数学入門公開講座

昭和54年8月7日（火）から8月16日（木）

講師

小　松　醇　郎

松　浦　重　武

伊　藤　　　清

一　松　　　信

京都大学数理解析研究所

講師及び内容

1．日本の洋算について（6時間）　　東京理科大学理工学部教授　小松醇郎

日本で正式な洋算教育を受けたのは，1855（安政2）年幕府が長崎海軍伝習所を作り，オランダ海軍士官による，航海術・測量術等の教育を始めた時からである。明治初期までは和算家・洋算家が共存したのであるが次第に洋算家のみとなり，その後100年，日本の数学は世界一流になったのであるが，それは世界の驚異である。幕末時代・明治時代を主として，洋算発達の状況を述べ，数学発達のルーツを解説する。

2．円形の池に浮かぶ中の島の形について（6時間）　　京都大学数理解析研究所教授　松浦重武

上記表題のもとに，一見して簡単な初等平面幾何の問題から出発して（未知の？）新曲線群の話におよびたいと思う。

3．確率模型の話（6時間）　　学習院大学理学部教授　伊藤清

数学の諸概念，例えば関数，群などは，すべて実在の現象の論理模型として作られたものである。偶然的な要因の介入する現象の模型として確率模型があり，これを論理的に磨き上げたものが確率論の研究の対象である。この講義では簡単な確率模型を通して，確率論の諸概念の直観的意味と応用を説明する。

4．素数の話（6時間）　　京都大学数理解析研究所教授　一松信

1と自分自身以外で割り切れない整数が素数である。（たとえば1979は素数である）素数の性質は古代から研究されているが，いまだに数学の難問の宝庫である。近年いろいろな判定法が開発され，計算機の発展とあいまって大きな素数が数多く発見されている。そして符号系の理論，さらに暗号などへと思いかけぬ応用も開けつつある。それらの話題を含めて，これまでの学校教育で必ずしも十分にとりあげられていなかった素数をめぐるいくつかの結果を紹介する。

時間割

時間＼日	7日(火)	8日(水)	9日(木)	10日(金)	11日(土)	12日(日)	13日(月)	14日(火)	15日(水)	16日(木)
13:15～14:45	日本の洋算について（小松）						確率模型の話（伊藤）			
14:45～15:00	休憩						休憩			
15:00～16:30	円形の池に浮かぶ中の島の形について（松浦）						素数の話（一松）			

素数の話

講師：一松 信

期間：　昭和54年8月13日～16日

時間：　15：00 ～ 16：30

数学入門公開講座 (1979. 8. 13 – 16)

"素数の話"

京大 数理解析研究所　教授

一松　信

0. はしがき

1と自分自身とでしか割り切れない整数が素数である (例. 2, 5, 13, 79, 1979, 65537, 2147483647). 素数の性質は大昔から現在まで, 数論の宝庫である.

ここではそれらのうち, 高校段階までの数学で (原理的には) 理解できるはずの諸結果で, 意外に知られていない題材をいくつか論じ, 最後に近年注目をひいている暗号への応用に言及する予定である.

I. 素数の基本性質: 素朴な判定, Erathostenes の篩, 互除法, イデアル, 素因数分解の一意性.

II. p を法とする体系: 有限素体 $\mathbb{Z}_p$, Fermat テスト, 擬素数, Mersenne 素数 など

III. 素数は無限にある: $\Sigma(1/p) = \infty$; Beltrand = Čeby-šev の定理, 素数定理

IV. 暗号への応用: 一方通行関数, RSA 体系 など

I. 素数の基本性質

1.1. 素朴な判定法

与えられた正の整数 n が素数であるかどうか判定する最も素朴な方法は, 順次素数 2, 3, 5, 7, … で割ってみればよい. どこかで割り切れればもちろん合成数である. 素数でないとき素因数までほしければ事実上こうするしかない. 素数を順次作りだすのが厄介ならば, 素数をすべて含む容易に作れる列; たとえば2とすべての奇数とか, 2, 3, 5 以後は交互に 2, 4 を加えて, 3の倍数をとばした奇数列, が使われる.

ではどこまで割り切れなかったら, 素数と断定してよいか? n? $n/2$? … ? —— 正しい答は $\sqrt{n}$. そしてこのためには $\sqrt{n}$ を作らなくても, n を m で割った商 q が m より小さくなっても割り切れなくなれば素数と断定できる. なぜか?

1.2. Erathostenes の篩

ある範囲の素数を全部求めるには, いまでもこの古典的方法が有用である. たいていの教科書には初めの方があげられているが, 途中からやってもよい. 1900 と 2000 の間の素数を全部求めてみる. 簡単のために偶数は事前に篩って奇数のみ書いた. 上の p はその素数で割り切れる最初の数 (19を略) であり, 以後 p ごとに消す. 一度消した所はそれ以上消さなくてもよい. $\sqrt{2000} < 45$ なので, 43までで十分である.

	11	5 3		23	13 7				19	17		
01	~~03~~	~~05~~	07	~~09~~	~~11~~	13	~~15~~	~~17~~	~~19~~	~~21~~	23	~~25~~
	41			43				29				
~~27~~	~~29~~	31	33	~~35~~	~~37~~	~~39~~	~~41~~	~~43~~	~~45~~	~~47~~	49	51
31				37								
~~53~~	~~55~~	~~57~~	~~59~~	~~61~~	~~63~~	~~65~~	~~67~~	~~69~~	~~71~~	73	~~75~~	~~77~~
79	~~81~~	~~83~~	~~85~~	~~87~~	~~89~~	~~91~~	93	~~95~~	97	99		

— 20世紀は素数の多い (prime period) らしい. 特に双子素数が異常に多い感じである.

1.3. 互除法

2つの正の整数 m, n の最大公約数を求める算法である. 「原論」にあるのは, むしろ「互減法」である. 現代流にいうと, 次のようになる.

1. mとnをくらべ, $m<n$ なら名前を交換する.
2. $m \geqq n$ ならmをnで割り, 商q, 余りrを求める.
3. $r=0$ ならばそのときの除数nが最大公約数.(終り)
4. $r>0$ ならば, n, r を m, n におきかえ, 2に戻る.

これにはいろいろの変形, 改良がある.

Laméの定理. 互除法の演算は, m, n の小さい方を十進法で書いた桁数Nの5倍以内で完了する. したがってその計算量は, $\log \min(m,n)$ の定数倍ですむ.

証明. $m=a_{i+1} \geqq n=a_i$ とし, 順次 $a_{k+1}=q_k \cdot a_k+a_{k-1}$, $a_0=0<a_1<\cdots<a_i$ とする. $a_1 \geqq 1$, $q_1 \geqq 2\ (a_1<a_2)$, ゆえに $a_2 \geqq 2$, $a_3 \geqq 3$, $a_k \geqq f_k$ (Fibonacci列). しかし f_kは

帰納法で $f_{5+k} > 10 \cdot f_k$ なので，$5k < l \leqq 5(k+1)$ ならば f_l は少くとも $(k+1)$ 桁，ゆえに a_l が少くとも $(k+1)$ 桁 なる回数 $l \leqq 5(k+1) \leqq 5 \times a_l$ の桁数，となる．

同様に二進法のビット数 M では，$\leqq 1.48M$ である.」

この定理は，なぜ最大公約数を求めるのに，小学校で最初に習うような素因数分解して比較する算法が非実用的であり，互除法が有用であるかを明確に説明してくれる。

1.4. イデアル

便宜上 0 及び負の整数をも考え，その全体を $\mathbb{Z}$ とおく．$\mathbb{Z}$ 内では，加，減，乗の演算が自由にできる（整域）．

$\mathbb{Z}$ の部分集合 A がつぎの性質をもつとき，A をイデアルという．$1°$ $x, y \in A$ のとき $x - y \in A$（詳しくは $0 \in A$; $x \in A$ なら $-x \in A$; $x, y \in A$ なら $x + y \in A$）

$2°$ $x \in A$, $a \in \mathbb{Z}$ ならば $ax \in A$.

例. $n \in \mathbb{Z}$ の倍数全体．これを n から生成される単項イデアルといって $[n]$ で表す．$[1] = \mathbb{Z}$, $[0] = \{0\}$.

補助定理1. $\{0\}$ 以外の $\mathbb{Z}$ のイデアルは，つねにそれに含まれる正の最小の整数 n から生成される．

系. $m, n \in \mathbb{Z}$ に対して $[m, n] = \{am + bn \mid a, b \in \mathbb{Z}\}$ はイデアルであり，m, n の最大公約数 d から生成される．

定理2. 正の整数 m, n に対して，適当に $a, b \in \mathbb{Z}$ をと

って，$am+bn=d$（m, n の最大公約数）とできる．

定理2で a, b を具体的に求めるには，互除法を活用するとよい．

系　m, n が互いに素ならば，適当に $a, b \in \mathbb{Z}$ をとって $am+bn=1$ とできる．

1.5. 素因数分解の一意性

［初等整数論の基本定理］任意の正の整数は，順序を問わなければ，ただ一通りに素因数の積に分解される．

［注意］普通1を素数の仲間に入れないのは，この定理に余分な但し書きをつけたくないためである．

補助定理3　整数の積 mn が素数 p で割り切れれば，m か n か少くとも一方が p で割り切れる．

証明．m が割り切れなければ，m, p は互いに素なので，$am+bp=1$ をみたす $a, b \in \mathbb{Z}$ がある．$n=amn+bnp$ は p の倍数である．」

系．p が素数，n が p の倍数でないとき，an と bn を p で割った剰余が等しければ，a と b を p で割った商も相等しい．（このとき $a \equiv b \pmod{p}$ と書く．）

一意性定理の証明．分解可能なことは，正の整数の無限降下列がないことからわかる．一意性は，2通りに

$$n=p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

と分解されたとすると，p_1 は q_i のどれかを割る．それを q_1 と

すると，$p_1 = q_1$；これを除いて同じ論法をくりかえす.」

[応用] 素数の平方根はすべて無理数である：もし $\sqrt{p} = m/n$ なら $pn^2 = m^2$ と2通りに素因数分解ができる！

II. pを法とする体系

2.1. 有限素体$\mathbb{Z}_p$

正の整数nを定め，すべての整数をnで割った剰余$0, 1, \cdots, n-1$に還元した体系を，nを法とする剰余系といい，$\mathbb{Z}_n$で表す。これには加減法が自然に導入され，しばしば時計代数とよばれる。さらに乗法が自然に導入される．

nが合成数のときには，0でない数同志の積が0になることがある（$\mathbb{Z}_{12}$中で $3 \times 4 = 0$）．しかしnが素数のときにはこのようなことはない（補助定理3）．しかも定理2系により，0でないmによる除法ができる．すなわちpが素数のときには，有限個の要素からなる$\mathbb{Z}_p$は，0で割ることを除いて四則の演算が自由にできる.—— 数学の術語で体（タイ）という．

$\mathbb{Z}_p$は標数pの体の最小のもので素体とよばれる．有限体はすべてある素数pの累乗p^l個からなり，$\mathbb{Z}_p$上のl次元線型空間として特徴づけられる．有限体は符号系や組合せ論などに広く応用され，それだけでもこの講義で話しきれないほどの豊かな内容をもつ．

2.2. Fermatテストと擬素数

[Fermat の小定理] pが素数ならば, pの倍数でないaに対してつねに $a^{p-1}\equiv 1 \pmod p$.

系1. つねに $a^p \equiv a \pmod p$. $a^{1+(p-1)n}\equiv a \pmod p$

証明. $\mathbb{Z}_p$ 中 $a\cdot 1, a\cdot 2, \cdots, a\cdot(p-1)$ はすべて相異なる(補助定理3系)から, 全体として $1, 2, \cdots, (p-1)$ のいれかえである. これを全部掛ければ $a^{p-1}\cdot(p-1)!\equiv(p-1)! \pmod p$ だが, $(p-1)!$ はpで割り切れないから $a^{p-1}\equiv 1 \pmod p$.」

系2 (Fermat テスト) もしもあるnと互いに素なあるaについて, $a^{n-1}\not\equiv 1 \pmod n$ なら, nは素数でない.

ただしこのテストで素数でないことがわかっても, nの素因数は普通にはわからない.

Fermat テストの逆は一般には成立しない. しかし $n<341=11\times 31$ に対しては, $2^{n-1}\equiv 1 \pmod n$ であるnは偶然(?)すべて素数である. そのために「$2^{n-1}\equiv 1 \pmod n$ であるnは素数」という(誤った)命題が, しばしば「中国の一古定理」とよばれる. またこのようなnを擬素数とかPoulet数という. このようなnは無限にある. さらにnと互いに素なすべてのaに対して $a^{n-1}\equiv 1 \pmod n$ となる(素数でない)nを絶対擬素数とかCarmichael数という. 最小の絶対擬素数は $561=3\times 11\times 17$ である. その条件は, nを素

因数分解して $n=p_1\cdots p_r$ としたとき, p_i がすべて相異なら, $(p_i-1)|(n-1)$ である.(少くとも3個の素因数あり.)

絶対擬素数が無限にあるか否かは不明だが, たぶんそうらしい. 根拠: 10^{10}までに6000個以上ある; 計算機により, 数十桁のものが続々発見されている; xまでの個数の予想($x\to\infty$ とともに発散)と実験が非常によくあっている. など.

それにもかかわらず, ランダムにとったいくつかの a に対して $a^{n-1}\equiv 1 \pmod n$ をためすのは, n が素数であるか否かの有用な方法である。近年これを改良して, ある限界 b まで $(a,n)=1$, $a^{n-1}\equiv 1 \pmod n$, $(a^{(n-1)/2^k} \pmod n, n)=1$ $(1<a\leqq b)$ をためせば, n が素数と断定できる改良算法も求められた. 現在50桁程度の n が素数か否かの判定は, 高速計算機で最大1時間以内でできる. これに反して, 素数でないとき, その素因数を求めるのは, 運が悪ければ, 何年もかかるだろう. この計算量の差が RSA暗号体系(N)の基礎になる.

[Wilsonの定理] 正の整数 n が素数 $\Longleftrightarrow$ $n|(n-1)!+1$

証明. 偶数のときは明らか. 奇数で合成数なら, $n=\prod p^r$ に対し, $n-1$ までに p が r 個あって $n|(n-1)!$; n が奇素数なら, $1,-1$ 以外の $\mathbb{Z}_p$ の要素は逆数の対に分れ, $(n-1)!\equiv -1 \pmod n$ 」

実用には不向きだが, 理論上重要である.

2.3. Mersenne 素数

古代ギリシャ人は,正の整数 n に対して n の真の約数(1を含み n 自身を除く)の和 $s(n)$ に深い関心をもち,

$n=s(n)$ のとき n を完全数; $n=s(m)$, $m=s(n)$ である対を友愛数, などとよんだ. 6と28が完全数であることや, 220と284という友愛数の対は古くから知られていた. ── 以下 n 自身も約数に入れて $\sigma(n)=s(n)+n$ とする.

「原論」第9巻の末尾に, 次の定理が載っている.

<u>定理4.</u> もしも $p=2^k-1$ が素数ならば, $n=2^{k-1}\cdot p$ は完全数である.

証明(現代流) $n=p_1^{e_1}\cdots p_r^{e_r}$ と素因数分解すれば,

$$\sigma(n)=\sum_{a_1=0}^{e_1}\cdots\sum_{a_r=0}^{e_r}p_1^{a_1}\cdots p_r^{a_r}=\frac{p_1^{e_1+1}-1}{p_1-1}\cdots\frac{p_r^{e_r+1}-1}{p_r-1}.$$

ゆえに $n=2^{k-1}\cdot p$ については, $\sigma(n)=(2^k-1)(p+1)=2n$」

興味あるのは, この逆が成立することである.

<u>定理5</u>(Euler). 偶数の完全数は, 定理4の型に限る.

証明. a, b が互いに素ならば $\sigma(ab)=\sigma(a)\cdot\sigma(b)$;
$n=2^k\cdot l$ (l は奇数)とすると, $\sigma(n)=2n=(2^{k+1}-1)\times\sigma(l)$; つまり $\sigma(l)=l+l/(2^{k+1}-1)$. これは l が素数で, $l=2^{k+1}-1$ のとき以外は成立しない.」

2^k-1 の型の素数を <u>Mersenne 素数</u>という. そのためには

kも素数でなければならない．ただしkが素数でも，2^k-1が素数とは限らない．今日知られているMersenne素数は僅かに27個にすぎない．

kの値．｜ 2　3　5　7　13　17　19　31　61　89
(2^k-1) ｜ $\underbrace{3\quad 7}_{\text{古代}}$　$\underbrace{31\quad 127}_{\text{記録は中世}}$　$\underbrace{}_{\text{ルネサンス期}}$　↦ Lucasテストによる

107　127　　521　607　1279　2203　2281　3217
永らく世界記録　↦以後計算機　SWAC(1952/3)　↤ BECK('57)

4253　4423　9689　9941　11213　19937　21701
PEGASUS('59)　ILLIAC II ('61)　IBM('71)　('78) Cyber174 Noll-Nickel

23209　44497
('78)　('79) CRAY-1

Mersenne数にはLucasテストという特別な判定法があり，非常に大きい素数を具体的に作り出す手段として注目されている．Lehmerの改良したその方法は次の通り：

$m=2^k-1$ とし，$u_1=4$．以下 $u_{i+1}\equiv u_i^2-2 \pmod m$ として u_{m-1} まで作る．$u_{m-1}\equiv 0 \pmod m \Longleftrightarrow m$が素数．

（証明は和田秀男氏の論文参照）．

奇数の完全数は一つも知られておらず，あるとすれば少くとも50桁以上の数であることが証明されている．完全数が無限にあるかは未知；友愛数も数千組知られ，ある程度の一般形はあるが，完全な特徴づけはできていない．

（当日関連話題に言及する予定）．

III. 素数は無限にある.

3.1. 素数はいくらでもある.

標記の命題は Euclid の「原論」第9巻第20命題である. その証明は, おなじみの通り, 与えられた素数 $p_1, \cdots, p_r$ に対して $n = 1 + p_1 \cdots p_r$ を作れば, 他の素数があるはず, というものである. しかしこれはかなり「定性的」である. もっと詳しい結果は, 18世紀に Euler がだした.

定理1. $\Sigma(1/p)$ は発散する.

略証. $1/\Pi(1-1/p) = \Pi(1+1/p+1/p^2+\cdots) = \Sigma 1/n = \infty$.

Euclid のと同様にして, $4n+3$, $6n+5$ の型の素数が無限にあることは容易に示される. Dirichlet は, 初項と公差が互いに素な等差級数中に無限に素数があることを証明した.

3.2. 粗雑な素数定理

$x>0$ を超えない素数の数を $\pi(x)$ とすると, 素数定理

$$\lim_{x\to\infty} \pi(x)/(x/\log x) = 1$$

が知られている. (Gauss が予想; Hadamard と de la Vallée-Poussin とがほぼ同時に証明; 1896). $x/\log x$ は主要項であり, むしろ $\mathrm{li}\, x = \int_2^x dt/\log t$ のほうが正確である.

この証明は難しいが, Čebyšev による次の「粗雑」な結果でよければ, すぐに示される:

定理2. $0 < a < \pi(x)/(x/\log x) < b$ である定数 a, b

が存在する。

補助定理3. $n!$ を素因数分解して $\prod p^r$ とするとき，指数は $r=\sum_s [n/p^s]$ で与えられる。（[ ]は整数部）

系1. $\binom{2n}{n}=c_n=\dfrac{(2n)!}{n!\,n!}$ を素因数分解 $\prod p^r$ すると

$r=\sum_s([2n/p^s]-2[n/p^s])$. この各項は1か0なので，$r\leqq \log_p(2n)$, $p^r\leqq 2n$.

系2. 系1で $n<p<2n$ である素数は c_n の素因数分解に1乗で現れ，$2n/3<p\leqq n$ である素数は c_n に現れない。

補助定理4. $2^n\leqq c_n\leqq 4^n$；もっと詳しく $n\geqq 5$ なら $4^n/n<c_n<4^{n-1}$.

定理2の証明. 補助定理3系1により，$p\leqq 2n$ について p^r の積 $\geqq c_n\geqq 2^n$ は $(2n)^{\pi(2n)}$ を超えないから，

$\pi(2n)/(2n/\log 2n)\geqq \log 2>0$.

一方 $n<p<2n$ である素数の積 $\leqq c_n\leqq 4^n$ は $n^{\pi(2n)-\pi(n)}$ より大きいから $\pi(2n)-\pi(n)<b_1(n/\log n)$. これから $(\log 2y)\pi(2y)-\log y\cdot\pi(y)<b_2 y$ となり，$y=x/2,\ x/2^2,$ ---を順次代入して加えれば，$\pi(x)/(x/\log x)<b$（定数）.」

素数定理は，x までの素数を順次掛けると，ほぼ e^x 程度になる，と解釈できるが，n までの素数の積を P_n とすると.

定理5. $(\sqrt{2})^n\leqq P_n\leqq 4^n$（左側は $n\geqq 2$ について）.

証明. n が小さいときは明らか. 右側は n を奇数 $2m-1$ としてよい. n より小さいとき正しいとすると $P_m\leqq 4^m$.

mから$2m$までの素数の積$\leqq C_{2m} \leqq 4^{m-1}$ $(m \geqq 5)$．ゆえに$P_{2m-1} \leqq 4^{2m-1}$となって帰納法による．(左側は略)．

3.3. Beltrand - Čebyšev の定理

定理6．nと$2n$の間に必ず素数がある．

以下のは P. Erdős, Acta Szeged, 5 (1932) による．

証明．ないとすれば，C_nの素因数分解はQ_1 ($\sqrt{n}<p\leqq 2n/3$であるpの積)，Q_2 ($p\leqq\sqrt{n}$であるp^{ν}の積) の積になる．補助定理5から$Q_1 \leqq 4^{2n/3}$；補助定理3系1からQ_2の各項$\leqq 2n$で，$Q_2 \leqq (2n)^{\pi(\sqrt{n})}$．偶数は2以外素数でないから$\sqrt{n}\geqq 8$なら$\pi(\sqrt{n})\leqq\sqrt{n}/2$．ゆえに$n\geqq 64$なら$C_n=Q_1Q_2$から

$$n\log 4-\log n \leqq (2n/3)\log 4+(\sqrt{n}/2)\log(2n),\text{ すなわち}$$

$$2n/3 \leqq (\sqrt{n}/2)+(\sqrt{n}/2)\log_2 n+\log_2 n.$$

ところがこの左辺は右辺よりも急激に大きくなり，たとえば$n\geqq 64$では成立しない．ゆえに定理6は$n\geqq 64$で正しいが，それ以下でも素数表を見れば，3, 5, 7, 13, 23, 43, 83 という次々に2倍より小さい素数があるから正しい．

この形の定理の拡張はいろいろある．Riemann 予想が正しければ，十分大なnに対して，nと$n+c\sqrt{n}$ (cは定数) の間に素数が必ずあるが，現在のところnと$n+cn^{0.6}$の間に素数が必ずあるというのが最良の結果のようである．

［注意］この定理は「相対的」に長い無素数区間がないことを示す.「絶対的」な長さならく, $n!+x$ $(2\leqq x\leqq n)$ はすべて合成数だが, n に比べて $n!$ は大きすぎる. Riemann予想は, n に対して無素数区間は $\sqrt{n}$ 程度が限度であることを意味する.

B.Č. 定理はまた素数を順次作りだしてゆく手順で p から p^2 まで素数がなく, とびを生ずることがないことを保証してくれる。もっともこの事実だけならば, 同じようにして, もっと簡単に示される.

他の応用は $1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$ $(n\geqq 2)$ がけっして整数になりえないことの証明である. もしもある素数 p の倍数が分母にただ1つだけなら, まとめて $\frac{b}{a}+\frac{1}{lp}$ (a は p と互いに素) となり, 通分した $\frac{blp+a}{lap}$ の分子は p で割れないから整数にはなりえない. そういう p は n と $[n/2]$ の間に必ずある。—— もちろんこの事実は B,Č の定理を使わず, もっとエレガントに直接できる。

そういうわけで, B.Č. の定理は, 昔の教科書にあるように「証明が非常に難しい」ものでも,「役にたたないが有名だからあげておく」ものでもなく, もっと初級の教科書にあげて広く知られてよい事実の一つのように思われる.

Ⅳ. 暗号への応用

4.1 概論

暗号というと軍事機密という暗い影がつきまとうが，ここで論ずるのは，今後電子郵便，個人のデータ，などのプライバシー保護を目的とする「平和利用」である。

暗号の一般理論に深入りする余裕はないが，その方式に

換字式，　転置式，　挿入式

があること，また別の面から分類すると

逐字式，　ブロック式（小ブロック，大ブロック）

と大別されることを一言しておく。

現在では通信は手紙，すなわち情報を載せた媒体そのものを物品として運搬するよりも，無線通信のように情報だけを直接送付する方式が主流である。そのため，通信途上の秘密を守る暗号は，情報を圧縮できること，一部分欠けても全部が読めなくならないこと，などが要請される。この面から，必然的に換字式が中心となり，逐字式の機械暗号が主流であった。近年IC回路の発展により，記憶回路が安くなったので，小ブロック式の換字暗号が多くなってきた。

抽象化すれば，暗号とは，平文空間 X から他の文章空間 Y への写像　$E: X \to Y$　である。Eは全単射であることが望ましいので，以下ではそうする。Eの逆変換（解訳）をDと

する.「理想的」な暗号は, つぎのようなものであろう.

1° EもDもたとえば適切に設計された電子回路(電子計算機)によれば, きわめて容易に自動的に実行できる.

2° 順変換Eのみを知って, それから逆変換Dをもとめることは, 理論上は可能であっても, 現実には(計算量の点で)不可能に近い.

このような変換Eを隠し穴変換とか一方通行関数という.(その実例は後述). このような変換があれば, 次のような暗号体系ができる.

互いに通信しあいたいメンバーを$\{A_i\}_{i=1}^n$とする. 各A_iは個人でも団体(会社, その支社, 政府, 軍その他)でもよい. 各A_iは隠し穴変換E_iとその逆変換D_iを有する. ただし$E_1, \cdots, E_n$は公開されているが, D_iは対応するA_iの極秘とされる. 誰かがA_iに通信したければ, E_iで変換して送信すればよい. A_iはD_iで戻して読むことができる.

この方法は大きな副次的利益がある. 偽造不可能な署名がつけられる. A_jがA_kに送信するとする. A_jは平文xに秘密の逆変換D_jを施したものを平文とみなして

$$E_k \circ D_j(x)$$

を送る. A_kは自分の翻訳用変換D_kを行い, さらに公開の暗号化変換E_jを施すと,

$$E_j \circ D_k \circ E_k \circ D_j(x) = E_j \circ D_j(x) = x$$

となる。この「署名」は他人はもちろん A_k も偽造できない！

この暗号体系のもう一つの利点は，メンバーが n のとき，相互の通信は $n(n-1)/2$ 通りありうるのに，暗号は n 組用意すればすむことである。これは n が大きいとき非常な節約になる。

4.2. 一方通行関数

以上は Stanford 大学の Merkle, Diffie, Hellman らの着想である。問題は適切な一方通行関数の実例がえられなかった点である。

純粋数学の立場からいうと，これはナンセンスかもしれない。有限集合の全単射については，変換表を作ってしまえばよい。これが意味があるのは，その分量が取扱える範囲であり，時間が実用上意味がある限度内でなければ，事実上実行不可能になる点にある。

このような計算量の理論は，1970 年代に入ってから急激に進展してきた。純粋数学（神様または仙人）の立場では，非常に長い（たとえば百億年）有限の時間と，真の無限時間とは別であるが，寿命の短い普通の人間の立場では，どちらも不可能という点で，実質的な差はない。原理的に解読可能

でも，実際の計算に（超高速計算機をフルに使って）数年もかかるのなら，十分に実用になる．EとDと手間に大差がある例はありうる．

例1．ベクトルa（n次元）をbに変換するのに可逆行列Aを左から掛ける：E：$Aa=b$．これはn^2回の計算でできる．逆変換をAのみでやれば，連立1次方程式を解くことになるので，たとえば$n^3/3$回程度の計算がいる．

例2．2つの数x, y（順序を問わない）から$x+y=a$，$xy=b$を作るのは何でもない．逆にa, bからx, yを求めるには，2次方程式$t^2-at+b=0$を解く手間がいる．

これらは単なるモデルであって，実用には遠いが，古典的に有名な「詰めこみ問題」(Knapsack problem)：長さ$a_1, \cdots, a_n$の棒をうまく組み合せて，長さCの筒にできるだけきっちりはめてゆく問題；から，実際に陥し穴変換が作られる．

しかし実用上注目されているのはM.I.T.のRivest，Shamir，Adlemanらの発案した体系(RSA体系)である．これももちろん「解読不可能」と証明されたわけではない。しかしそれにかなり近いことを示す結果もあり，その公表にアメリカ国防省から横槍が入るなど，多くの話題を提供した体系である．

4.3. Rivestの着想（RSA体系）

前に（　　）述べたとおり，任意の素数pに対して，

$$a^{m(p-1)+1} \equiv a \pmod{p} \qquad (0 \leqq a < p \text{ なる還元して} a)$$

である．したがって$p-1$と互いに素なrをきめ，$a \mapsto a^r \equiv b \pmod{p}$を作れば，$rs+m(p-1)=1$である$s$を選ぶと

$$b^s = a^{rs} = a^{1-m(p-1)} \equiv a \pmod{p}$$

となってaが復元できる．但しpとrを知ってsを求めるのは，それほど大変ではない．

しかしもし$n=p\cdot q$（p, qは相異なる素数）に対して，$(p-1)(q-1)$と互いに素なrをきめ，$a \mapsto a^r \equiv b \pmod{n}$を作ると，復元は容易でない．原理的には$n$を素因数分解し，$p$に対する$s$，$q$に対する$t$を求めると，$\overset{\text{G.C.M.}}{(p-1,q-1)} \mid (s-t)$で，

$$u = s + l(p-1) = t + m(q-1) \text{ があり，} \quad b^u = a^{ur} \equiv a$$

とすればよいはずである．しかしnのみを知って，その素因数p, qを求めることは，大変な手間を要する．Rivestは，これを前記の一方通行関数として，暗号に採用することを提案した．（p, qがわかれば，s, t, uを求めるのは容易である．）

Rabinは，この暗号を解読する早い方法があれば，素因数分解$n=pq$が容易にできることを示した．このことは，直接にこの暗号を解読する早い方法がなさそうなことを意味する．

例. Rivest は, A=01, B=02, --, Z=26, 空白=00 という素朴な十進コードで文を数にし, $r=9007$, n を

114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541

ととった. nは65桁の2個の素数p, qの積である. 彼らは次の暗号文を100ドルの懸賞つきで出した: 9686 9613 7546 2206 1477 1409 2225 4355 8829 0575 9991 1245 7431 9674 6951 2093 0816 2982 2514 5706 3569 3147 6622 8839 8962 8013 3919 9055 1829 9451 5781 5154.

これに次の署名がついている: 16717861150380844246015271389168398245436901032358311217835038446929062655448792237114490509578608655662496577974840004057020373. これを9007乗(mod n)をすると(頭の0を除く)

06 09 18 19 20 00 19 15 12 22 05 18 00 23 09 14 19 00 15 14 05 00 08
F I R S T ␣ S O L V E R ␣ W I N S ␣ O N E ␣ H
21 14 04 18 05 04 00 04 15 12 12 01 18 19 となる.
U N D R E D ␣ D O L L A R S

アメリカ国防省が世界最高速の計算機CLAY-1によって強引に(nを素因数分解して)解読しようとしたというが, 結果はきいていない.

参考文献

一松 信, 数学概論, 新曜社, 1979

高木貞治, 初等整数論講義, 新版, 共立出版, 1971

内山三郎, 素数の分布, 槇書店, 1972.

ガードナー, 一松信訳. 続数学魔法館, 東京図書, 1979
(第12章. 完全数, 友愛数, 社交数)

ガードナー, 一松信訳, 数学ゲームI., 日本経済新聞社, 1979 (9. 新種の暗号)

R. Honsberger, Mathematical Gems I, II., Amer. Assoc. of Math. 1976 (Iの1章, 13章, IIの7章など)

M. E. Hellman, The mathematics of public-key cryptography, Scientific American, 1979 Aug
(日本語訳, サイエンス 10月号予定)

高橋磐郎, 組合せ理論とその応用, 岩波全書, 1979.

和田秀男, ルカス・テストについて, 数学セミナー, 1979, 6月号, 78－81.