数学アラカルト

第２回　公開鍵暗号の仕組み

§1　合同式

１つの正の整数 n を固定して考えます。２つの整数 a, b をそれぞれ n で割った余りが等しくなるとき、a と b は n を法（modulus）として合同であるといい、

$$a \equiv b \ (\mathrm{mod}\ \ n)$$

と書くことにします。これは、$a-b$ が n で割り切れることと同じです。

例　　$5 \equiv 3 \ (\mathrm{mod}\ \ 2)$,　　$10 \equiv 3 \ (\mathrm{mod}\ \ 7)$,　　$365 \equiv 5 \ (\mathrm{mod}\ \ 30)$

この合同の記号 ≡ は、等号の記号 ＝ と同じような性質を持っています。

$a \equiv b \ (\mathrm{mod}\ \ n)$,　$c \equiv d \ (\mathrm{mod}\ \ n)$ ならば

$a+c \equiv b+d \ (\mathrm{mod}\ \ n)$,　$ac \equiv bd \ (\mathrm{mod}\ \ n)$,　　$a^k \equiv b^k \ (\mathrm{mod}\ \ n)$　（k は自然数）

例　$10 \equiv 1 \ (\mathrm{mod}\ \ 9)$ より　$10^k \equiv 1 \ (\mathrm{mod}\ \ 9)$ であるから、

$$12345 \equiv 1+2+3+4+5 \equiv 15 \equiv 6 \ (\mathrm{mod}\ \ 9)$$

また、$10 \equiv -1 \ (\mathrm{mod}\ \ 11)$ より　$10^k \equiv (-1)^k \ (\mathrm{mod}\ \ 11)$ であるから

$$12345 \equiv 5-4+3-2+1 \equiv 3 \ (\mathrm{mod}\ \ 11)$$

今、5 を固定して考え、$a^k \ (\mathrm{mod}\ \ 5)$（$k=1, 2, 3, \cdots$）を調べてみよう。

$2^2 \equiv 4$,　　$2^3 \equiv 8 \equiv 3$,　　$2^4 \equiv 6 \equiv 1 \ (\mathrm{mod}\ \ 5)$

$3^2 \equiv 9 \equiv 4$,　　$3^3 \equiv 12 \equiv 2$,　　$3^4 \equiv 6 \equiv 1 \ (\mathrm{mod}\ \ 5)$

$4^2 \equiv 16 \equiv 1$,　　$4^3 \equiv 24 \equiv 4$,　　$4^4 \equiv 16 \equiv 1 \ (\mathrm{mod}\ \ 5)$

$5^2 \equiv 0 \ (\mathrm{mod}\ \ 5)$

$6^2 \equiv 1$,　　$6^4 \equiv 1 \ (\mathrm{mod}\ \ 5)$

$7^2 \equiv 2^2 \equiv 4$,　　$7^3 \equiv 8 \equiv 3$,　　$7^4 \equiv 6 \equiv 1 \ (\mathrm{mod}\ \ 5)$

一般に、a が 5 の倍数でないとき、$a^4 \equiv 1 \ (\mathrm{mod}\ \ 5)$　であることが分かります。このことを更に一般に主張するのが、有名なフェルマーの（小）定理です。

フェルマーの（小）定理　p を素数、a を p で割り切れない任意の整数とすると、

$$a^{p-1} \equiv 1 \ (\mathrm{mod}\ \ p)$$

この定理は次のように言い換えることができます。

p を素数、a を任意の整数とすると、$a^p \equiv a$（mod　p）

例　$a^3-a=a(a-1)(a+1)$　は 3 の倍数であり、また、偶数であるから 6 の倍数である。

例　$a^5-a=a(a^2-1)(a^2+1)=(a^3-a)(a^2+1)$より、$a^5-a$ は 5 の倍数であり、また 6 の倍数であるから 30 の倍数である。

例題 1. 次の式を満たす最小の正整数 x を求めよ.

$2^{2010}\times 3^{1867}\equiv x \pmod 5$

解答 フェルマーの定理より $2^{5-1}=2^4\equiv 3^4\equiv 1 \pmod 5$ だから

$$\begin{aligned}2^{2010}\times 3^{1867} &= 2^{4\times 502+2}\times 3^{4\times 466+3}\\ &= (2^4)^{502}\times 2^2\times (3^4)^{466}\times 3^3\\ &\equiv 1^{502}\times 4\times 1^{466}\times 27\equiv 3 \pmod 5\end{aligned}$$

$x=3$

問題 1. 次の式を満たす最小の正整数 x を求めよ.

(1) $5^{1001}\equiv x \pmod 3$　　(2) $7^{122}\equiv x \pmod 5$　　(3) $3^{2001}\equiv x \pmod 7$　　(4) $7^{14}\times 8^{25}\equiv x \pmod 5$

§2　オイラーの関数とオイラーの定理

次の算数の問題を考えよう：

30 個の分数　$\frac{1}{30}, \frac{2}{30}, \frac{3}{30}, \frac{4}{30}, \cdots\cdots, \frac{29}{30}, \frac{30}{30}$　のうち約分できない分数は何個ありますか。

また、それらの和はいくつでしょうか。　（土佐中学校入試問題）

この問題のように、自然数 n に対して n 個の分数　$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \frac{4}{n}, \cdots\cdots, \frac{n-1}{n}, \frac{n}{n}$　のうち約分できない分数（既約分数という）の個数を $\varphi(n)$ で表します。これをオイラーの関数といいます。$\varphi(n)$ は 1 から n までの自然数で、n と互いに素なものの個数と同じです。

例　$\varphi(1)=1$，$\varphi(2)=1$，$\varphi(3)=2$，$\varphi(4)=2$，$\varphi(5)=4$，$\varphi(6)=2$，$\varphi(7)=6$，$\varphi(8)=4$，$\varphi(9)=6$

オイラーの関数 $\varphi(n)$ に関しては、次の定理が知られています。

定理　(1)　$n=p$ が素数のとき、$\varphi(p)=p-1$

(2)　$n=p^k$ のとき、$\varphi(p^k)=p^k-p^{k-1}$

(3)　$n=ab$，$\gcd(a, b)=1$ のとき、$\varphi(ab)=\varphi(a)\,\varphi(b)$

上の算数の問題の前半の答は　$\varphi(30)=\varphi(2)\,\varphi(3)\,\varphi(5)=1\times 2\times 4=8$ です。

後半の答は　$\frac{k}{30}$ と $\frac{30-k}{30}$　が同時に既約分数になりますから、$\frac{1}{2}\varphi(30)=4$ です。

問題 2. 次の分数のうち約分できない分数はいくつありますか. また, それらの和はいくつですか.

(1) $\frac{1}{14}+\frac{2}{14}+\cdots+\frac{14}{14}$　(2) $\frac{1}{24}+\frac{2}{24}+\cdots+\frac{24}{24}$　(3) $\frac{1}{22}+\frac{2}{22}+\cdots+\frac{22}{22}$　(4) $\frac{1}{28}+\frac{2}{28}+\cdots+\frac{28}{28}$

§3　剰余類

さて、自然数 n に対して、整数を n で割ったときの余りの種類は 0，1，2，3，‥‥，$n-1$ の n 個あります。これらを、n を法とする剰余系、または、mod n の剰余系といい、$\boldsymbol{Z}_n$ で表します。これらの中で、n と互いに素であるものは全部で $\varphi(n)$ 個ありますが、それら全体を（mod n の）既約剰余系といい、$\boldsymbol{Z}_n^*$ で表します。

例　$\boldsymbol{Z}_2=\{0,\ 1\}$,　$\boldsymbol{Z}_2^*=\{1\}$,　$\boldsymbol{Z}_5=\{0,\ 1,\ 2,\ 3,\ 4\}$,　$\boldsymbol{Z}_5^*=\{1,\ 2,\ 3,\ 4\}$

$\boldsymbol{Z}_6=\{0,\ 1,\ 2,\ 3,\ 4,\ 5\}$,　$\boldsymbol{Z}_6^*=\{1,\ 5\}$

mod n の既約剰余系 $\boldsymbol{Z}_n^*$ に関しては、フェルマーの定理の一般化である次の定理が知られています。

オイラーの定理　$\gcd(a, n)=1$ ならば、$a^{\varphi(n)}\equiv 1\ (\mathrm{mod}\ \ n)$

例　$n=p$ が素数のとき、$\varphi(p)=p-1$ であるから、 $\gcd(a, p)=1$ のとき、 $a^{p-1}\equiv 1\ (\mathrm{mod}\ \ p)$

$n=10$ のとき、$\varphi(10)=4$，$\gcd(3,\ 10)=1$ であるから、　$3^4\equiv 1\ (\mathrm{mod}\ \ 10)$

$n=15$ のとき、$\varphi(15)=8$，$\gcd(2,\ 15)=1$ であるから、　$2^8\equiv 1\ (\mathrm{mod}\ \ 15)$

§4　「群」

現代数学の中心的概念に、「集合」と「構造」があります。個々のものよりもそれらが作る集合を考え、集合が満たす性質を構造と捉えます。集合の要素同士の結合という関係を扱うのが、代数的構造です。代数的構造としては、「群」、「環」、「体」があります。

群の定義

集合 G の任意の２つの要素 x，y に対して、それらの結合として G の要素（それを $x\circ y$ で表す）が定まり、次の（1）～（3）の性質を満たすとき G は群(group)であるという。

（1）　任意の要素 x, y, z に対して、結合法則　$(x\circ y)\circ z=x\circ(y\circ z)$　が成り立つ

（2）　要素 e（単位元という）があって、任意の要素 x に対して、$x\circ e=e\circ x=x$　が成り立つ

（3）　任意の要素 x に対して、$x\circ x^{-1}=x^{-1}\circ x=e$　を満たす要素（逆元という）x^{-1} が存在する

G の要素の数が有限個であるとき、G を有限群といい、G の要素の数を位数という。要素の数が有限個でないときは、無限群という。

$\boldsymbol{Z}_n$ の任意の要素 a, b に対して、$a+b\equiv c\ (\mathrm{mod}\ \ n)$ となる $\boldsymbol{Z}_n$ の要素 c があるので、このとき $a+b=c$　と書くことにすると、この演算（加法）に関して $\boldsymbol{Z}_n$ は群になる。

$\boldsymbol{Z}_n^*$の任意の要素 a, b に対して、$a \times b \equiv c \pmod{n}$ となる $\boldsymbol{Z}_n^*$の要素 c があるので、このとき　$a \times b = c$　と書くことにすると、この演算（乗法）に関して $\boldsymbol{Z}_n^*$は群になる。

$\boldsymbol{Z}_n^*$の要素の数（位数）は、$\phi(n)$（オイラーの関数）である。

例　$\boldsymbol{Z}_3 = \{0, 1, 2\}$、$\boldsymbol{Z}_3^* = \{1, 2\}$ の要素の間の演算の結果を表にすると次のようになる。

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	1	2
1	1	2
2	2	1

例　$\boldsymbol{Z}_4 = \{0, 1, 2, 3\}$、$\boldsymbol{Z}_4^* = \{1, 3\}$ の要素同士の演算の結果を表にすると次のようになる。

＋	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	1	3
1	1	3
3	3	1

問題 3. 次の剰余類, 既約剰余類の演算の結果の表を求めよ.
(1) $\boldsymbol{Z}_5 = \{0, 1, 2, 3, 4\}$　(2) $\boldsymbol{Z}_5^* = \{1, 2, 3, 4\}$　(3) $\boldsymbol{Z}_8^* = \{1, 3, 5, 7\}$　(4) $\boldsymbol{Z}_{12}^* = \{1, 5, 7, 11\}$

§5　暗号

現代(20 世紀後半～)の暗号は高度情報通信社会の情報セキュリティを支える技術の核である。

現代暗号の用途

1) 秘密のメッセージを伝える（守秘・伝達）
2) 相手の身元を確認する（認証）
3) プライバシーの保護
4) 情報の改ざん防止とその発見
5) 電子証明書、電子現金

暗号の２大方式

共通鍵暗号と公開鍵暗号

用語

- 暗号化する前の文を「平文（ひらぶん)」という。
- 暗号文から平文を得る作業を「復号」という。
- 正当でない人が、暗号文から平文を復元しようとする作業を「解読」という。
- ある値を知ることによって暗号化したり、また復号化できるとき、その値を「鍵」という

暗号と「純粋数学」

文字と数値との対応付けを「文字コード」と呼ぶ。

ASCII(American Standard Code for Information Interchange)

では、大小の英文字・数字・記号などの文字を 0～127 までの数値に対応させている。

現代暗号では、文字を ASCII コードなどにより数値に直した上で、暗号化する。このとき使われる「鍵」

は数値である。この鍵を秘密にできれば、暗号方式は他人に知られても構わない。鍵によって暗号文は変わるから、多くの人で同じ暗号方式が使える。

文字をn文字ずらすシーザー暗号において、鍵 n の種類は、英語では 26 個、日本語では 46 個程度であり、すべての可能性を試せば解読できてしまう。それに対して現代暗号の鍵の数は、何億・何兆以上あるようになっている。

現代暗号は数値から数値への変換であり、暗号は数式（関数）で表現される。

3 文字ずらすシーザー暗号は、$y=f(x)=x+3 \pmod{128}$ と表される。

群・環・体等の抽象代数学、整数論、楕円曲線論など、長い間実社会には役に立たないと考えられていた「純粋数学」の幅広い分野が、今日では、暗号と関わりを持ち社会に役立つようになってきた。

暗号の問題点

暗号に使う「鍵」を相手に秘密に伝えることが必要になる。

この問題を解決したのが、公開鍵暗号である。

§6 公開鍵暗号

鍵 A を公開して暗号文を送ってもらう。鍵 A では暗号文を平文に復元することはできない。

秘密にしてある鍵 B を用いると暗号文を平文に復元できる。1976 年 Diffie と Hellman はこのアイデア（公開鍵暗号）を思いついたが、その具体的な方法は分からなかった。

1977 年 MIT の Rivest、Shamir、Adelman の 3 人が公開鍵暗号のアイデアを実現する数学的手法を発明した。これが「RSA 暗号」である。

RSA 暗号（公開鍵暗号）の仕組み

p, q は2つの大きな素数

$N=pq$

$L=\mathrm{lcm}(p-1, q-1)$ ： $p-1$ と $q-1$ の最小公倍数(least common multiple)

$L=(p-1)s=(q-1)t$

a, n は任意の自然数

とすると、フェルマーの定理 $a^{p-1} \equiv 1 \pmod{p}$, $a^{q-1} \equiv 1 \pmod{q}$ より、

$$a^{nL+1} \equiv a(a^L)^n \equiv a(a^{p-1})^{sn} \equiv a \pmod{p}, \quad a^{nL+1} \equiv a(a^L)^n \equiv a(a^{q-1})^{tn} \equiv a \pmod{q}$$

よって、

$$a^{nL+1} \equiv a \pmod{N} \qquad \text{（RSA 暗号の基本定理）}$$

そこで、

$nL+1=ed$ を満たす自然数 e, d（$e<L, d<L$）をとる。$ed \equiv 1 \pmod{L}$ である。

N と e の値を公開する。e が公開鍵、d が秘密鍵である。

平文 a に対して $b \equiv a^e \pmod{N}$ という暗号文を作成する。

これを復元する鍵は d である。

$$b^d = (a^e)^d = a^{ed} = a^{nL+1} \equiv a \pmod{N}$$

RSA 暗号の例

実際に使われる素数 p, q は 512 ビットほど、つまり 10 進数では 155 桁位の大きなものですが、ここではその原理を理解するのが目的ですから、ずっと小さく、2 桁以下の素数とします。

1） $p=3, q=11$ のとき、

$N=pq=33$

$L=\mathrm{lcm}(p-1, q-1)=\mathrm{lcm}(2, 10)=10$

$nL+1=10n+1=ed$（$1<e<10, 1<d<10$）

$\varphi(L)=\varphi(10)=\varphi(2)\,\varphi(5)=4$, $\mathbf{Z}_{10}^{*}=\{1,\ 3,\ 7,\ 9\}$ であり、$ed=21$ となる。

$N=33$ と鍵 $e=3$ を公開する。$d=7$ は秘密鍵である。

平文 $a=5$ に対して暗号文 $b\equiv a^{e}\equiv 5^{3}\equiv 26$（mod 33）である。これを復元する。

$b^{d}\equiv 26^{7}\equiv 5\equiv a$（mod 33）となる。

平文 $a=7$ に対して暗号文 $b\equiv a^{e}\equiv 7^{3}\equiv 13$（mod 33）である。これを復元する。

$b^{d}\equiv 13^{7}\equiv 7\equiv a$（mod 33）となる。

2） $p=19,\ q=23$ のとき、

$N=p\,q=437$

$L=\mathrm{lcm}(p-1,\ q-1)=\mathrm{lcm}(18,\ 22)=198$

$nL+1=198n+1=ed$（$1<e<198,\ 1<d<198$）

である。$\varphi(L)=\varphi(198)=\varphi(2)\,\varphi(9)\,\varphi(11)=60$,

$\boldsymbol{Z}_{198}^{*}=\{1,\ 5,\ 7,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 35,\ 37,\ 41,\ 43,\ 47,\ 49,\ \cdots,\ 197\}$

である。

$e=5$ とすると、$198n-5d=-1$ であるから、この 1 次不定方程式を第 1 回の方法で解く。

$$\frac{198}{5}=39+\frac{3}{5}=39+\frac{1}{\frac{5}{3}}=39+\frac{1}{1+\frac{2}{3}}=39+\frac{1}{1+\frac{1}{\frac{3}{2}}}=39+\frac{1}{1+\frac{1}{1+\frac{1}{2}}}$$

であるから、

$$39+\frac{1}{1+\frac{1}{1}}=39+\frac{1}{2}=\frac{79}{2}=\frac{d_1}{n_1}$$

より、$n_1=2$, $d_1=79$とおく。このとき、$198n_1-5d_1=396-395=1$ よって、

$$198(n+n_1)-5(d+d_1)=0,\quad 198(n+2)=5(d+79)$$

これより、$n+2=5t$, $d+79=198t$ とおける。よって最小の正整数解は $n=3$, $d=119$ となる。

$N=437$ と鍵 $e=5$ を公開する。$d=119$ は秘密鍵である。

$e=7$ とすると、$198n-7d=-1$ で

$$\frac{198}{7}=28+\frac{2}{7}=28+\frac{1}{\frac{7}{2}}=28+\frac{1}{3+\frac{1}{2}}\qquad 28+\frac{1}{3}=\frac{85}{3}\qquad 198\cdot 3-7\cdot 85=-1$$

よって $d=85$ を得る。

問題 4. 素数 p, q および公開鍵 e が次の値のとき，秘密鍵 d の値を求めよ.

(1) $p=19,\ q=23,\ e=13$　　(2) $p=19,\ q=23,\ e=17$

(3) $p=23,\ q=29,\ e=3$　　(4) $p=23,\ q=29,\ e=5$

$N=437$, 公開鍵 $e=5$, 秘密鍵 $d=119$ のとき

平文 $a=100$ に対して

$100^2 = 10000 \equiv 386 \pmod{437}$, $100^4 \equiv 386^2 = 148996 \equiv 416 \pmod{437}$

$b \equiv a^e \equiv 100^5 \equiv 100^4 \cdot 100 \equiv 416 \cdot 100 \equiv 41600 \equiv 85 \pmod{437}$ である。

これを復元すると

$85^2 = 7225 \equiv 233 \pmod{437}$, $85^4 \equiv 233^2 = 54289 \equiv 101 \pmod{437}$

$85^8 \equiv 101^2 = 10201 \equiv 150 \pmod{437}$, $85^{16} \equiv 150^2 = 22500 \equiv 213 \pmod{437}$

$85^{32} \equiv 213^2 = 45369 \equiv 358 \pmod{437}$, $85^{64} \equiv 358^2 = 128164 \equiv 123 \pmod{437}$

$b^d = 85^{119} = 85^{64} \cdot 85^{32} \cdot 85^{16} \cdot 85^4 \cdot 85^2 \cdot 85$,

$85^{64} \cdot 85^{32} \cdot 85^{16} \equiv 123 \cdot 358 \cdot 213 = 44034 \cdot 213 \equiv 334 \cdot 213 = 71142 \equiv 348 \pmod{437}$

$85^4 \cdot 85^2 \cdot 85 \equiv 101 \cdot 233 \cdot 85 = 23533 \cdot 85 \equiv 372 \cdot 85 = 31620 \equiv 156 \pmod{437}$

$b^d \equiv 348 \cdot 156 = 54288 \equiv 100 = a \pmod{437}$ となる。

$N=437$, 公開鍵 $e=7$, 秘密鍵 $d=85$ のとき

平文 $a=100$ に対して(上の計算も使って)

$b \equiv a^e \equiv 100^7 \equiv 100^5 \cdot 100^2 \equiv 85 \cdot 386 \equiv 32810 \equiv 35 \pmod{437}$ である。

これを復元すると

$35^2 = 1225 \equiv 351 \pmod{437}$, $35^4 \equiv 351^2 = 123201 \equiv 404 \pmod{437}$

$35^8 \equiv 404^2 = 163216 \equiv 215 \pmod{437}$, $35^{16} \equiv 215^2 = 46225 \equiv 340 \pmod{437}$

$35^{32} \equiv 340^2 = 115600 \equiv 232 \pmod{437}$, $85^{64} \equiv 232^2 = 53824 \equiv 73 \pmod{437}$

$b^d = 35^{85} = 35^{64} \cdot 35^{16} \cdot 35^4 \cdot 35 \equiv 73 \cdot 340 \cdot 404 \cdot 35 = 24820 \cdot 14140$

$\equiv 348 \cdot 156 = 54288 \equiv 100 = a \pmod{437}$

となる。

問題 5. $N=187$($p=11$, $q=17$)のとき次の問に答えよ.

(1)公開鍵 $e=7$ のとき平文 $a=10$ を暗号化せよ.

(2)公開鍵 $e=9$ のとき平文 $a=10$ を暗号化せよ.

(3)公開鍵 $e=23$ のとき秘密鍵 d を求め, 暗号文 $b=20$ を複合化せよ.

第 2 回レポート問題

1. $\boldsymbol{Z}_{11}^*$ と $\boldsymbol{Z}_{24}^*$ の要素同士の乗法の結果を表にせよ。
2. ある人が暗証番号 a（3 桁の数）を公開数 $N=437$、公開鍵 $e=61$ で暗号化したら、$b=11$ を得た。この人の暗証番号 a を求めよ。