1　整数の演算

定理 1.1 (**剰余の定理**)
　正の整数 m と 整数 a に対して
　$a = mq + r$ かつ $0 \leq r < m$ を満たす整数の組 q, r がただひと組存在する。

定義 1.1 (**商と余り**)
　上記の q を a を m で割った商、 r を a を m で割った余りという。
a を m で割った余りを $a\,(Mod\ m)$ と表わす。

定義 1.2 (**約数、倍数**)　a が b の約数であるとは
　$b = ac$ を満たす整数 c が存在することである。
このとき、b は a の倍数であるという。
　またこのことを $a \mid b$ なる記号で表わす。

注意 1.1 $a \neq 0$ のとき，次は皆同値である。
(1)　a は b の約数。
(2)　b は a の倍数
(3)　$a \mid b$
(4)　$b = ac$ を満たす整数 c が存在する。
　　$(\mathbb{Z} \ni {}^{\exists}c\ s.t.\ b = ac)$
(5)　$\mathbb{Z} \ni \dfrac{b}{a}$

注意 1.2 $m \mid a \iff a\,(Mod\ m) = 0$

命題 1.2　次が成り立つ
(0)　$a \mid b \implies a \mid bc$
(1)　$a \mid b\ ,\ a \mid c \implies a \mid b + c$
(2)　$a \mid b\ ,\ a \mid c \implies a \mid b - c$

定義 1.3 (**公約数、公倍数、最大公約数、最小公倍数**)
(1)　a と b の双方の約数を a と b の公約数という。
(2)　a と b のどちらかが 0 でないとき a と b の公約数のうち最大なものが存在するが、それを a と b の最大公約数という。
(3)　a と b の双方の倍数を a と b の公倍数という。
(4)　a と b がともに 0 でないとき a と b の正の公倍数のうち最小なものが存在するが、それを a と b の最小公倍数という。

定義 1.4 (**互いに素**)
a と b の最大公約数が 1 つまり a と b の正の公約数が 1 しかないとき、a と b は互いに素であるという。

定義 1.5 (素数)
p が 2 以上の整数で p の約数が 1 と p しかないとき p は素数であるという。

注意 1.3　p が素数で a が p の倍数でないときは
a と p は互いに素である。

m が素数でないととすると、 $m = ab$, $2 \leq a \leq b$ をみたす整数 a, b が存在する。 このとき
$a = \sqrt{a^2} \leq \sqrt{ab} = \sqrt{m}$

注意 1.4　*(1)*　m が 2 以上の整数のとき、2 以上 $\sqrt{m}$ 以下の約数を持たない時 m は素数である。
(2)　m が 2 以上の整数のとき、2 以上 $\sqrt{m}$ 以下の素数で割り切れないとき、m は素数である。

2　$\mathbb{Z}$ のイデアル

I を a の倍数全体のなす集合とすると I は次の条件を満たす。

$$\begin{cases} I \ni x, y & \Longrightarrow \quad I \ni x+y, x-y \\ \mathbb{Z} \ni r, I \ni x & \Longrightarrow \quad I \ni rx \end{cases}$$

これを踏まえて $\mathbb{Z}$ のイデアルの定義を与えよう。

3　($\mathbb{Z}$ のイデアル)

定義 3.1 ($\mathbb{Z}$ **のイデアル**) $\mathbb{Z}$ の空でない集合 I が条件

$$\begin{cases} I \ni x, y & \Longrightarrow \quad I \ni x+y \\ \mathbb{Z} \ni r, I \ni x & \Longrightarrow \quad I \ni rx \end{cases}$$

を満たすとき I を $\mathbb{Z}$ のイデアルであるという。

注意 3.1　I が $\mathbb{Z}$ のイデアルのとき次が成り立つ。

$$\begin{cases} I \ni 0 \\ I \ni x & \Longrightarrow \quad I \ni -x \\ I \ni x, y & \Longrightarrow \quad I \ni x-y \end{cases}$$

注意の証明　(1)　I が空でないのでその中に何か元がある。a を I の要素とする。 $\mathbb{Z} \ni 0$ なので $I \ni 0a = 0$
(2)　$I \ni x$ とする。 $\mathbb{Z} \ni -1$ なので $I \ni (-1)x = -x$

(3)　$\mathrm{I} \ni x, y$ とする。$\mathrm{I} \ni x, -y$ なので $\mathrm{I} \ni x + (-y) = x - y$

定義 3.2 ($a\mathbb{Z}$)
a の倍数全体のなす集合は $\mathbb{Z}$ のイデアルであるが、これを $a\mathbb{Z}$ で表わす。

定理 3.1 ($\mathbb{Z}$ **のイデアルは単項イデアルである**)
　I を $\mathbb{Z}$ のイデアルとする。このとき
(0)　$I = \{0\}$ のとき $I = 0\mathbb{Z}$ である。
(1)　$I \neq \{0\}$ のとき I には正の整数が含まれるが、I に含まれる最小の正の数を n とおくと
　　$I = n\mathbb{Z}$ である。

定理の証明　(0) は自明。(1) を証明しよう。
$\mathrm{I} \neq \{0\}$ より I には 0 以外の要素がある。その一つを a とおくと I には $-a$ が入っている。
a と $-a$ のどちらかは正である。
よって、I には正の数が入っている。
n を I に含まれる最小の正の整数とすると
任意の整数 r に対して $\mathrm{I} \ni rn$
よって $\mathrm{I} \supset n\mathbb{Z}$
逆に $\mathrm{I} \ni x$ とする。
x を n で割った商を q 余りを r とすると
　$x = nq + r,\ 0 \leq r < n$
　$\mathrm{I} \ni x, n$ なので $\mathrm{I} \ni x - nq = r < n$
n が I に含まれる最小の正の整数なので $r = 0$
　$n\mathbb{Z} \ni nq = x$
よって $\mathrm{I} \subset n\mathbb{Z}$
以上より $\mathrm{I} = n\mathbb{Z}$

注意 3.2　$a\mathbb{Z} \ni a, -a$ であり $a\mathbb{Z} = (-a)\mathbb{Z}$ である。

定義 3.3 (**イデアルの和**)　I と J を $\mathbb{Z}$ のイデアルとするとき
　$\{z \mid I \ni x,\ J \ni y\ s.t.\ z = x + y\}$
は $\mathbb{Z}$ のイデアルになるが、これを $I + J$ で表わす。

I + J が $\mathbb{Z}$ **のイデアルになることの証明**
$\mathrm{I} \ni 0,\ \mathrm{J} \ni 0$ より $\mathrm{I} + \mathrm{J} \ni 0 + 0 = 0$
$\mathrm{I} + \mathrm{J} \ni x, y$ で $\mathbb{Z} \ni r$ とする
$\mathrm{I} + \mathrm{J} \ni x, y$ より $\mathrm{I} \ni {}^{\exists}x_1, y_1$, $\mathrm{J} \ni {}^{\exists}x_2, y_2$　s.t.　$x = x_1 + x_2,\ y = y_1 + y_2$

$\mathbb{Z} \ni r$ だったので $\mathrm{I} \ni x_1 + y_1,\ rx_1,\ \mathrm{J} \ni x_2 + y_2,\ rx_1$
よって $\mathrm{I}+\mathrm{J} \ni x_1 + y_1 + x_2 + y_2 = x + y,\ \mathrm{I}+\mathrm{J} \ni rx_1 + rx_2 = rx,$
故に $\mathrm{I}+\mathrm{J}$ は $\mathbb{Z}$ のイデアルになる。

命題 3.2　I, J を $\mathbb{Z}$ のイデアルとするとき
$I+J \supset I$ であり $I+J \supset J$ である。

証明　$\mathrm{I} \ni x$ とすると $\mathrm{J} \ni 0$ なので $\mathrm{I}+\mathrm{J} \ni x+0 = x$
よって $\mathrm{I}+\mathrm{J} \supset \mathrm{I}$ である。
$\mathrm{I}+\mathrm{J} \supset \mathrm{J}$ も同様に示せる。

命題 3.3　Iをイデアルとする。 このとき
(1)　$I \ni a$ のとき $I \supset a\mathbb{Z}$ である。
(2)　$I \ni a,b$ のとき $I \supset a\mathbb{Z}+b\mathbb{Z}$ である。

定理 3.4 ($\mathbb{Z}$ のイデアルの和)
a と b のどちらかが 0 でないとき d を a と b の最大公約数とすれば
$$a\mathbb{Z}+b\mathbb{Z} = d\mathbb{Z}$$
が成り立つ。

証明　$a\mathbb{Z}+b\mathbb{Z}$ は $\{0\}$ と異なる $\mathbb{Z}$ のイデアルなので、正の整数 c で $a\mathbb{Z}+b\mathbb{Z} = c\mathbb{Z}$ となるものがある。
ここで $c=d$ を示す。
$c\mathbb{Z} = a\mathbb{Z}+b\mathbb{Z} \ni a+0 = a$ なので c は a の約数である。
同様に c は b の約数である。
c は a と b の公約数なので $c \leq d$ である。
$a\mathbb{Z}+b\mathbb{Z} = c\mathbb{Z} \ni c$ なので $c = ax+by$ を満たす整数の組 x, y が存在する。
d はa と b の公約数なので d は c の約数になる。
c は正の数なので $c \geq d$
よって $c = d$ が示せた。

この定理の系として次のふたつの定理が成り立つ。 これらは有用な定理である。

一つはユークリッドの互除法である。

定理 3.5 (ユークリッドの互除法) $a = bq + r$ のとき
(1)　$a\mathbb{Z}+b\mathbb{Z} = b\mathbb{Z}+r\mathbb{Z}$
(2)　a と b の最大公約数は b と r の最大公約数に一致する

証明　(1) の証明
$a\mathbb{Z}+b\mathbb{Z} \ni b$ であり $a\mathbb{Z}+b\mathbb{Z} \ni a-bq=r$ なので $a\mathbb{Z}+b\mathbb{Z} \supset b\mathbb{Z}+r\mathbb{Z}$
$b\mathbb{Z}+r\mathbb{Z} \ni b$ であり $b\mathbb{Z}+r\mathbb{Z} \ni bq+r=a$ なので $a\mathbb{Z}+b\mathbb{Z} \subset b\mathbb{Z}+r\mathbb{Z}$
よって $a\mathbb{Z}+b\mathbb{Z} = b\mathbb{Z}+r\mathbb{Z}$
(2) は (1) より明らか

もう一つは 1 を作る定理である。

定理 3.6 (**1 を作る定理**)
　a と b が互いに素のとき a と b で *1* が作れる。
つまり、次が成り立つ。
　$ax+by=1$ を満たす整数の組 x, y が存在する。

この定理の直接の系として次の定理を得る。

定理 3.7 定理 (**互いに素と約数**)
a と b が互いに素で $a \mid bc$ ならば $a \mid c$ である。

証明　a と b が互いに素なので　$ax+by=1$ を満たす整数の組 x, y が存在する。
　よって $c=axc+bcy$ である。
　$a \mid bc$ なので $a \mid bcy$
　$a \mid acx$ であるので $a \mid axc+bcy$ つまり $a \mid c$ である。

特に p が素数で $p \nmid a$ のときは p と a は互いに素なので、次を得る。

定理 3.8 (**素数の性質**)
p が素数で $p \mid ab$ のとき $p \mid a$ 又は $p \mid b$ である。

定理 (**互いに素な数の積は互いに素**)　b 及び c が a と互いに素なとき
　　bc は a と互いに素である。

証明　p が a の約数である素数とすると
　b 及び c が a と互いに素なので $p \nmid b$ かつ $p \nmid c$ なので $p \nmid bc$
これは bc が a と互いに素を意味している。

また素数の性質の定理の系として次を得る。

定理 3.9 定理 (**素因数分解**)
　全ての自然数は素因数分解ができそれは一意的である。

4　合同式

定義 4.1 (**合同式**) $m \mid a-b$ のとき a と b は合同であるといい
$a \equiv b \pmod{m}$
と表わす。

注意 4.1 (**余りと合同**)　次が成り立つ。
(0)　$0 \leq a, b < m$ で $a \equiv b \pmod{m}$ のとき $a = b$ である。
(1)　$a \equiv b \pmod{m} \Longleftrightarrow$
「a を m で割った余り」＝「b を m で割った余り」
(2)　r を a を m で割った余りとするとき $(r = a \ (Mod\ m))$
$a \equiv r \pmod{m}$

合同式には次が成り立つ。

定理 4.1 (**合同式の性質**)　合同式には次が成り立つ
I　*(1)*　$a \equiv a \pmod{m}$
(2)　$a \equiv b \pmod{m} \Longrightarrow b \equiv a \pmod{m}$
(3)　$a \equiv b \pmod{m}$, $b \equiv c \pmod{m} \Longrightarrow a \equiv c \pmod{m}$
II　$a \equiv b \pmod{m}$ のとき
(1)　$a + c \equiv b + c \pmod{m}$
(2)　$a - c \equiv b - c \pmod{m}$
(3)　$ca \equiv cb \pmod{m}$
III　$a \equiv b \pmod{m}$ で $c \equiv d \pmod{m}$ のとき
(1)　$a + c \equiv b + d \pmod{m}$
(2)　$a - c \equiv b - d \pmod{m}$
(3)　$ac \equiv bd \pmod{m}$
IV　m と a が互いに素のとき
$ab \equiv ac \pmod{m} \Longrightarrow b \equiv c \pmod{m}$

定義 4.2 定義 (m **を法とした逆元**)
整数 a に対して
$ab \equiv 1 \pmod{m}$ を満たす整数 b が存在するとき
a は m を法として逆元をもつといい b を m を法とした a の逆元という。

注意 4.2 注意 (m **を法とした逆元**)
a は m を法として逆元をもつ $\Longleftrightarrow$ 方程式 $ax \equiv 1 \pmod{m}$ が解をもつ

定理 4.2 (m **を法とした逆元と互いに素**)
a が m を法として逆元を持つための必要十分条件は
a が m と互いに素であることである。

証明　a が m を法として逆元を持つとする。 b をその逆元とする。
　$ab \equiv 1 \,(mod\ m)$ が成り立つ
d を a と m の最大公約数とすると
d は ab と m の約数なので d は 1 の約数
d は 1 の正の約数なので $d = 1$
つまり a と m は互いに素である。
逆に a が m と互いに素とすると
　$ax + my = 1$ を満たす整数の組 x, y が存在する。
　$ax \equiv 1 \,(mod\ m)$
が成り立つので、 a は m を法としての逆元 x を持つ。

定義 4.3 定義 (オイラー関数)　$0, 1, 2, \cdots, m-1$ の内 m と互いに素な数の個数を m のオイラー数といい $\phi(m)$ で表わす。

オイラー数に関して次の定理が成り立つ。（証明は後で行う)

定理 4.3 (オイラー数)
(1)　p が素数のとき $\phi(p) = p - 1$
(2)　p が素数で $s \geq 1$ とき $\phi(p^s) = p^{s-1} \times (p-1)$
(3)　m と n が互いに素のとき $\phi(mn) = \phi(m)\phi(n)$

定理 4.4 (フェルマーの定理)　a が素数 p と互いに素な整数とするとき
　$a^{p-1} \equiv 1 \,(mod\ p)$

定理 4.5 (オイラーの定理)　a が自然数 m と互いに素な整数とするとき
　$a^{\phi(m)} \equiv 1 \,(mod\ m)$

5　剰余類環

定義 5.1 （剰余類環） $a + n\mathbb{Z}$ なるものを考え
$a \equiv b \,(mod\ n)$ の時のみ $a + n\mathbb{Z} = b + n\mathbb{Z}$ と約束する。
$\{x + n\mathbb{Z} \mid \mathbb{Z} \ni x\}$
なる集合を $\mathbb{Z}/n\mathbb{Z}$ で表わし $\mathbb{Z}$ の $n\mathbb{Z}$ による剰余類環という。

例 5.1　*(1)*　$\mathbb{Z}/2\mathbb{Z} = \{0 + 2\mathbb{Z},\ 1 + 2\mathbb{Z}\}$
(2)　$\mathbb{Z}/3\mathbb{Z} = \{0 + 3\mathbb{Z},\ 1 + 3\mathbb{Z},\ 2 + 3\mathbb{Z}\}$
(3)　$\mathbb{Z}/4\mathbb{Z} = \{0 + 4\mathbb{Z},\ 1 + 4\mathbb{Z},\ 2 + 4\mathbb{Z},\ 3 + 4\mathbb{Z}\}$
(4)　$\mathbb{Z}/5\mathbb{Z} = \{0 + 5\mathbb{Z},\ 1 + 5\mathbb{Z},\ 2 + 5\mathbb{Z},\ 3 + 5\mathbb{Z},\ 4 + 5\mathbb{Z}\}$
(5)　$\mathbb{Z}/6\mathbb{Z} = \{0 + 6\mathbb{Z},\ 1 + 6\mathbb{Z},\ 2 + 6\mathbb{Z},\ 3 + 6\mathbb{Z},\ 4 + 6\mathbb{Z},\ 5 + 6\mathbb{Z}\}$

注意 5.1 注意　$\mathbb{Z}/n\mathbb{Z}$ は n 個の元よりなる集合である。

定義 5.2 （和と積）$\mathbb{Z}/n\mathbb{Z}$ に和と積を次のように定義する。
(1)　$(a+n\mathbb{Z})+(b+n\mathbb{Z}) = (a+b)+n\mathbb{Z}$
(2)　$(a+n\mathbb{Z})(b+n\mathbb{Z}) = ab+n\mathbb{Z}$

定理 5.1 (剰余類環は可換環である)　$\mathbb{Z}/n\mathbb{Z}$ は可換環である
実際
(1)　$0+n\mathbb{Z}$ がゼロの役目をなす。
(2)　$(-a)+n\mathbb{Z}$ が $a+n\mathbb{Z}$ のマイナス $-(a+n\mathbb{Z})$ である
(3)　$1+n\mathbb{Z}$ がイチの役目をなす。

可換環において積に関する逆元を持つ元を単元というが、この言葉を使えば、次が成り立つ

定理 5.2 (単元)　$a+n\mathbb{Z}$ が単元であるための必要十分条件は a が n と互いに素であることである。

注意 5.2　$\mathbb{Z}/n\mathbb{Z}$ の単元の個数は $\phi(n)$ である。

次が成り立つ。

定理 5.3 (単元群)　可換環において単元全体の集合は群をなす。

定義 (群の位数と元の位数) G を有限群とし e をその単位元とする。
(1)　G の元の個数を G の位数という。
(2)　G の元 g に対して
　$g^s = e$ となる最小の正の数 s を g の位数という。

定理 5.4 (群の位数と元の位数) G を有限群とすると G の元の位数は G の位数の約数である。

この定理の一般の場合の証明は省略する。G が可換群のときの証明を与えておこう。

証明 G の位数を m として
$\mathrm{G} = \{g_1, g_2, \cdots, g_m\}$ とおく。g_1 は G の単位元 e としておく
h を G の元とすると
$hg_1, hg_2, \cdots, hg_m$ は全て G の元でありどのふたつも相異なる。つまりこれらは G の元を並び変えたものである。
よって

$h^m g_1 g_2 \cdots g_m = hg_1 hg_2 \cdots hg_m = g_1 g_2 \cdots g_m$
が成り立つ。(可換性を使った)
両辺に右から $(g_1 g_2 \cdots g_m)^{-1}$ をかけて
$h^m = e$
を得る。
s を h の位数とすると
$h^s = e$ であり
$0 < t < s$ なる整数 t では $h^t \neq e$ である。
m を s で割った商を q 余りを r とおくと
$m = sq + r,\ 0 \leq r < s$ である。
$h^s = e$ であり $h^m = e$ なので
$h^r = h^r (h^s)^q = h^{sq+r} = h^m = e$
$\leq r < s$ だったので $r = 0$ をえる。
つまり s は m の約数である。

この定理の直接の結果として次の定理が成り立つ。

定理 5.5 ($a + n\mathbb{Z}$ **の位数は** $\phi(n)$ **の約数である。**)
a と n が互いに素のとき
$a + n\mathbb{Z}$ の位数は $\phi(n)$ の約数である。

上の定理は合同式の言葉で述べれば次のようになる。

注意 5.3 a と n が互いに素のとき
(1) $a^{\phi(n)} \equiv 1 \ (mod\ n)$
(2) s を $a^s \equiv 1 \ (mod\ n)$ なる最小の正の整数とすれば
$s \mid \phi(n)$
である。

6 環準同型写像

$f : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ を
$\mathbb{Z} \ni^{\forall} x$ に対して $f(x) = x + n\mathbb{Z}$
と定めると f は次を満たしている。

$$\begin{cases} \mathbb{Z} \ni^{\forall} a, b \text{ に対して } f(a+b) = f(a) + f(b) \\ \mathbb{Z} \ni^{\forall} a, b \text{ に対して } f(ab) = f(a) f(b) \\ f(1) = 1 + n\mathbb{Z} \quad (1 + n\mathbb{Z} \text{ は } \mathbb{Z}/n\mathbb{Z} \text{ のイチ} \end{cases}$$

一般に、環 R から環 S への準同型写像の定義が次のように定義される。

定義 6.1 (**環準同型写像**) 、環 R から環 S への写像 f が次を満たすとき f は環準同型写像であるという。

$$\begin{cases} R\ni^{\forall} a,b \text{ に対して } f(a+b) = f(a)+f(b) \\ R\ni^{\forall} a,b \text{ に対して } f(ab) = f(a)f(b) \\ f(1_R) = 1_S \end{cases}$$

最初に述べた $f(x) = x+n\mathbb{Z}$ で定まる $\mathbb{Z}$ から $\mathbb{Z}/n\mathbb{Z}$ への写像 f は環準同型写像になっている。 この f は $\mathbb{Z}$ から $\mathbb{Z}/n\mathbb{Z}$ への自然な全射と呼ばれる (実際全射になっている)。

注意 6.1 (**全射、単射、全単射**)*(復習)*
写像 $f : X \longrightarrow Y$ に対して
(1) Y の任意の元 b に対して
X の元 s で $b = f(a)$ を満たすものが存在するとき
f は全射であるという。
全射のことを上への写像ともいう。
(2) a,b が X の異なる元とすれば、*(必ず)* $f(a)$ と $f(b)$ が異なるとき
f は単射であるという。
単射のことを一対一写像ともいう。
(3) f が全射であり単射であるとき、
f は全単射であるという。
全単射な写像を一対一対応ともいう。

注意 6.2 上の *(2)* は対偶を取って次と同値である。
(2)′ a,b が X の元で $f(a) = f(b)$ とすると $a = b$ である。 これが成り立つとき f は単射であるという。

定義 6.2 (**環の直和**) R と S を可換環とするとき
R と S の直積集合
$\{(a,b) \mid R\ni a,\ S\ni b\}$
に和と積を
$(a,b)+(c,d) = (a+c,b+d),\ (a,b)(c,d) = (ac,bd)$
で定めたものを R と S の直和といい
$R\oplus S$
で表わす。

命題 6.1 (**二つの可換環の直和は可換環になる**) R と S を可換環とするとき $R\oplus S$ は可換環であり
$0_{R\oplus S} = (0_R, 0_S)$

$1_{R\oplus S} = (1_R, 1_S)$
$R \oplus S \ni (a,b)$ のとき $-(a,b) = (-a,-b)$
である。

二つの環の直和の単元と、元の環の単元との間に密接な関係がある。

命題 6.2 (直和の単元) R と S を可換環とするとき
(a,b) が $R \oplus S$ の単元
$\Longleftrightarrow$ a は R の単元であり、b は S の単元である。

証明は演習に残そう。

上の命題より R の単元の個数と S の単元の個数が有限のとき
R⊕S の単元の個数 = R の単元の個数 × S の単元の個数
が成り立つことがわかる。

命題 6.3 (直和への写像)
$R,\ S,\ T$ が可換環であり
$f : R \longrightarrow S,\ f : R \longrightarrow T$ を環準同型写像とするとき
写像
$h : R \longrightarrow S \oplus T$
を、R の任意の元 x に対して
$h(x) = (f(x), g(x))$
で定めると、この写像は環準同型になる。

証明は演習に残そう。

$m,\ n$ を二つの自然数とするとき 環 $\mathbb{Z}/m\mathbb{Z}$ と 環 $\mathbb{Z}/n\mathbb{Z}$ ができる。従って、その直和の可換環
$\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$
ができる。
$\mathbb{Z}/m\mathbb{Z}\oplus\mathbb{Z}/n\mathbb{Z} = \{(x+m\mathbb{Z}, y+n\mathbb{Z}) \mid \mathbb{Z}/m\mathbb{Z} \ni x+m\mathbb{Z},\ \mathbb{Z}/n\mathbb{Z} \ni y+n\mathbb{Z}\}$
であり、和と積は
$$\begin{cases} (a+m\mathbb{Z}, b+n\mathbb{Z}) + (a'+m\mathbb{Z}, b'+n\mathbb{Z}) = ((a+a')+m\mathbb{Z}, (b+b')+m\mathbb{Z}) \\ (a+m\mathbb{Z}, b+n\mathbb{Z})(a'+m\mathbb{Z}, b'+n\mathbb{Z}) = (aa'+m\mathbb{Z}, bb'+m\mathbb{Z}) \end{cases}$$
で定まっていて
$0_{\mathbb{Z}/m\mathbb{Z}\oplus\mathbb{Z}/n\mathbb{Z}} = (0+m\mathbb{Z}, 0+n\mathbb{Z})$
$1_{\mathbb{Z}/m\mathbb{Z}\oplus\mathbb{Z}/n\mathbb{Z}} = (0+m\mathbb{Z}, 0+n\mathbb{Z})$
であるような、 mn 個の元よりなる環となる。

m と n を二つの整数とする。

$\mathbb{Z}\, a, b$ で $a + mn\mathbb{Z} = b + mn\mathbb{Z}$ とすると
$mn \mid a - b$
なので
$m \mid a - b$
つまり
$a + m\mathbb{Z} = b + m\mathbb{Z}$
がなりたつ。 このことは
$\mathbb{Z}/mn\mathbb{Z}$ から $\mathbb{Z}/m\mathbb{Z}$ への写像で
$\mathbb{Z}/mn\mathbb{Z}$ の任意の元 $x + mn\mathbb{Z}$ を $x + m\mathbb{Z}$ に移すものが
存在することを保証している。
この写像を $\mathbb{Z}/mn\mathbb{Z}$ から $\mathbb{Z}/m\mathbb{Z}$ への標準全射という
(実際全射になっている。)

命題 6.4 $\mathbb{Z}/mn\mathbb{Z}$ から $\mathbb{Z}/m\mathbb{Z}$ への標準全射は環準同型写像である。

$\mathbb{Z}/mn\mathbb{Z}$ から $\mathbb{Z}/n\mathbb{Z}$ への標準全射も存在し、それは環準同型になっている。
従って
$\mathbb{Z}/mn\mathbb{Z}$ から $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ への環準同型写像で
$\mathbb{Z}/mn\mathbb{Z}$ の任意の元 $x + mn\mathbb{Z}$ を $(x + m\mathbb{Z}, x + n\mathbb{Z}$ に移すものが存在する。
これも $\mathbb{Z}/mn\mathbb{Z}$ から $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ への標準写像という。
自然な準同型写像ともいう。

一般的にはこの標準写像は全射にはならない。しかし m と n が互いに素のときには、全射になる (実は全単射になる) ことをこれから示していく。

一般論のを準備を用意しよう。

定義 6.3 定義 (核、Kernel) $f : R \longrightarrow S$ を環準同型写像とするとき
$\{x \in R \mid f(x) = 0_S$
を f の核またはカーネル *(Kernel)* といい $Ker\, f$ で表わす。

命題 6.5 (単射と核) $f : R \longrightarrow S$ を環準同型写像とするとき、次は同値である。
(1) f は単射。
(2) $Ker\, f = \{0_R\}$
(3) $R \ni a$ で $f(a) = 0_S$ ならば $a = 0_R$

証明 証明にはいる前に $f(0_R) = 0_S$ を見ておく。
f が環準同型なので
$f(0_R) + f(0_R) = f(0_R + 0_R) = f(0_R)$

両辺に $-f(0_R)$ を加えて

$$f(0_R) = 0_S$$

を得る。このことは $\mathrm{Ker}\, f \supset \{0_R\}$ が成り立つことを意味している。
証明に入ろう。
(3) の主張は $\mathrm{Ker}\, f \subset \{0_R\}$ と同じでいつも $\mathrm{Ker}\, f \supset \{0_R\}$ だったので、(2) と (3) は同値である。
(1) $\Longrightarrow$ (3)

$R \ni a$ で $f(a) = 0_S$ とすると

$f(a) = 0_S = f(0_R)$

f は単射なので $a = 0_R$ である。
(3) $\Longrightarrow$ (1)

$R \ni a, b$ で $f(a) = f(b)$ とすると

$R \ni a - b$ で $f(a - b) = f(a) - f(b) = 0_S$

よって $a - b = 0_R$ となり $a = b$ を得る。
よって f は単射である。

定理 6.6 m, n を互いに素な二つの自然数とするとき

$\mathbb{Z}/mn\mathbb{Z}$ から $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ への自然な準同型写像は全単射である。
(全単射な準同型写像を同型写像という)

この定理は中国人の剰余定理を剰余類環の言葉で述べたものである。

証明 $\mathbb{Z}/mn\mathbb{Z}$ から $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ への自然な準同型写像を φ と表わすと、φ は $\mathbb{Z}/mn\mathbb{Z} \ni a + mn\mathbb{Z}$ に対して

$$\varphi(a + mn\mathbb{Z}) = (a + m\mathbb{Z}, a + n\mathbb{Z})$$

である。
いま

$$\varphi(a + mn\mathbb{Z}) = 0_{\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}}$$

とすると

$$0_{\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}} = (0 + m\mathbb{Z}, 0 + n\mathbb{Z})$$

なので $a + m\mathbb{Z} = 0 + m\mathbb{Z}$, $a + n\mathbb{Z} = 0 + n\mathbb{Z}$
つまり

$$m \mid a \text{ かつ } n \mid a$$

を得る。
m, n が互いに素だったので

$$mn \mid a$$

を得るが、これは

$$a + mn\mathbb{Z} = 0 + mn\mathbb{Z}$$

を意味している。
よって φ は単射である。

$\mathbb{Z}/mn\mathbb{Z}$ は mn 個の元よりなり、$\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ も同じ mn 個の元よりなっている。
φ は mn 個の元よりなる集合から mn 個の元よりなる集合への単射なので自動的に全射になる。よって φ は全単射である。

同型写像と単元については次が成り立つ。

命題 6.7 (同型写像と単元) $f : R \longrightarrow S$ を全単射な環準同型写像とすると次が成り立つ。
(1) a を R の単元とすると $f(a)$ は R の単元である
(2) b を S の単元とすると R の単元 a で
$$b = f(a)$$
を満たすものが存在する。

証明 (1) a を R の単元とすると a^{-1} が R の中にある。
$$f(a)f(a^{-1}) = f(aa^{-1}) = f(1_{\mathrm{R}}) = 1_{\mathrm{S}}$$
なので $f(a)$ は S の単元であり, $f(a^{-1}) = f(a)^{-1}$ である。
(2) b を S の単元とすると S の中に b^{-1} がある。
f は全射なので R の元 a, c で
$$b = f(a),\ b^{-1} = f(c)$$
を満たすものがある。
$$f(ac) = f(a)f(c) = bb^{-1} = 1_{\mathrm{S}}$$
$$f(1_{\mathrm{R}}) = 1_{\mathrm{S}}$$
であり、f は単射なので
$$ac = 1_{\mathrm{R}}$$
をえる。
よって a は単元である。
また $b = f(a)$ であった。

注意 6.3 注意 (同型写像と単元の数) 上の定理は可換環 R から 可換環 S への同型写像があるとき
R の単元群から S の単元群への全単射があることを示している。
したがってこのときは、R の単元の個数と S の単元の個数は同じである。

定理 6.8 定理 (オイラー数) オイラー数に関しては次が成り立つ
(1) p を素数とするとき
$$\phi(p) = p - 1$$
(2) p を素数とし t を自然数とするとき
$$\phi(p^t) = p^{t-1}(p-1)$$

(3) m と n を互いに素な二つの自然数とするとき

$$\phi(mn) = \phi(m)\phi(n)$$

証明 n を自然数としたとき $0 \sim n-1$ のうち n と互いに素なものの個数を n のオイラー数といい $\phi(n)$ で表わした。(復習)
(1) p を素数としたとき、$0 \sim p-1$ の中で p と互いに素でないのは 0 の一個のみである。よって

$$\phi(p) = p-1$$

(2) p を素数としたとき、$0 \sim p^t-1$ の中で p と互いに素でないのは p の倍数である数のみである。その個数は p^{t-1} 個、よって

$$\phi(p^t) = p^t - p^{t-1} = p^{t-1}(p-1)$$

(3) m と n を互いに素なので
$\mathbb{Z}/mn\mathbb{Z}$ から $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ への自然な準同型写像は全単射である。
よって双方の単元の個数は同じ。
$\phi(mn)$ は $\mathbb{Z}/mn\mathbb{Z}$ の単元の個数、
$\phi(m)\phi(n)$ は $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ の単元の個数である。
従って

$$\phi(mn) = \phi(m)\phi(n)$$

系 6.9 系 $n = p_1^{t_1}p_2^{t_2}\cdots p_s^{t_s}$
を n の素因数分解とすると

$$\phi(n) = p_1^{t_1-1}(p_1-1)p_2^{t_2-1}(p_2-1)\cdots p_s^{t_s-1}(p_1-1)$$

である。

これの証明は定理の (3) を何度か使いあと (2) を使えば良い。

例題 6.1 次を求めよ
(1) $\phi(17)$
(2) $\phi(15)$
(3) $\phi(1000)$

解答 (1) 17 は素数なので $\phi(17) = 17-1 = 16$
(2) $\phi(15) = \phi(3\times 5) = \phi(3)\phi(5) = 2\times 4 = 8$
(3) $\phi(1000) = \phi(2^3\times 5^3) = 2^2(2-1)5^2(5-1) = 400$

問 6.1 次を求めよ
(1) $\phi(31)$

(2) $\phi(60)$

(3)　$\phi(400)$

例題 6.2　2010^{2010} を 17 で割った余りを求めよ。

解答　$2010^{2010} + 17\mathbb{Z}$ を計算する。
2010 を 17 で割った余りは 4 なので
$$2010 + 17\mathbb{Z} = 4 + 17\mathbb{Z}$$
である。
$(4 + 17\mathbb{Z})^2 = 16 + 17\mathbb{Z} = -1 + 17\mathbb{Z}$
$(4 + 17\mathbb{Z})^4 = ((4 + 17\mathbb{Z})^2)^2 = (-1 + 17\mathbb{Z})^2 = 1 + 17\mathbb{Z}$
$2010 = 4 \times 502 + 2$ なので
$2010^{2010} + 17\mathbb{Z} = (2010 + 17\mathbb{Z})^{2010} = (4 + 17\mathbb{Z})^{4\times502+2}$
$= ((4 + 17\mathbb{Z})^4)^{502}(4 + 17\mathbb{Z})^2 = 16 + 17\mathbb{Z}$
答えは 16 である。

7　循環小数の話

7.1　有理数と循環小数

ここでは数は正の数に限ろう。
整数は小数点以下が全て 0 と小数展開ができる。
$\frac{7}{25} = 0.28$ と有限小数で表わされる。
$\frac{1}{6} = 0.16666666\cdots$ と無限小数であるが、或部分から循環する小数 (循環小数で表わされる。もちろん整数は小数第 1 位から 0 が循環していると思ってもよいし、 0.28 は整数は小数第 1 位から 0 が循環していると思ってもよい。その意味では整数も有限小数も広い意味での循環小数と思ってもよい。

次の命題が成り立つ。

命題 7.1 $(\frac{n}{m})$　m, n が自然数で
$0 < n < m$ で m, n が互いに素とする。このとき次の三つの場合に分けて次が成り立つ。
(1)　m を割る素数はあっても 2 や 5 しかないとき
$\frac{n}{m}$ は有限小数である。
(2)　m は偶数でも 5 の倍数でもないとき
(m と 10 が互いに素のとき)

$\frac{n}{m}$ は小数第１位から循環する循環小数である。

(3) m は偶数または *5* の倍数で *2* 及び *5* 以外の素数で割り切れるとき $\frac{n}{m}$ は循環小数だが、小数第１位からは循環しない。

この命題は今すぐは証明しない。

次が成り立つ。

定理 7.2 定理 (有理数と循環小数) 正の実数 a において

a が有理数 $\Longleftrightarrow$ a は広い意味での循環小数である。

この定理も直ちには証明はしない。

循環小数について調べていこう。

7.2 小数展開

定義 7.1 (級数) 数列 $\{x_n\}_{n=1,2,3,\cdots}$ に対して

$$x_1 + x_2 + \cdots + x_n + \cdots$$

を級数といい

$\lim_{n\to\infty} x_1 + x_2 + \cdots + x_n$ が存在するとき

$$x_1 + x_2 + \cdots + x_n + \cdots$$

は収束するといい、

$x_1 + x_2 + \cdots + x_n + \cdots$ で $\lim_{n\to\infty} x_1 + x_2 + \cdots + x_n$ を表わす。

$\lim_{n\to\infty} x_1 + x_2 + \cdots + x_n$ が存在しないとき

$$x_1 + x_2 + \cdots + x_n + \cdots$$

は発散するという。

定義 7.2 (十進小数) ゼロ以上の整数 a と $0 \sim 9$ からなる数列 $\{a_n\}_{n=1,2,3,\cdots}$ に対して

$$a + \frac{a_1}{10} + \frac{a_2}{10^2} + \frac{a_3}{10^3} + \cdots + \frac{a_n}{10^n} + \cdots$$

は収束するがそれを $a.a_1a_2\cdots a_n\cdots$ で表わす。

定義 7.3 (循環小数) 小数 $q = a.a_1a_2\cdots a_n\cdots$ に対して

$$a_{s+1} = a_{s+m+1} = a_{s+2m+1} = a_{s+3m+1} = \cdots$$

$$a_{s+2} = a_{s+m+2} = a_{s+2m+2} = a_{s+3m+2} = \cdots$$

$$\vdots$$

$$a_{s+m} = a_{s+2m} = a_{s+3m} = a_{s+4m} = \cdots$$

が成り立つとき、この小数 q を

$$a.a_1a_2\cdots a_s\dot{a}_{s+1}a_{s+2}\cdots\dot{a}_{s+m}$$

で表わす。

このような、q を循環小数といい

循環小数 q に対して、このような s と m を最小に選んだとき

m を循環小数 q の循環の長さといい、$a_{s+1}a_{s+2}\cdots a_{s+m}$ を循環の節という。

例 7.1 *(1)* $0.0\dot{6}$ は長さが *1* で節が *6* の循環小数

(2) $0.\dot{0}60\dot{6}$ これは $0.0\dot{6}$ なので長さが *2* 節が 06 の循環小数

(3) $0.62\dot{5}\dot{2}$ これは $0.62\dot{5}$ なので長さが *2* 節が 25 の循環小数

例 7.2 *(1)* $0.\dot{0}0\dot{1} = \dfrac{1}{1000} + \dfrac{1}{1000^2} + \dfrac{1}{1000^3} + \cdots = \dfrac{1}{1000}(1 + \dfrac{1}{1000} + \dfrac{1}{1000^2} + \cdots)$

$= \dfrac{1}{1000}\dfrac{1}{1 - \dfrac{1}{1000}} = \dfrac{1}{999}$

(2) $0.\dot{3}5\dot{7} = 357 \times 0.\dot{0}0\dot{1} = \dfrac{357}{999}$

注意 7.1 *(1)* 長さが m で節が $00\cdots01$ の循環小数 $0.\dot{0}0\cdots0\dot{1}$ は $\dfrac{1}{10^m - 1}$

つまり $\dfrac{1}{99\cdots9}$ である *(*$99\cdots9$ は 9 が m 個並んでいる*)*

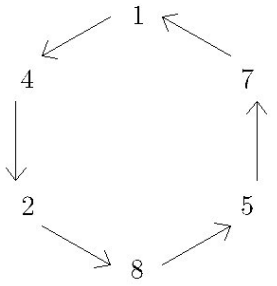
(2) 長さが m で節が $a_1a_2\cdots a_m$ の循環小数 $0.\dot{a_1}a_2\cdots\dot{a_m}$ は $\dfrac{a_1a_2\cdots a_m}{99\cdots9}$

である *(*分子の $a_1a_2\cdots a_m$ は十進数とみて $99\cdots9$ は 9 が m 個並んだものである*)*

7.3 循環小数の観察

$\dfrac{1}{7} \sim \dfrac{6}{7}$ を小数展開をしよう

$10\times1 = 7\times1+3$
$10\times3 = 7\times4+2$
$10\times2 = 7\times2+6$
$10\times6 = 7\times8+4$
$10\times4 = 7\times5+5$
$10\times5 = 7\times7+1$
$10\times1 = 7\times1+3$
$10\times3 = 7\times4+2$
$10\times2 = 7\times2+6$
$10\times6 = 7\times8+4$
$10\times4 = 7\times5+5$
$10\times5 = 7\times7+1$
$\vdots$



$10^6 = 7\times142857+1$

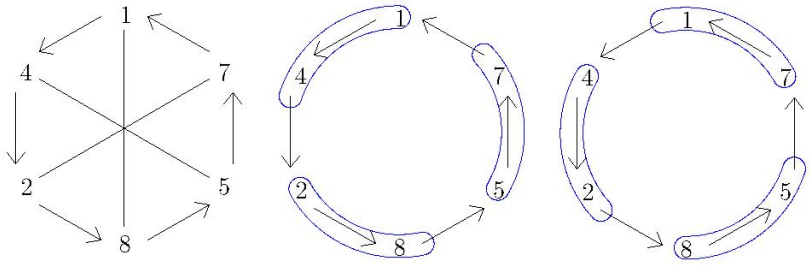
つまり $\dfrac{1}{7} = \dfrac{142857}{999999} = 0.\dot{1}42857\dot{}$

$10^6\times3 = 7\times428571+3$

つまり $\dfrac{3}{7} = \dfrac{428571}{999999} = 0.\dot{4}28571\dot{}$

同様に $\frac{2}{7} = 0.\dot{2}85714\dot{}$, $\frac{6}{7} = 0.\dot{8}57142\dot{}$, $\frac{4}{7} = 0.\dot{5}71428\dot{}$, $\frac{5}{7} = 0.\dot{7}14285\dot{}$

次を観察しよう



次の表は 19 までの m についての $\frac{1}{m}$ の循環の表である。

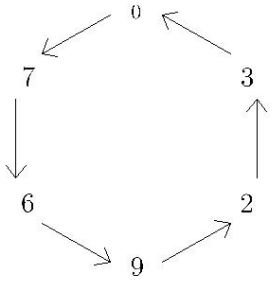
表 1

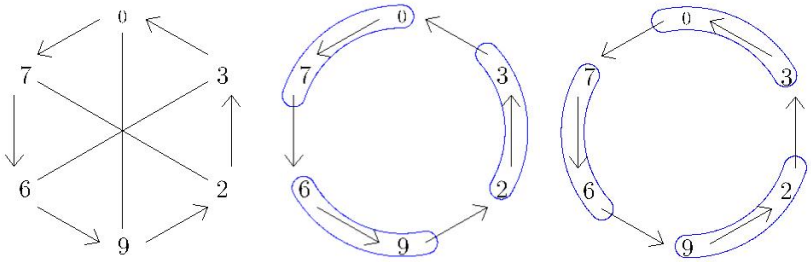
		長さ	節			長さ	節
$\frac{1}{2}$	0.5			$\frac{1}{3}$	$0.\dot{3}$	1	3
$\frac{1}{4}$	0.25			$\frac{1}{5}$	0.2		
$\frac{1}{6}$	$0.1\dot{6}$	1	6	$\frac{1}{7}$	$0.\dot{1}42857\dot{}$	6	142857
$\frac{1}{8}$	0.125			$\frac{1}{9}$	$0.\dot{1}$	1	1
$\frac{1}{10}$	0.1			$\frac{1}{11}$	$0.\dot{0}\dot{9}$	2	09
$\frac{1}{12}$	$0.08\dot{3}$	1	3	$\frac{1}{13}$	$0.\dot{0}76923\dot{}$	6	076923
$\frac{1}{14}$	$0.07\dot{1}42857\dot{}$	6	142857	$\frac{1}{15}$	$0.0\dot{6}$	1	6
$\frac{1}{16}$	0.0625		0	$\frac{1}{17}$	$0.\dot{0}588235294117647\dot{}$	16	0588235294117647
$\frac{1}{18}$	$0.0\dot{5}$	1	5	$\frac{1}{19}$	$0.\dot{0}52631578947368421\dot{}$	18	052631578947368421

注意 7.2　上の表において $\frac{1}{m}$ の小数展開において m が偶数であったり、5 の倍数であったりしたときとそうでないときに差異がみられるが、いつでもそうかな？

次に分母が 13 の分数の小数展開を観察しよう

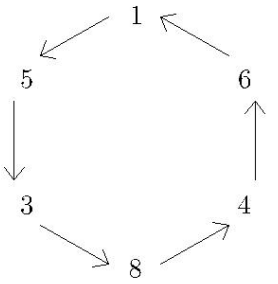
$$
\begin{aligned}
10\times 1 &= 13\times 0+10\\
10\times 10 &= 13\times 7+9\\
10\times 9 &= 13\times 6+12\\
10\times 12 &= 13\times 9+3\\
10\times 3 &= 13\times 2+4\\
10\times 4 &= 13\times 3+1
\end{aligned}
$$

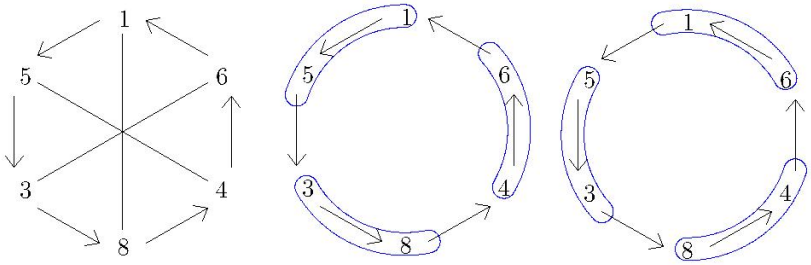




$$\frac{1}{13}=\dot{0}76923\dot{}\quad \frac{10}{13}=\dot{7}6923\dot{0}\quad \frac{9}{13}=\dot{6}9230\dot{7}$$
$$\frac{12}{13}=\dot{9}2307\dot{6}\quad \frac{3}{13}=\dot{2}3076\dot{9}\quad \frac{4}{13}=\dot{3}0769\dot{2}$$

$$
\begin{aligned}
10\times 2 &= 13\times 1+7\\
10\times 7 &= 13\times 5+5\\
10\times 5 &= 13\times 3+11\\
10\times 11 &= 13\times 8+6\\
10\times 6 &= 13\times 4+8\\
10\times 8 &= 13\times 6+2
\end{aligned}
$$

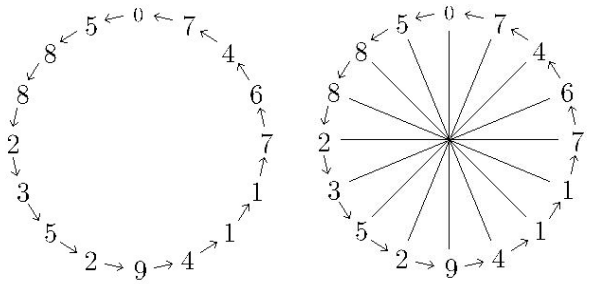




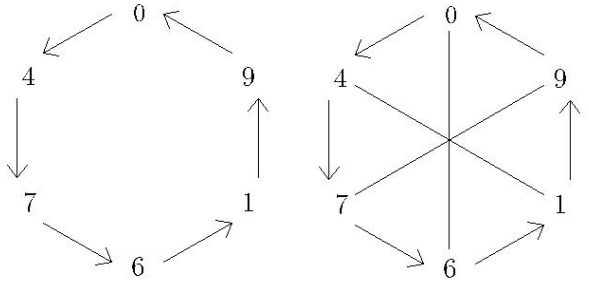
$$\frac{2}{13}=\dot{1}5384\dot{6}\quad \frac{7}{13}=\dot{5}3846\dot{1}\quad \frac{5}{13}=\dot{3}8461\dot{5}$$
$$\frac{11}{13}=\dot{8}4615\dot{3}\quad \frac{6}{13}=\dot{4}6153\dot{8}\quad \frac{8}{13}=\dot{6}1538\dot{4}$$

$$\frac{1}{17}=0.\dot{0}588235294117647\dot{}$$

これは循環の長さが 16 で 循環の節が 0588235294117647 の循環小数である。

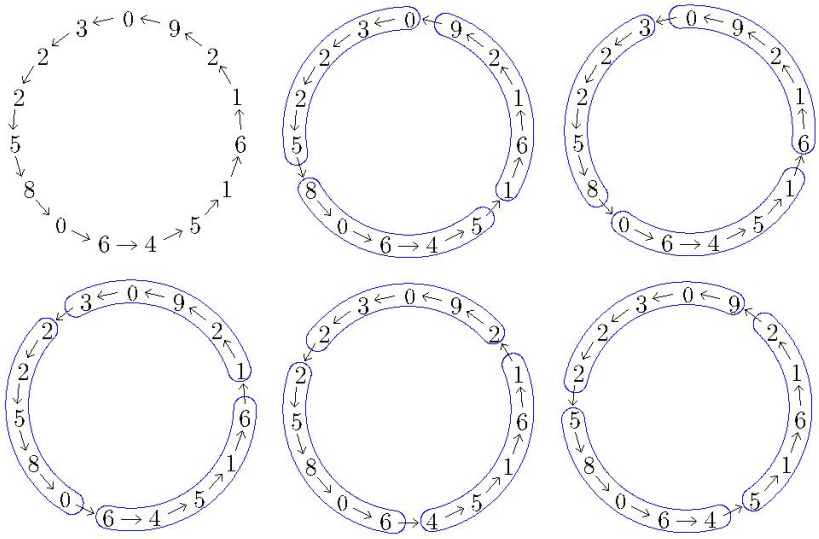


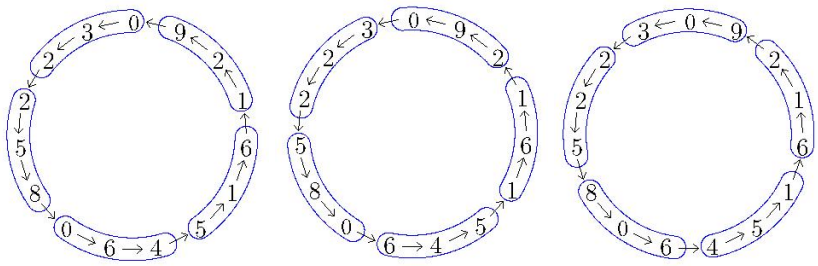
$\frac{1}{21} = 0.\dot{0}47619\dot{0}$ は循環の長さが 6 で循環の節が 047619 の循環小数である



今までの図と共通点と相違点がありますね。

$\frac{1}{31}$ は循環の長さが 15 で循環の節が 032258064516129 である。　次を観察しよう





次の表は、$\frac{1}{m}$ が循環小数になるときの循環小数の循環の長さと m のオイラー数との関係を示す表です。
(オイラー数の定義は後でします)

m	$\phi(m)$	長さ	m	$\phi(m)$	長さ	m	$\phi(m)$	長さ	m	$\phi(m)$	長さ
3	2	1	7	6	6	11	10	2	13	12	6
17	16	16	19	18	18	21	12	6	23	22	22
29	28	28	31	30	15	33	20	2	37	36	3
39	24	6	41	40	5	43	42	21	47	46	46
49	42	42	51	32	16	53	52	13	57	36	18

注意 7.3　オイラー数と循環の長さとの関係が見えますか？

一般的に次が成り立つ。

命題 7.3 (循環の長さとオイラー数)　m, n を $0 < n < m$ で m と n は互いに素、m と 10 が互いに素とするとき、次が成り立つ。
(1)　$\frac{n}{m}$ は小数第 1 位から循環する。
(2)　$\frac{n}{m}$ の循環の長さは $10 + m\mathbb{Z}$ の位数に等しい。
　従って、それは m のオイラー数 $\phi(m)$ の約数である。
(3)　$10 + m\mathbb{Z}$ の位数を k とするとき $\frac{n}{m}$ の循環の節は、$\frac{n(10^k - 1)}{m}$ を k 桁の 10 進数とみたものである。

証明　$\frac{n}{m}$ が小数第 s 位より循環していてその長さが t だとする。
このとき、$\frac{10^{s-1}n}{m}$ は小数第 1 位から循環しその長さは t である。
　$10^{s-1}n$ を m で割った余りを r_0 とおく。
10 も n も m と互いに素なので $10^{s-1}n$ も m と互いに素である。
よって r_0 も m と互いに素で $0 < r_0 < m$ である。
　$\frac{10^{s-1}n}{m}$ を小数展開したものの小数部分は $\frac{r_0}{m}$ を小数展開したものである。
　$\frac{r_0}{m}$ の循環の節を $q'_1q'_2q'_3\cdots q'_t$ とし、これを 10 進数とみると

$$\frac{r_0}{m} = \frac{q'_1q'_2q'_3\cdots q'_t}{\underbrace{99\cdots9}_{t\text{個}}} = \frac{q'_1q'_2q'_3\cdots q'_t}{10^t-1}$$

が成り立っている。

故に

$$r_0\times(10^t-1) = m\times q'_1q'_2q'_3\cdots q'_t$$

が成り立っている。

これより m は $r_0\times(10^t-1)$ の約数であることが分かるが、r_0 は m と互いに素だったので m は 10^t-1 の約数であることが分かる。

よって

$$(10+mF)^t = 1+mF$$

となる。

k を $10+m\mathbb{Z}$ の位数とおくと k は t の約数である。

特に $k\leq t$ である。

$$(10+mF)^k = 1+mF$$

より 10^k-1 は m の倍数であり、従って $n(10^k-1)$ も m の倍数である。

よって $n(10^k-1)m$ は整数である。

$0<\frac{n}{m}<1$ だったので $0<\frac{n(10^k-1)}{m}<10^k-1$

$\frac{n(10^k-1)}{m}$ は高々 k 桁の自然数である。これを 10 進数 $q_1q_2q_3\cdots q_k$ と表わすと

$$\frac{n}{m} = \frac{q_1q_2q_3\cdots q_k}{10^k-1}$$

これは $\frac{n}{m}$ が小数第 1 位から長さが k で循環していることをいみする。

循環の長さの定義より $t\leq k$ であるが、$k\leq t$ だったので

$$t = k$$

である。以上より

$\frac{n}{m}$ は小数第 1 位から循環しその循環の長さが $10+m\mathbb{Z}$ の位数に等しいことがわかった。

また、循環の節は $q_1q_2q_3\cdots q_k$ であり、これは $\frac{n(10^k-1)}{m}$ を 10 進数でみたものである。

定理 7.4 定理 p 5 をより大きな素数とし a を $0<a<p$ なる自然数とする。$\frac{a}{p}$ の循環の長さを k 循環の節を $q_1q_2q_3\cdots q_k$ とする。

m, n を自然数で m が 2 以上で $k=mn$ を満たすものとする。

m 個の 10 進数

$$q_1q_2\cdots q_n,$$
$$q_{n+1}q_{n+2}\cdots q_{2n},$$
$$q_{2n+1}q_{2n+2}\cdots q_{3n},$$

$\vdots$,

$q_{(m-1)n+1}q_{(m-2)n+2}\cdots q_{mn}$

を各々 $x_1, x_2, \cdots, x_m$ とするとき

$x_1 + x_2 + \cdots + x_m$ は $10^n - 1$ の倍数である。

理解を深めるため例から始めよう。

$p = 13, a = 1$ とすると

$$\frac{1}{13} = 0.\dot{0}76923\dot{}$$

であり、循環の長さが 6 で循環の節は 076923 である。

$m = 3, n = 2$ とみると

$$07 + 69 + 23 = 99$$

確かになっている。

一般論にも適用できる方法でこれを見てみよう。

下のの右側の計算では $p = 13, r_0 = a = 1$ として、商と余りの計算である。

$$\begin{array}{rcl|rcl} 10\times 1 &=& 13\times 0+10 & 10\times r_0 &=& p\times q_1+r_1\\ 10\times 10 &=& 13\times 7+9 & 10\times r_1 &=& p\times q_2+r_2\\ 10\times 9 &=& 13\times 6+12 & 10\times r_2 &=& p\times q_3+r_3\\ 10\times 12 &=& 13\times 9+3 & 10\times r_3 &=& p\times q_4+r_4\\ 10\times 3 &=& 13\times 2+4 & 10\times r_4 &=& p\times q_5+r_5\\ 10\times 4 &=& 13\times 3+1 & 10\times r_5 &=& p\times q_6+r_6\\ & & & (r_6 &=& r_0) \end{array}$$

これを少し加工すると

$$\begin{array}{rcl|rcl} 10\times 10\times 1 &=& 13\times 10\times 0+10\times 10 & 10\times 10\times r_0 &=& p\times 10\times q_1+10\times r_1\\ 10\times 10 &=& 13\times 7+9 & 10\times r_1 &=& p\times q_2+r_2\\ 10\times 10\times 9 &=& 13\times 10\times 6+10\times 12 & 10\times 10\times r_2 &=& p\times 10\times q_3+10\times r_3\\ 10\times 12 &=& 13\times 9+3 & 10\times r_3 &=& p\times q_4+r_4\\ 10\times 10\times 3 &=& 13\times 10\times 2+10\times 4 & 10\times 10\times r_4 &=& p\times 10\times q_5+10\times r_5\\ 10\times 4 &=& 13\times 3+1 & 10\times r_5 &=& p\times q_6+r_0 \end{array}$$

10 進数 q_1q_2, q_3q_4, q_5q_6 は各々 $10\times q_1+q_2, 10\times q_3+q_4, 10\times q_5+q_6$ を表わしているが、これらを各々 x_1, x_2, x_3 であらわすと、上記の式をふたつづつを一つの式にまとめると

$$\begin{array}{rcl|rcl} 10^2\times 1 &=& 13\times 07+9 & 10^2\times r_0 &=& p\times x_1+r_2\\ 10^2\times 9 &=& 13\times 69+3 & 10^2\times r_2 &=& p\times x_2+r_4\\ 10^2\times 3 &=& 13\times 23+1 & 10^2\times r_4 &=& p\times x_3+r_0 \end{array}$$

となる。 これらを足し合わせて変形して、次を得る。

$$(10^2-1)(1+9+3) = 13\times(07+69+23) \mid (10^2-1)(r_0+r_2+r_4) = p(x_1+x_2+x_3)$$

この右側の式を解釈する。

いま $p = 13$ の場合 $10 + p\mathbb{Z}$ の位数は 6 なので

$$(10 + p\mathbb{Z})^2 \neq 1 + p\mathbb{Z}$$

つまり $10^2 - 1$ は p で割り切れない。 p は素数だったので、$10^2 - 1$ と p

は互いに素である。
よって $x_1+x_2+x_3$ は 10^2-1 の倍数である。

上の右側の方法で定理を証明しよう。

定理の証明 $\frac{a}{p}$ の循環の長さが k なので $10+p\mathbb{Z}$ の位数は k である。
$2 \leq m$ なので $0 < n < mn = k$
従って $(10+p\mathbb{Z})^n \neq 1+p\mathbb{Z}$、
つまり 10^n-1 は p で割り切れない。
p は素数だったので p と 10^n-1 は互いに素である。
$\frac{a}{p}$ の循環の節 $q_1q_2q_3\cdots q_{mn}$ を n 桁づつ m 個に区切った、m 個の 10 進数を順に $x_1, x_2, \cdots, x_m$ とおく
$s_0 = a$ とおいて $s_1, s_2, \cdots, s_m$ を順に次のように定める。

$$s_i = 10^n s_{i-1} Mod p \quad i = 1, 2, \cdots m$$

つまり、$10^n s_{i-1}$ を p で割った余り s_i とする。
このとき

$10^n a$ を p で割った商が x_1 で余りが s_1
$10^n s_1$ を p で割った商が x_2 で余りが s_2
$10^n s_2$ を p で割った商が x_3 で余りが s_3
$\vdots$
$10^n s_{m-1}$ を p で割った商が x_m で余りが s_m

となっている。作り方より $s_m = a = s_0$ となるのは明らかである。
以上のことを式で表わすと

$$\begin{aligned} 10^n s_0 &= px_1 + s_1 \\ 10^n s_1 &= px_2 + s_2 \\ 10^n s_2 &= px_3 + s_3 \\ &\vdots \\ 10^n s_{m-1} &= px_m + s_m \\ & (s_m = s_0) \end{aligned}$$

これを全て足し合わせて変形して

$$(10^n-1)(s_1+s_2+\cdots+s_m) = p(x_1+x_2+\cdots+x_m)$$

をえる。
10^n-1 と p は互いに素だったので
$x_1+x_2+\cdots+x_m$ が 10^n-1 の倍数であることが分かる。

この定理の系として次の定理を得る。

定理 7.5 定理 p 5 をより大きな素数とし a を $0 < a < p$ なる自然数とする。$\frac{a}{p}$ の循環の長さが偶数 $2n$ 循環の節を $q_1q_2q_3\cdots q_{2n}$ とする。

このとき $1 \leq i \leq n$ なる全ての i に対して

$$q_i + q_{n+i} = 9$$

が成り立つ。

証明　前定理より $q_1q_2q_3\cdots q_n + q_{n+1}q_{n+2}q_{n+3}\cdots q_{2n}$ は $\underbrace{99\cdots9}_{n\text{個}}$ の倍数である。

一方 $q_1q_2q_3\cdots q_n$ 及び $q_{n+1}q_{n+2}q_{n+3}\cdots q_{2n}$ は共に 0 以上で $\underbrace{99\cdots9}_{n\text{個}}$ 以下の整数であるが、

共に 0 に等しいことはなく、共に $\underbrace{99\cdots9}_{n\text{個}}$ 等しいことはない。

このことより

$$q_1q_2q_3\cdots q_n + q_{n+1}q_{n+2}q_{n+3}\cdots q_{2n} = \underbrace{99\cdots9}_{n\text{個}}$$

このことより、求める結果を得る。

分母が素数の場合をみたが、分母が素数でない場合はどうであろうか？
次の表は分母が１０と互いに素でな数 m 分子が 1 の分数を小数表示したときの循環の長さ k と循環の節を表わしたものである。ただし $21 \leq m \leq 59$ である。

m	k	
21	6	047619
23	22	0434782608695652173913
27	3	037
29	28	0344827586206896551724137931
31	16	0322580645161290
33	2	03
37	3	027
39	6	025641
41	5	02439
43	21	023255813953488372093
47	46	0212765957446808382978723404⋯
49	42?	020408164265306122448979591836735⋯
51	16	0196078431372549
53	26	01886792452830188679245283
57	18	017543859649122807
59	58?	

8　素数と RSA 暗号システム

8.1　エラトステネスの篩

　次の素数を見つける方法はエラトステネスの篩 (ふるい) と呼ばれる方法である。

100 迄の素数を全て求めよう。

1	◯2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

1 から 100 までの数の表を作る。
先ず 1 は消す。
その次の 2 に ◯ をつける。
その後の 2 の倍数を全て消す。

1	◯2	◯3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

◯ の次に最初に残っている数に
◯ をつける。
その後のその数の倍数を全て消す。

ここでは 3 に ◯ をつける。
その後の 3 の倍数を全て消す。

1	◯2	◯3	4	◯5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

◯ の次に最初に残っている数に
◯ をつける。
その後のその数の倍数を全て消す。

ここでは 5 に ◯ をつける。
その後の 5 の倍数を全て消す。

1	②	③	4	⑤	6	⑦	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

◯ の次に最初に残っている数に
◯ をつける。
その後のその数の倍数を全て消す。

ここでは 7 に ◯ をつける。
その後の 7 の倍数を全て消す。

ここまでの操作で 10 までの数は全て ◯ がついたか消されている。
100 までの数で消されていないもの (◯ のついたものも含めて) が
100 までの数の中の素数の全てである。

実際
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97
がその全てである

このやり方で素数が求められることは次の命題が保証している。

命題　n を 2 以上の整数とする。このとき
　n が素数 $\Longleftrightarrow$ n は $\sqrt{n}$ までの素数で割り切れない
が成り立つ。

10000 まで素数を全て求めるには、10000 までの数の表を作り、上記と同じ操作を 100 迄の数で行えばよい。

また p が素数であることを示すためには、p が 2 以上 $\sqrt{p}$ までの整数で割り切れないことを示せばよい。
この方法だと数が 100 倍近く大きくなれば、難しさは 10 倍近くになる。

8.2　素因数分解と RSA 暗号システム (記事から)

　特定の大きな数が素数か否かを判定する、あるいは素因数分解するという問題はその数が大きいときはかなり困難な問題である。この問題に起因する話題を紹介しよう。
先ずいくつかの記事から出発しよう。

2007 年 05 月 25 日 13:07

スイスのローザンヌにあるローザンヌ連邦工科大学（EPFL）の教授で、暗号技術が専門のアルジェン・レンストラ氏は、700 ビットの RSA 暗号キーを破るのと同等の難問を解いたことを明らかにした。

レンストラ氏は、11 カ月にわたる分散コンピューティング・プロジェクトの末に、この難問を解くことに成功した。同氏はこの結果について、「電子商取引などで広く使われている 1,024 ビットの RSA 暗号技術が、コンピュータと数学的手法の進歩に伴い、いずれ有効性を失うことを示している」と語る。

RSA 暗号化アルゴリズムは、公開鍵と秘密鍵のシステムを使ってメッセージの暗号化と復号を行っている。公開鍵は、きわめて大きな 2 つの素数を掛けることで算出される。素数とは、2、3、5、7 など、その数自体と 1 以外では割り切れない数のことだ。

公開鍵の作成に使われた 2 つの素数を特定できれば、秘密鍵を計算してメッセージを復号することができる。しかし、きわめて大きな整数の基になっている 2 つの素数を特定するのは、膨大な数のコンピュータを使って長時間演算を行わないかぎり、ほとんど不可能だ。

レンストラ氏らは今回、EPFL やボン大学などにある 300〜400 台の市販コンピュータを使い、307 ケタの整数を因数分解して 2 つの素数を算出することに成功した。因数分解とは、整数を素数の積にすることであり、例えば 12 を因数分解すると 2 × 2 × 3 になる。

レンストラ氏は、他の数に比べ因数分解が容易になるような特性を持つ 307 ケタの数を慎重に選択した。今回使われたのは、2 の 1,039 乗から 1 を引いた数だった。

しかしそれでも、素数を計算するために作成した専用の数式を複数のコンピュータで処理するのに 11 カ月を要したという。

こうした作業の果てに、ようやく 307 ケタの数から作られた暗号鍵を割り出して、メッセージを読むことができたわけだが、RSA 暗号化アルゴリズムを使用するシステムは、異なる鍵をそれぞれのユーザーに割り当てており、これらの鍵を破るには、素数の算出作業を繰り返さなければならない。

レンストラ氏によると、現在使われている RSA の 1,024 ビット公開鍵から素数成分を算出できるようになるのは 5〜10 年先だという。公開鍵は通常、およそ 150 ケタの素数を 2 つ掛け合わせることで生成されており、今回のプロジェクトで使用された 307 ケタの整数よりも因数分解が難しいからだ。

レンストラ氏の次のターゲットは 768 ビットの公開鍵だ。「いずれは 1,024 ビットの公開鍵にも挑戦したい」と同氏は語っている。

(ジェレミー・カーク／ IDG News Service ロンドン支局)

ローザンヌ連邦工科大学（スイス）

http://www.epfl.ch/
提供：Computerworld.jp
http://sourceforge.jp/magazine/07/05/25/0412211

いくつかの言葉が出てきました。
700 ビット、1024 ビット
RSA 暗号技術
公開鍵と秘密鍵 メッセージの暗号化と復号
きわめて大きな 2 つの素数を掛ける
因数分解

別の記事を紹介しよう。

PRESS RELEASE
2010 年 1 月 18 日
富士通株式会社
株式会社富士通研究所
独立行政法人情報通信研究機構

楕円曲線暗号と RSA 暗号の強度比較基準を策定
インターネット通信などを安全に利用するための基準作りに成功
富士通株式会社（代表取締役社長：間塚道義）および株式会社富士通研究所（代表取締役社長：村野和雄）は、インターネット通信などの新暗号技術である楕円曲線暗号（注 1）について、現在標準的に用いられている RSA 暗号（注 2）との精密な強度比較基準を策定することに成功しました。今回の成果により、楕円曲線暗号が従来よりも数千倍程度相対的に高い強度であると考えられることが分かりました。今後は、得られた強度比較基準に基づき、最適な暗号システムを構築することで、インターネット通信などをより安全かつ便利に使用していただくことが可能になります。

⋮
中略
⋮

注 2 RSA 暗号：1978 年に公表された公開鍵暗号および電子署名方式で、Rivest、Shamir、Adleman の 3 人の開発者の名前の頭文字から RSA の名がついた。公開鍵暗号・電子署名方式として、現在最も広く使われている。鍵と同程度の大きさの合成数の素因数分解問題が解ければ、RSA 暗号も解読される。

⋮

略

⋮

この記事により、次のことが分かります。
RSA 暗号システムは現在標準的に使われていること。
素因数分解の難しさがこのシステムの命綱であること。

素因数分解については少し古い記事ですが、ここに紹介しておこう。

RSA-576 素因数分解コンテストで数学者のグループが解答を出す
米 RSA Laboratories は 27 日、同社が実施した素因数分解コンテスト「RSA-576」を世界各地の数学者が協力して解読することに成功したことを正式に認め、研究者グループに 1 万ドルの賞金を授与したと発表した。この素因数分解に成功したことは 2003 年 12 月 3 日に RSA に報告されていた。

RSA-576 とは、2 進法で 576 桁（10 進法で 174 桁）の数を素因数分解するコンテスト。RSA 暗号は、「小さい数を掛け合わせて大きな数にすることは一瞬で計算できるが、大きな数を素因数分解するには、どんな高速なコンピュータを使用しても多大な時間がかかる」という法則に基づいて設計されている暗号だ。そのため、素因数分解に関する研究は、公開鍵暗号の解読に関する研究ということもできる。RSA がこの素因数分解コンテストを行なうのは、世界中の優秀な頭脳にこの問題に取り組んでもらい、RSA 暗号の限界を確かめ続けることで結果的に同社の暗号の安全性を高めるためだ。

RSA-576 で出題された数字は、

188198812920607963838697239461650439807163563379417382700763356422988859715234665485319060606504743045317388011303396716199692321205734031879550656996221305168759307650257059

であり、これを素因数分解した結果は、

3980750864240649373971255005503864911990643623425 2
6708406385189575946388957261768583317
×
4727721461074353025362230719730482246329146953020 9
7116459852171130520711256363590397527

だった。

今回コンテストに挑戦して素因数分解に成功したのは、ドイツの Scientific Computing Institute と Pure Mathematics Institute、オランダの National Research Institute for Mathematics and Computer Science およびその他複数の組織である。ドイツにある Experimental Mathematics Institute と Bundesamt fur Sicherheit in der Informationstechnologie（BSI）も解読に使用するハードウェアを提供したほか、米国、カナダ、英国の数体ふるい法ネットワーク所属の数学者たちも参加している。

なお、現在インターネットや携帯電話で使用される代表的な暗号鍵の大きさは最低でも 1024bit（10 進法で 310 桁）であるため、今回 576bit（10 進法で 174 桁）の暗号が解読されたとしても実質的な影響はない。

RSA では継続的にコンテストを行なっている。次のコンテストは 640bit を素因数分解するコンテストである RSA-640 で、2 万ドルの賞金がかかっている。ちなみに最高賞金がかかっているコンテストは RSA-2048（10 進法で 617 桁）であり、この素因数分解に成功すれば 20 万ドルの賞金が授与される。

http://internet.watch.impress.co.jp/cda/news/2004/04/28/2970.html

この記事から、１０進数で ３１０桁の数の素因数分解は一般に難しいことが分かりますね。

もう一つ、素因数分解の記事を紹介します。

NTT などが世界記録となる 1017 ビットの合成値の素因数分解に成功，RSA 暗号の安全性確認で

NTT は 2007 年 5 月 21 日，公開鍵暗号の安全性の根拠となる素因数分解の難しさに関する検証実験として，特殊合成数の従来の世界記録である 911 ビットを上回る 1017 ビットの合成数に対する素因数分解を達成したことを明らかにした。NTT，ドイツのボン大学，スイスのスイス連邦工科大学ローザンヌ校（EPFL）の 3 者による共同実験。ボン大の PC クラスタを数時間動かすことで素因数分解を完了した。

素因数分解の対象は「a の b 乗プラスマイナス 1」という特殊な形の合成数であり，この型に有効に働く素因数分解アルゴリズムである特殊数体ふるい法を用いた。実際に用いた合成数は「$(2^{1039}-1)/5080711$」であり，因数分解の対象は 1017 ビットになる。このビット数は，一般的な合成値に一般数体ふるい法を適用した場合で言うと，約 700 ビットの難しさに相当する。

一般に，公開鍵暗号の鍵長を長くすればするほど安全になるが，どの程度の長さがあれば事実上安全になるかを推測する手段として，今回のような素因数分解の実験が実施されている。コンピュータの計算処理能力と素因数分解技術の進化によって，安全性を確保するための鍵長が伸びることになる。なお，SSL などで用いられている RSA 暗号の鍵長の主流は，現在 1024 ビット。

「$(2^{1039}-1)/5080711$」を，以下に示す 80 桁と 227 桁のペアに素因数分解した。

80 桁の数値：

55853666619936291260749204658315944968646527018488637648010052346319853288374753

227 桁の数値：

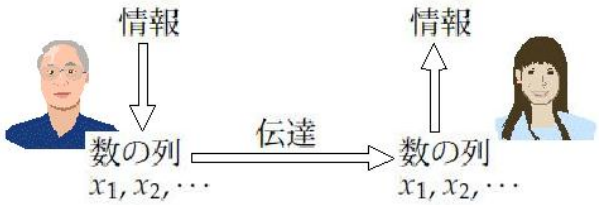
20758181946442382764570481370359469516293970800739520988120838703792729090324679382343143884144834882534053344769112223028158327696525376091410189105241993899334109711624358962065972167481161749004803659735573409253205425523689

http://itpro.nikkeibp.co.jp/article/NEWS/20070521/271718/

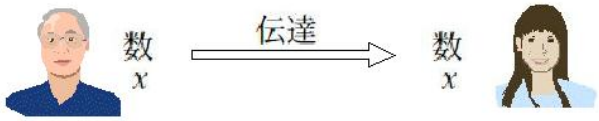
8.3 RSA 暗号システム

ここで RSA 暗号システムの仕組みについて簡単に紹介しておく。
このシステムは RSA 公開鍵暗号システムとも呼ばれている。
先ず暗号についての説明から入ろう。
一口にいうと暗号システムとは
情報伝達を秘密に行うシステムである。
下図は情報の直接伝達である。

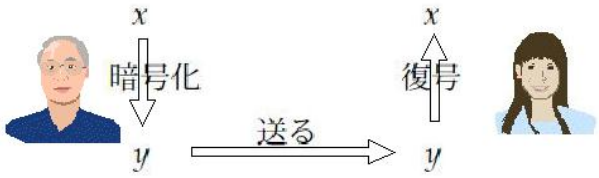
普通デジタル伝達で情報を数の列に変えて送り、それを元の情報に戻し、情報を送る。



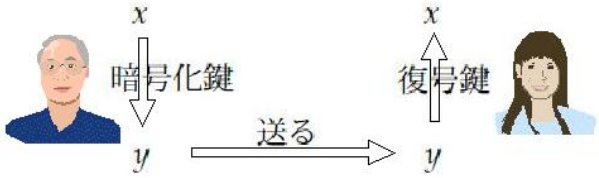
ここでの数の列と情報は誰にでも簡単に互いに変換できるものである。
情報伝達はつまるところ、数の伝達になる。



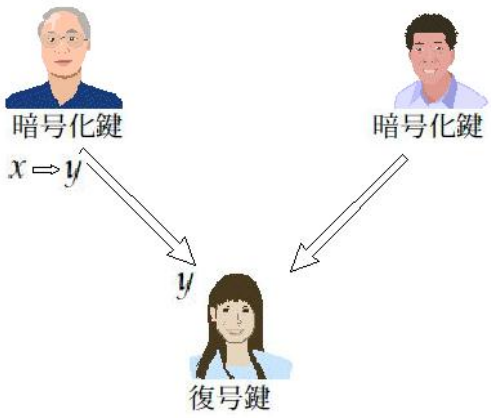
情報が秘密の場合、ただ素直に数 x をそのまま送ると、その情報が途中で盗まれる危険がある。ここで暗号が登場するわけである。
数 x を相手に伝達するのに、数 x を暗号化して数 y に変え、その y を相手に送り、相手はそれを復号して元の x に戻す。結果的に情報が伝達されるというのが、暗号の仕組みである。



x を暗号数 y に変える道具 (システム) を暗号化鍵といい、暗号数 y を元の数 x に戻す道具 (システム) を復号鍵という。 数 x を暗号化鍵を使って暗号数 y に変え、暗号数 y を復号鍵を使って元の数 x に変える訳である。



よくある、暗号システムでは暗号化鍵と復号鍵は同じものを使う。普通の家の鍵と同じで、扉を閉じる鍵とそれを開く鍵は同じもので使い方が開ける時は閉じる時と逆に回すだけである。
RSA 暗号システムでは、暗号化鍵と復号鍵が異なる。たとえ他の人や組織が暗号化鍵をもっていても、復号鍵を手に入れない限り、暗号を復号できない。



それでは RSA 暗号システムについて説明しよう。

$p\ q$　素数　秘密
$N = pq$　公開
$M = (p-1)(q-1) = \phi(N)$
秘密
$a\ b$　自然数
$ab \equiv 1\ (mod M)$
(N, a)　暗号化鍵　公開
(N, b)　復号鍵　秘密

システム構築者は
　大きな異なる二つの素数 p, q を用意する。
　　これは秘密にする。
　p と q の積 N を作る。
　$p-1$ と $q-1$ の積 M を作る。
　　これは N のオイラー数 $\phi(N)$ である。これは秘密にする。
　M と互いに素な大きな自然数 a を用意する。ただし $1 < a < M$
　$ab \equiv 1\ (mod\ M)$ を満たす自然数 b を作る。ただし $1 < b < M$
　(N, a) を暗号化鍵として、情報の送り手に渡す。
　　これは、公開鍵として公開してもかまわない。秘密にしなくても良い。
　(N, b) を復号鍵として、情報の受けてに渡す。

(情報の受け手がシステム構築者なら安全)
　これは、秘密鍵として、秘密にする。

これで、暗号システムが構築された。この暗号システムでどのように情報を伝達するのか、即ち数を伝達するのかを紹介しよう。

暗号化鍵を使って
$y = x^a \ Mod\ N$
と y を作る
y を送る

　情報の送り手は情報を数の列に変えて伝達するだが、伝達する数 x は $1 < x < N$ としておく。つまり N より小さな数に分割しておくる。
　伝えたい数 x に対して

$$y = x^a \ (mod\ N)$$

なるように y を計算する。
　この y が x を暗号化したものである。
この y を情報の受け手に渡す。

y を受ける
復号鍵を使って
$z = y^b \ Mod\ N$
と z を作る
$z = x$ である

情報の受けては受け取った数 y を元に、復号鍵を使って

$$z = y^b \ (mod\ N)$$

と計算して z を作る。このとき実は

$$z = x$$

となり、情報が受け手に伝わることになる。

実際 $z = x$ になることを示そう。

$y = x^a \ Mod\ N$
$z = y^b \ Mod\ N$
であるから
$z \equiv x^{ab} \ (mod\ N)$
である。
　x が N と互いに素のときは
$x^{\phi(N)} \equiv 1 \ (mod\ N)$
であり $ab \equiv 1 \ (mod\ \phi(N))$ なので

$x^{ab} \equiv x \,(mod\ N)$
よって、このときは
$z \equiv x \,(mod\ N)$
また
$1 < x < N$ かつ $0 \leq z < N$
であったので
$z = x$
を得る。
x が N と互いに素でないときは x は p の倍数かあるいは q の倍数である。
x が p の倍数のときは $1 < x < pq$ で p と q は互いに素なので x は q の倍数ではない。
このときは
x が p の倍数なので y も z も p の倍数である。
x と q は互いに素なので
$x^{q-1} \equiv 1 \,(mod\ q)$
$M = (p-1)(q-1)$ で $ab \equiv 1 \,(mod\ M)$ なので $ab \equiv 1 \,(mod\ q-1)$
よって
$x^{ab} \equiv x \,(mod\ q)$
以上より
$$\begin{cases} z \equiv x \,(mod\ p) \\ z \equiv x \,(mod\ q) \end{cases}$$
を得る。
p と q は互いに素で $N = pq$ だったので、Chinese Remainder Theorem より
$z \equiv x \,(mod\ N)$
を得て
$z = x$
を得る。
x が q の倍数のときも、同様にして
$z = x$
を得る。

RSA 暗号システムが安全かつ有効に働いているには理由があります。

(1) $N = pq$ の素因数分解は難しい
(2) M, a から $ab \equiv 1 \,(mod\ M)$ なる
b は簡単に見つかる
(3) (N, a) を知っていても (N, b) は分からない
(4) $x^a \ Mod\ N$ が比較的簡単に計算できる。

(1)　N が大きい数、今までに紹介した記事にも述べたように 1024 ビット、１０進法で 310 桁の数ほどの大きさでは、現時点では困難 (不可能に近い) である。
例え、コンピュータの発展により何とか可能になったとすれば、桁を４桁ほど増やせば少なくとも因数分解の困難さは１桁増えるから、桁を２０桁も増やせば困難さは１０万倍になる。

(4)　N が 1024 ビットほどの大きさの数とすると、x や a もほぼ 1024 ビットくらいの大きさの数になる。$x^a\ Mod\ N$ を求めるのに $a-1$ 回の掛け算を行うのは、到底不可能である。しかし、掛け算してその結果を N による剰余を求める操作を１回の計算と勘定すれは $x^a\ Mod\ N$ を求めるのはには多くても２０４６回の計算ですむ。この事は後で示すことにしよう。

(2)　M と互いに素な数 a と M との与えられたとする。これらが１０２４ビットほどの数のときには、$ab \equiv 1\ (mod\ M)$ なる b を求めるのは一連の操作をせいぜい１０２３回ほど行って求められる。このことも後で示そう。

(3)　例え (N,a) を知っていても M が分からなければ b の求めようがない。M は $N = pq$ となる素数 p と q により $(p-1)(q-1)$ となる数であるが。N の素因数分解が不可能な時点では、p と q さえ秘密にしておけば、M を求めるのは不可能、従って b を求めるのは不可能である。

RSA 暗号システムの要点は大きな素数の発見と素因数分解の不可能性をその原理として持っている。どの程度の大きさの数であれば素因数分解が可能かあるいは不可能かその技術や仕組みの研究がずっと続いている。その最先端の研究や技術はある意味では国家機密や企業秘密である。早い話が、みんなが不可能と思っている因数分解を可能にする技術を密かに保持している国や企業があれば、そこは多くの秘密を密かに覗き見る機会を得ることになる。

8.4　RSA 暗号システムの仕組みで主張したことのはなし

ここでは、前の部分節で主張しその説明を持ちこしたことを証明 (説明) しよう。

a が n ビットの自然数とすると
$x^a\ Mod\ N$ は $2(n-1)$ 以下の操作で
求めることができる。

これは、一般に証明するまえに例で説明した方が分かりやすいでしょう。

$a = 443 = 110111011_{(2)}$
の場合で説明しよう。

a は 9ビットの数であり、2進法で表わしたときには1 が7 個あらわれている。

$a = 2^8 + 2^7 + 2^5 + 2^4 + 2^3 + 2 + 1$
である。

$x_0 = x$
$x_1 = x^2 \ Mod\ N$
$x_2 = x^{2^2} \ Mod\ N$
$\vdots$
$x_8 = x^{2^8} \ Mod\ N$
とおくと

$x_1 = x_0 \times x_0 \ Mod\ N$
$x_2 = x_1 \times x_1 \ Mod\ N$
$x_3 = x_2 \times x_2 \ Mod\ N$
$\vdots$
$x_8 = x_7 \times x_7 \ Mod\ N$
なので

$x_0, x_1, x_2, \cdots, x_8$ を求めるのに8回の操作が必要である。

$y_1 = x^{1+2} \ Mod\ N$
$y_2 = x^{1+2+2^3} \ Mod\ N$
$y_3 = x^{1+2+2^3+2^4} \ Mod\ N$
$\vdots$
$y_6 = x^{1+2+2^3+2^4+2^5+2^7+2^8} \ Mod\ N$
とおくと

$y_1 = x_0 \times x_1 \ Mod\ N$
$y_2 = y_1 \times x_3 \ Mod\ N$
$y_3 = y_2 \times x_4 \ Mod\ N$
$\vdots$
$y_6 = y_5 \times x_8 \ Mod\ N$
と y_6 を求めるのに後6回の操作で済む。

$y_6 = x^a \ Mod\ N$
であるので、$x^a \ Mod\ N$ は8+6 の計１４回の操作で求められる。

一般に a が n ビットの数であり a を2進法で表わしたとき1 の数が m 個あるとき

$x^{2^{n-1}} \ Mod\ N$ まで求めるのに $n-1$ 回の操作が必要であり

$x, x^2 \ Mod\ N, x^{2^2} \ Mod\ N, \cdots, x^{2^{n-1}} \ Mod\ N$ を元にして $x^a \ Mod\ N$ は $m-1$ 回の操作で求められる。よって $x^a \ Mod\ N$ は $n+m-2$ 回の操作で求められる。

a と M が互いに素な自然数とする。
a が n ビットの自然数とするとき

$$ab \equiv 1 \pmod{M}$$

なる自然数 b はせいぜい $n-1$ 回の操作で
求めることができる。

これは、n についての数学的帰納法で示。される