

## “大きな数”とその情報理論への応用

京大・数理研 一 松 信

### §1. “大きな数”のパラドックス

Gamovの『1, 2, 3, ...,  $\infty$ 』(日本語訳, 白揚社)の冒頭に次のような笑話が出てくる。2人のバンガリーの貴族がたいくつしのぎに大きな数をいうゲームをした。1人がさんざん考えて「3」といった。相手は長いこと考えて降参した!——

ところが1960年代にオーストラリアの数学者達が、ニューギニアの原住民に数学教育を始めたとき、この笑話が現実となった。彼らの最初の仕事は、現地の人々の言語で、教詞を作ることであった。(後の話はガモフの本にはない。Exeterでの国際数学教育会議の報告による。)

ところで大きな数をいうゲームは、順次にやれば後手必勝であるから、公平にするために双方とも秘密に紙に書いて審判に渡すとしよう。すると妙なパラドックスを生ずる。書く数を正の整数に限定すると、 $m$ を定めれば、 $m$ より小さい数は有限個で選ばれる確率0であり、 $m$ より大きい数は無限個で選ばれる確率1である。どちらも数を書いてしまえば、負

ける確率が1になる!?

このパラドックスの一つの解決案は、有限時間内に、有限の大きさの紙片に書ける数には上限がある、という事実を認めることである。そうすると上記のゲームは、小さい字を早く書く能力をもった者が勝になる?

急激に大きくなる漸化式としては、Ackermann 函数や、Knuth の  $\uparrow$  記号 [2] などがある。最近 Graham は組合せ問題のある上限で、想像を絶する巨大な整数を与えた [3]。  
(たぶん Littlewood の  $10^{10^{34}}$  など足許にも及ばない数である)  
Graham (?) は  $3^{3^3} = 7625597484987$  を「小さい数だから実際に書き下せた」と皮肉をいっている [3]。

要するに、直接苦勞なく扱える数が「小さい数」らしい。最初の FORTRAN-I では  $2^{15} = 32768$  は大きい数であり、現在の研究所の TOSBAC-3400 では  $2^{23} = 8388608$  は大きい数である。

ここで扱う「大きな数」は、それほどでらぼうな怪物ではなく、十進 100 桁くらいの、特別な多倍長プログラムを作れば扱える数である。

## §2. 大きい素数の判定法

大きい整数  $n$  が素数か否かを判定する技法は、近年著るしく発展した。素因数を求めるには、実質的に  $\sqrt{n}$  までの素数

で割ること ( $n$  の性質により、素因数の型を限定して多少手間を減らせるが) しかない。しかし素数か否かの判定だけなら、ずつと容易である。その鍵は Fermat の小定理:  $n$  が素数ならば、 $1 < a < n$  に対し  $a^{n-1} \equiv 1 \pmod{n}$  である。この逆は正しくない。しかし「 $2^{n-1} \equiv 1 \pmod{n}$  ならば  $n$  は素数」という命題は "old Chinese Theorem" [5], I とよばれ、実際  $341 = 11 \times 31$  より小さい数に対しては正しい。Erdős は、こういう  $n$  を pseudo-prime とよんで研究している。(無限にあること、偶数のものも無限にあることなど)。さらに強く、 $(a, n) = 1$  なら  $a^{n-1} \equiv 1 \pmod{n}$  である  $n$  を「絶対擬素数」という。素数でない最小のものは  $561 = 3 \times 11 \times 17$  であり、<sup>(他にも)</sup>  $2821 = 7 \times 13 \times 31$  などいくつかある。これらは少くとも3個の素因数を含む。無限にあるらしいがはっきりしない [5], I.

Fermat テストのみでは、素数と断定するには不十分だが (素数でないほうには  $\neq 1$  ができれば断定できる), Solovay-Strassen [6] は、モンテ・カルロ式にランダムに  $a \in \mathbb{Z}$  を選び、 $(a, n) = 1$  ? (NO なら合成数),  $\varepsilon \equiv a^{(n-1)/2} \pmod{n}$   $\neq \left(\frac{a}{n}\right)$  ? (Jacobi の記号; YES なら合成数) を反復し、いくつかの  $a$  で通れば、素数とみなす。この方法で  $2^{200} + 235$  が、PDP-10 で 45 秒で素数と判定されたという [1].

もつと確実な、計算量  $n^{1/4}$  または  $\lceil \log_2 n \rceil^4$  強、の判定法も知られている。なお最大公約数は、古典的な互除法でも、小正整数の十進桁数の5倍以下の反復で求められる (Lamé の定理; たとえば [5], II 巻)。このように素数か否かの判定は比較的容易だが、素因数を実際に求めることはものすごく大変という計算量の差が、以下の話の鍵になる。

### §3. 暗号への応用

最近 Diffie-Hellmann の着想を基にし、Rivest (M.I.T.) が、画期的な暗号を考案した。現在でも「一回限りの乱数使用」によって、理論的に解読不可能な暗号はあるが、鍵字(乱数)の生成、配布、消去に大変な手間を要する。この暗号は、秘密通信という以上に、日常の電話や「電子郵便」の盗聴(盗視)防止用として有用と思われる。

その抽象的な形はつぎのとおりである:

$A_1, \dots, A_n$ : 相互に交信した  $n$  メンバー (会社, 政府機関等)

$\{M\}$ : 通信文空間. コード化して  $N = \{0, 1, 2, \dots\}$  の有限部分集合としてよい。

$D_e, E_e$ : 互いに逆である  $\{M\} \rightarrow \{M\}$  の全単射;  
条件として,  $D_e, E_e$  それぞれは速やかに計算できるが

$E_k$  のみか既知でも, それから  $D_k$  の具体的な算法を求めることは, 計算量の点で実質的に不可能であること.

利用法 各  $A_k$  は秘密の変換  $D_k$  をもつ.  $A_k$  あての文は  $E_k$  (公開してよい) によって変換して送る.

この方法の長所 1.° 作成法  $E_k$  自体は秘密にしなくてもよい. 誰でも利用できる.

2.°  $n$  メンバーに対し  $n$  個の暗号で十分であり,  $n(n-1)/2$  個を要しない.

3.° 次のようにして偽造不可能な署名が可能: たとえば  $A_1 \rightarrow A_2$  ならば, 平文  $M$  に対して

$$E_2 \circ D_1(M) = M^*$$

を送る.  $A_2$  は

$$E_1 \circ D_2(M^*) = M$$

として翻訳する.  $D_1$  は  $A_1$  以外は知らないはずである. もし  $A_1$  が公開文を発表するときは,  $D_1(M)$  を出す.  $E_1$  によって“翻訳”ができる.

具体的な方法 当初 Hellmann のあげた行列の積や, 素数乗法とする累乗は十分でなかったが, Rivest が次のように改良した.

大きな(十進数十桁の)素数  $p, q$  をとり,  $p-1, q-1$  と互いに素な  $e$  を選ぶ.  $N=pq$  と  $e$  とは公表する. 平文  $M$

数字列に直し、必要ならいくつかは区切って、 $N$  以下の数  $x$  (のいくつかの組) にする。各  $x$  に対して

$$y \equiv x^x \pmod{N}$$

を計算して  $y$  を送る。翻訳は適当な  $s$  により

$$x \equiv y^s \pmod{N}$$

とする。この累乗計算は、2乗、4乗、... を作ることにより、 $\log N$  程度の時間でできる。 $s$  は  $N = pq$  と素因数分解し、 $\forall s \equiv 1 \pmod{p, \text{mod } q}$  である  $s$  を求めればよいが、百数十桁の  $N$  を高速度に素因数分解することは、きわめて難しい。——当然  $p, q$  と  $s$  とは極秘にされる。

各  $A_i$  は別々の  $x$  と  $N$  (そして秘密の  $p, q, s$ ) を持つばよい。

適宜分割すれば error-detecting codes としても活用できそうである。(ただし error-correcting codes としては、難しそうである。)

M.I.T. のグループは、例題として、100ドル懸賞の暗号を提出し、上記の逆算法で暗号化した

FIRST SOLVER WINS ONE HUNDRED  
DOLLARS (を「暗号化」した数字)

という署名をつけ加えた。

#### §4. むすびにかえて——ある横槍

このような研究の発展にたじて、IEEEは1977年10月10日、コーネル大学で暗号学の研究集会を予定した。ところが直前に、アメリカ国防省(に勤める某個人)から、この研究集会は機密保持法に違反する、という横槍が入り[4]、罵いた Hellmann や Rivest らは、処理を大学の顧問弁護士にまかせて、当分 Technical Reports の発送をとりやめたといわれる。既に[1]などに発表された分については不問というようであるが、この横槍は、研究発表の自由、という問題に、思いもかけないショックをいま起したものといえる。

[1]に従って、詳しい実例もあげる予定だったが、版權に反するとか、予算節約とかいう事情以上に、このニュース[4]は、私にとってショックであった。したがって本稿も、この要旨にもの生えた程度でお許し願いたい。

## 参考文献

- [1] M. Gardner; 新種の暗号, 解読に数百万年かかるはずのもの, サイエンス (日本語訳), 1977年10月号
- [2] D.E. Knuth; Mathematics and Computer Science: Coping with Finiteness, Science, 1976 Dec 17, No. 4271, p. 1235-1242.
- [3] M. Gardner; う4せーグラフ, サイエンス (日本語訳), 1978年1月号.
- [4] D. Shapley - G. B. Kolata; Cryptology: Scientists puzzle over threat to open research, publication, Science, 1977 Sept 30, No. 4311, p. 1345-9
- [5] Honsberger; Mathematics Gems I, II. Amer. Math. Association 1974, 76.
- [6] Solovay-Strassen, A fast Monte-Carlo test for primality, SIAM J. Comp. 6, No. 1. (1977), 84-85.