f(x)\equiv ax$ で定める。⑵より f は 1 対 1 ゆえ $f(x)\equiv 1$ を満たす x がただ 1 つ存在する。

§4. フェルマーの小定理

フェルマーの小定理を証明します。この証明は入試でよくみかけます。

問題 3　（**フェルマーの小定理**）

p：素数，a，b，n：整数とする。mod p で次が成り立つことを示せ。

(1) $1 \leqq k \leqq p-1$ のとき ${}_pC_k \equiv 0$

(2) $(a+b)^p \equiv a^p + b^p$

(3) $n^p \equiv n$ (4) $n \not\equiv 0$ のとき $n^{p-1} \equiv 1$

解答 (1) ${}_pC_k = \dfrac{p!}{k!(p-k)!}$ は自然数。分母の素因数はすべて p 未満ゆえ，p は約分されない。
よって ${}_pC_k$ は p の倍数。

(2) 二項定理より
$(a+b)^p = {}_pC_0 a^p + {}_pC_1 a^{p-1}b + \cdots + {}_pC_p b^p$
(1)より ${}_pC_1 \equiv {}_pC_2 \equiv \cdots \equiv {}_pC_{p-1} \equiv 0$

(3) (2)より
$n^p = (1+1+\cdots+1)^p \equiv 1^p + 1^p + \cdots + 1^p = n$

(4) $n \not\equiv 0$ のとき n，p は互いに素ゆえ $mn \equiv 1$ となる整数 m が存在する。
(3)の両辺に m を掛けて $mn^p = mnn^{p-1} \equiv n^{p-1} \equiv 1$

問題 4 2^{50} を 13 で割った余りを求めよ。

解答 フェルマーの小定理より mod13 で $2^{12} \equiv 1$
$2^{50} = (2^{12})^4 \cdot 2^2 \equiv 1^4 \cdot 4 = 4$

§5. 中国剰余定理とオイラー関数

$(Z/pqZ)^\times \cong (Z/pZ)^\times \times (Z/qZ)^\times$
$\phi(n) = \#(Z/nZ)^\times$

今回，RSA 暗号の原理の証明には使いませんが，証明の背景にあるので紹介します。どちらも入試で出題されます。

問題 5 （中国剰余定理）

(1) $x \equiv 2 \bmod 3$，$x \equiv 1 \bmod 5$ $(0 \leqq x \leqq 14)$ を満たす整数 x を求めよ。

(2) p，q：互いに素な自然数とする。
$S = \{0, 1, \cdots, pq-1\}$
$T = \{(a, b) | a = 0, 1, \cdots, p-1,\ b = 0, 1, \cdots, q-1\}$
とし，$f : S \to T$ を
$f(x) = (x$ を p で割った余り，x を q で割った余り$)$
で定める。$f(x) = f(y)$ のとき $x = y$ となることを示せ。

(3) $\boxed{x \equiv a \bmod p,\ x \equiv b \bmod q\ (0 \leqq x < pq)}$
を満たす整数 x がただ 1 つ存在することを示せ。

解答 (1) 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14
$x \equiv 2 \bmod 3$ の解は公差 3 の等差数列。
$x \equiv 1 \bmod 5$ の解は公差 5 の等差数列。
共通項は $x = 11$

(2) $x \geqq y$ としてよい。
$x \equiv y \bmod p$ ゆえ $x - y$ は p の倍数。
同様に q の倍数ゆえ $x - y$ は pq の倍数。
$0 \leqq x - y \leqq b - 1$ より $x - y = 0$ よって $x = y$

(3) S と T の要素の個数はどちらも pq
(2)より f は 1 対 1 ゆえ $f(x) = (a, b)$ を満たす x がただ 1 つ存在する。

問題 6 （オイラー関数）

自然数 n に対し $\phi(n)$ を $1 \sim n$ のうち n と互いに素な自然数の個数と定める。p，q は異なる 2 素数とする。次の値を求めよ。

(1) $\phi(15)$ (2) $\phi(pq)$ (3) $\phi(p^2q)$

解答 (1) $15 = 3 \times 5$ 1 から 15 までの全 15 個のうち 3 の倍数は 5 個，5 の倍数は 3 個あり，これらは 15 と互いに素。そのうち 15 の倍数 1 個は重複するから $\phi(15) = 15 - 5 - 3 + 1 = 8$

(2) (1)と同様に $\phi(pq) = pq - q - p + 1$
$= (p-1)(q-1)$

(3) $p(p-1)(q-1)$

§6. RSA 暗号の原理の証明

ようやく準備ができたので原理を証明します。

問題 7 （RSA 暗号の原理の証明）

異なる 2 素数 p，q に対し，$N = pq$，
$b = (p-1)(q-1)$ とする。e は b と互いに素な自然数，x は任意の整数とする。

(1) $ed = bk + 1$ を満たす非負整数 k と自然数 d が存在することを示せ。

(2) フェルマーの小定理を用いて
$x^{b+1} \equiv x \bmod N$ を示せ。

(3) $(x^e)^d \equiv 1 \bmod N$ を示せ。

解答

(1) e，b：互いに素ゆえ $ed \equiv 1 \bmod b$
$(0 \leqq d \leqq b-1)$ を満たす自然数 d が存在する。
つまり，ある整数 k が存在して $ed = bk + 1$
$ed \geqq 1$ より $k \geqq 0$

(2) $\bmod p$ でフェルマーの小定理より $x^p \equiv x$
$x^{b+1} = x^{(p-1)(q-1)+1} \equiv x^{p-1} \cdots x^{p-1} x \equiv \cdots \equiv x$
ゆえ $x^{b+1} - x$ は p の倍数。同様に q の倍数ゆえ pq の倍数。つまり $x^{b+1} - x \equiv 0 \bmod N$

(3) (1)，(2)より mod$N$ で
$(x^e)^d \equiv x^{bk+1} \equiv x^b \cdots x^b x \equiv \cdots \equiv x$

問題 8　$(N,\ e)=(3649,\ 3)$ とする。任意の整数 x に対し $(x^e)^d \equiv x \mod N$ となる自然数 d を 1 つ見つけよ。

解答　$3649=41\cdot89$ ゆえ $p=41$, $q=89$ として

$(p-1)(q-1)=3520$

$3\cdot2347=3520\cdot2+1$ より $d=2347$ とすればよい。

問題 9　$N=5621977$ を素因数分解せよ。

解答　1231×4567

RSA 暗号の安全性の根拠は素因数分解の非対称性（積は簡単，分解は難しい）です。

§7. おわりに

RSA 暗号の証明はよくみかけますが，$x^{\phi(N)}\equiv1$ で済ませているものが大半です。今回は $x\notin(Z/pZ)^\times$ の場合も含めて証明してみました。3 年生の演習等でご利用下さい。

《参考文献》

〔1〕 HP:http://www.maitou.gr.jp/rsa/rsa01.php　まいとう情報通信研究会
「サルにも分かる RSA 暗号」

〔2〕 伊藤正史『図解雑学　暗号理論』（ナツメ社）

（愛知県立旭丘高等学校）

コード表とべき乗表

字	x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}	x^{11}	x^{12}	x^{13}	x^{14}	x^{15}	x^{16}	x^{17}	x^{18}	x^{19}	x^{20}	x^{21}
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
A	2	4	8	16	32	31	29	25	17	1	2	4	8	16	32	31	29	25	17	1	2
B	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3
C	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4
D	5	25	26	31	23	16	14	4	20	1	5	25	26	31	23	16	14	4	20	1	5
E	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15	24	12	6
F	7	16	13	25	10	4	28	31	19	1	7	16	13	25	10	4	28	31	19	1	7
G	8	31	17	4	32	25	2	16	29	1	8	31	17	4	32	25	2	16	29	1	8
H	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9
I	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10
J	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11
K	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
L	13	4	19	16	10	31	7	25	28	1	13	4	19	16	10	31	7	25	28	1	13
M	14	31	5	4	23	25	20	16	26	1	14	31	5	4	23	25	20	16	26	1	14
N	15	27	9	3	12	15	27	9	3	12	15	27	9	3	12	15	27	9	3	12	15
O	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16
P	17	25	29	31	32	16	8	4	2	1	17	25	29	31	32	16	8	4	2	1	17
Q	18	27	24	3	21	15	6	9	30	12	18	27	24	3	21	15	6	9	30	12	18
R	19	31	28	4	10	25	13	16	7	1	19	31	28	4	10	25	13	16	7	1	19
S	20	4	14	16	23	31	26	25	5	1	20	4	14	16	23	31	26	25	5	1	20
T	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21
U	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22
V	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23
W	24	15	30	27	21	9	18	3	6	12	24	15	30	27	21	9	18	3	6	12	24
X	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25
Y	26	16	20	25	23	4	5	31	14	1	26	16	20	25	23	4	5	31	14	1	26
Z	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27
	28	25	7	31	10	16	19	4	13	1	28	25	7	31	10	16	19	4	13	1	28
	29	16	2	25	32	4	17	31	8	1	29	16	2	25	32	4	17	31	8	1	29
	30	9	6	15	21	3	24	27	18	12	30	9	6	15	21	3	24	27	18	12	30
	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31
	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32