

等差集合の電子計算機による探査

東女大 山本幸一

1. まえがき.

等差集合の電子計算機による探査は、筆者が在米中にもしばしば試みたところである。大きさが素数で、multiplier 指数 e が小さい場合を問題にしているわけであるが、 $e=10$ 及び $e=12$ に対しては完全に成功を収めることができたと信ずる。これに対し $e=14$ の場合は、諸般の事情のため停滞を余儀なくされている。本文は現実の計算様式を説明して大方の批評をあちぎ、計算の実行を容易ならしめることができればと願いつつ書かれたものである。

以下に説明する手続きによって、可能な候補が極めて強く限定される。現実には $e=14$ の場合の等差集合が存在するかどうかさえよく分らない位であるから、その可能性が姿を現わした時に数学的にそれを解明することはむしろ容易であろう。要するにどんな形のものに可能性が残されているか

が興味の中点であって、その辺の事情は単純群の探索の場合に似ているようである。

2. 等差集合の定義.

法 7 で考えた 3 つの数 1, 2, 4 から差を作るとき, 1 乃至 6 が各, 1 回ずつ現われる.

$$2-1=1, \quad 4-2=2, \quad 4-1=3,$$

$$1-4=4, \quad 2-4=5, \quad 1-2=6.$$

このように一定の法 v について考えた k 個の数の集合 D があって, 0 以外の元が, それらの差として常に一定回数, λ 回ずつ表わされているならば, D を等差集合といい, v, k, λ をそのパラメーターという. v は法, k は大きさ, λ は重複度である. これらの間には

$$(1) \quad (v-1)\lambda = k(k-1)$$

なる束縛条件がある.

他の例として $v=13, k=4, \lambda=1$ のもの $\{0, 1, 3, 9\}$ がある. 上掲の条件 (1) は必要ではあるが十分条件ではない. たとえば $v=16, k=6, \lambda=2$ では (1) が成立するが, 対応する等差集合は存在しない.

いわゆる BIBD, balanced incomplete block design の用語でいうならば, 位数 v の群 G から取った大きさ k の部分集合

D に群 G を自然的に作用させる時に生ずる v 個の部分集合がパラメーター (v, k, λ) の対称 BIBD を作ることにして等差集合が定義される。なお上記では一般の群 G を取っているが、 G が巡回群の場合が前述の定義と一致する。

G は有理整数を法 v で考えた加法群とし、 G 上の 1 次変換

$$f: x \rightarrow \alpha x + \beta, \quad (\alpha, v) = 1$$

があれば、 D と共に fD も等差集合になるので、これらの 1 次変換群に基づいて等差集合を同値類に分けることができる。

特に 1 次変換 f が D を不変に保つならば、そのような f と与える α を D の multiplier と呼び、これらの α が作る群を multiplier 群という。

3. 素数位の等差集合.

本稿では法 $v = p$ が素数の場合と考察する。その際 multiplier 群は、 G の自己同型群の部分群で、前者に対する群指数 e を単に等差集合の指数という。それを普通記号 e で表わす。われわれは e の大きさによって、等差集合 D の複雑さを測るべき規準と見る。

たとえば §2 に挙げた例、 $v=7, k=3, \lambda=1, D=\{1, 2, 4\}$

では、 D が 7 の平方剰余の全体であることから知られるとおり、multiplier 群は D 自身で、従って指数 $e=6/3=2$ とな

る。また $(13, 4, 1)$ -等差集合 $D = \{0, 1, 3, 9\}$ は 0 及び、
13 の四乗剰余から成立つ。故に multiplier 群は 13 の四乗
剰余の群で、 G の自己同型群中に指数 $e=4$ を持つ。これら
の例では e が比較的にかさい。われわれの規準からすれば
比較的にか簡単な等差集合といえるわけである。

ある種の自明な等差集合、たとえば $D = \emptyset$ (空集合) とか
 $D = \{0\}$ とかを除けば、 D の指数 e は必ずか偶数であること
が知られている。 e が小さい場合次のような古典的結果があ
る。

[1°] $e=2$ の時。素数 p は $p \equiv -1 \pmod{4}$ を満たすことが

必要で、その時には p の平方剰余の全体が等差集合と作
る。本質的にはこれと違ふ等差集合は存在しない。

[2°] $e=4$ の時。素数 p は

$$p = 1 + 4x^2, \quad x: \text{奇数}$$

又は

$$p = 9 + 4x^2, \quad x: \text{奇数}$$

の形をしてゐることが必要である。前の場合には p の四
乗剰余の全体が等差集合となり、後の場合には p の四
乗剰余の全体に 0 を合併したものが等差集合を作る。

本質的にはそれ以外の等差集合は存在しない。

[3°] $e=8$ の時。素数 p は

$$p = 9 + 64x^2 = 1 + 8y^2, \quad y \text{ 奇数}$$

又は

$$p = 441 + 64x^2 = 49 + 8y^2, \quad y \text{ 奇数}$$

であることが必要である。前者の場合には p の 8 乗剰余の全体が等差集合を作り、後者の場合には p の 8 乗剰余の全体に 0 を合併したものが等差集合となる。本質的には以上が凡ての場合と盡くす。

[4°] 素数 $p \equiv 1 \pmod{16}$ について、 p の 16 乗剰余の全体、乃至それに 0 を合併したものが等差集合になることは起らない（自明の場合： $p=17$ を除く）。

[5°] $e=6$ の時 素数 p は

$$p = 27 + 4x^2$$

なる形であることが必要である。 p の原始根 g に対して 1, g 及び g^3 に対応する 6 乗剰余の合併として D が得られる。本質的にはこれで凡てが盡くされる。

[注] 1° は昔昔からの結果である。2° も発見者は多いがたとえば S. Chowla. 3° は E. Lehmer, 5° は M. Hall に負う。4° は A. L. Whiteman に依るが、このあたりになると計算がひどく大変で、電子計算機にでもよう外はない。 e が大きくなると等差集合の複雑さが急激に増すことの一つの現われというべきである。

4. 計算のもととなる主要定理.

指数 e が与えられた時、法 p の等差集合 D の存在するような素数 p を有限の形で求めるのに筆者は次の定理を証明した.

$p = ef + 1$, $f \equiv 1 \pmod{2}$ とし, 1 の e 等分体における p の素イデアル因子 $\mathfrak{p}$ を固定し, 法 p の e 乗剰余指標 χ を

$$\chi(x) \equiv x^{(p-1)/e} \pmod{\mathfrak{p}}$$

のように定める. 1 の e 乗根 s 個をえらんで作られる集合 B に対して

$$\chi(x) \in B$$

なる $x \pmod{p}$ の全体を E とすると, $D = E$ 又は $D = E \cup \{0\}$ が等差集合と作るための必要十分条件として

$$(2) \quad s(sf + 2d - 1) \equiv 0 \pmod{e}$$

及び

$$(3) \quad 2(s - de)K_\nu + \sum_{\mu=1}^{\nu-1} (-1)^\mu \pi(\chi^\mu, \chi^{\nu-\mu}) K_\mu K_{\nu-\mu} \equiv 0 \pmod{\mathfrak{p}}$$

$$(\nu = 2, 4, \dots, e-2)$$

がある. d は $D \ni 0$ の時 1 , $D \not\ni 0$ の時 0 を表わす数とする. K_ν は B に属する数の ν 乗の和であり $\pi(\chi_1, \chi_2)$ は Jacobi の和である;

$$\pi(\chi_1, \chi_2) = - \sum_{x+y \equiv 1 \pmod{p}} \chi_1(x) \chi_2(y).$$

古典的結果 (§3 の 1° 乃至 5°) において $\mathfrak{p}$ の形が問題になる

のは、円周等分論における Jacobi の和の現出するところにその原因がある。

5. 数値計算.

$e=10$ 及び $e=12$ に対しては筆者が計算様式を指示して所期の目的を達することができたが、 $e=14$ の場合には、単に依頼するに止まり、プログラムのための技術面で数年間にわたって進展がない。ここではその大要を説明する。

A. 法 14 の剰余の部分集合を §2 の意味の 1 次変換群のもとにおいて同値類に分け、各類の代表を決定すること。

(この程度ならば手でもできる。実際 145 個の類がある。)

B. 以下 34 個の量は円周 7 等分体における整数であるが、これらを用いて 7 次元のベクトルとして書き表わす。ベクトル

$$\mathbf{a} = (a_0, a_1, a_2, a_3, a_4, a_5, a_6)$$

$$\mathbf{b} = (b_0, b_1, b_2, b_3, b_4, b_5, b_6)$$

の和及びスカラー倍を例の如くに定義し、その積は

$$\mathbf{ab} = \mathbf{c} = (c_0, c_1, c_2, c_3, c_4, c_5, c_6)$$

$$c_i = \sum_{j=0}^6 a_j b_{i-j} \quad (i=0, 1, 2, 3, 4, 5, 6)$$

で定義する。ただし b の添数は法 7 で取るものとする。

34 個の量

$$E, K_i \quad (i=1, \dots, 12)$$

$$L_i, M_i, N_i \quad (i=0, 1, \dots, 6)$$

$$P, Q, R$$

は凡てベクトルで、**A** で作られた列 $\alpha_1, \dots, \alpha_n$ によって次のように作られるべきものとする。

$$E = (0, 1, 0, 0, 0, 0, 0),$$

$$K_i = \sum_{\nu=1}^n (-E)^{i\alpha_\nu} \quad (i=1, 2, \dots, 12).$$

$(-E)^m$ は $m \pmod{14}$ で決まるので $i\alpha_\nu$ は その法 14 の剰余をもって、予め置き換えておくものとする。

$$L_0 = -2K_2^4 K_3^2 K_6 - 4K_1^3 K_2 K_3 K_4 K_8,$$

$$L_1 = 8K_1 K_2^3 K_3 K_4 K_6 + 2K_1^4 K_4^2 K_8,$$

$$L_2 = -5K_1^2 K_2^2 K_4^2 K_6,$$

$$L_3 = -2K_1 K_2^3 K_3^2 K_7 - 2K_2^3 K_3^3 K_5,$$

$$L_4 = 8K_1^2 K_2^2 K_3 K_4 K_7 + 8K_1 K_2^2 K_3^2 K_4 K_5,$$

$$L_5 = -4K_1^3 K_2 K_4^2 K_7 - 8K_1^2 K_2 K_3 K_4^2 K_5,$$

$$L_6 = 2K_1^3 K_4^3 K_5 + K_1^2 K_2^2 K_3^2 K_8,$$

$$M_0 = -4K_2^4 K_4^2 K_6^2 + 2K_1 K_2^3 K_3^2 K_7 K_8 + 2K_2^3 K_3^3 K_5 K_8 - 2K_1 K_2 K_3 K_4^3 K_5^2,$$

$$M_1 = 2K_1^3 K_2^2 K_4 K_8 K_9 + 2K_1^2 K_2^2 K_3 K_4 K_7 K_8 + K_1^2 K_4^4 K_5^2,$$

$$M_2 = -4K_1 K_2^4 K_4 K_6 K_9 - 4K_2^4 K_3 K_4 K_6 K_7 + 4K_1^2 K_2 K_3 K_4^2 K_5 K_8,$$

$$M_3 = -4K_1 K_2^3 K_4^2 K_6 K_7 - 4K_2^3 K_3 K_4^2 K_5 K_6 - 2K_1^3 K_4^3 K_5 K_8 - K_1^2 K_2^2 K_3^2 K_8^2,$$

$$M_4 = 2 K_2^4 K_3^2 K_6 K_8,$$

$$M_5 = -4 K_1^2 K_2^3 K_4 K_7 K_9 - 4 K_1 K_2^3 K_3 K_4 K_7^2 - 4 K_1 K_2^3 K_3 K_4 K_5 K_9 - 4 K_2^3 K_3^2 K_4 K_5 K_7,$$

$$M_6 = -K_1^2 K_2^2 K_4^3 K_{10} + 3 K_1^2 K_2^2 K_4^2 K_6 K_8,$$

$$N_0 = 2 K_1^3 K_2 K_4^3 K_{11} + 2 K_1^2 K_2 K_4^3 K_5 K_7 + 2 K_1^2 K_2^3 K_3 K_8 K_9 + K_2^4 K_4^2 K_6^2 \\ + 2 K_1 K_2^3 K_3^2 K_7 K_8 + 2 K_2^3 K_3^3 K_5 K_8,$$

$$N_1 = -4 K_2^5 K_3 K_6 K_9,$$

$$N_2 = 4 K_1^2 K_2 K_3 K_4^2 K_5 K_8,$$

$$N_3 = -2 K_1^3 K_4^3 K_5 K_8 - K_1^2 K_2^2 K_3^2 K_8^2,$$

$$N_4 = -4 K_1 K_2^4 K_3 K_7 K_9 - 4 K_2^4 K_3^2 K_5 K_9,$$

$$N_5 = -4 K_1 K_2^3 K_3 K_4^2 K_{10},$$

$$N_6 = -K_1^2 K_2^3 K_4^2 K_{12} - 4 K_1^2 K_2^2 K_3 K_4^2 K_{11} + 2 K_1^2 K_2^2 K_4^3 K_{10} - 4 K_1 K_2^2 K_3 K_4^2 K_5 K_7 \\ + K_1^2 K_2^2 K_4^2 K_6 K_8.$$

L_i ($i=0, 1, 2, 3, 4, 5, 6$) 等は 7 次元ベクトルなので 7×7 の行列 L, M, N が与えられることになる。これらは **A** から取り出されたデータ $\alpha_1, \dots, \alpha_n$ にのみ依存する。

次に P, Q, R はパラメータ s にも関係する。

s を順次 $0, 1, 2, 3, 4, 5, 6$ として

$$P = \sum_{i=0}^6 E^{s_i} L_i,$$

$$Q = \sum_{i=0}^6 E^{s_i} M_i,$$

$$R = \sum_{i=0}^6 E^{si} N_i$$

を定める。

C. 次の段階は円周7等分体の整数 P, Q, R の絶対ノルムの計算である。3次の実部分体を仲介として相対ノルムの絶対ノルムとして計算を実行する。 S_2 及び S_3 はそれぞれ Q, R からノルム演算でえられるから、ここでは P からその絶対ノルム S_1 を得る操作を記述することにする。

$$P = (p_0, p_1, p_2, p_3, p_4, p_5, p_6)$$

から

$$a_i = p_i - p_0 \quad (i=1, 2, 3, 4, 5, 6),$$

$$f_1 = a_1 + a_6, f_2 = a_2 + a_5, f_3 = a_4 + a_3,$$

$$g_1 = a_1 - a_6, g_2 = a_2 - a_5, g_3 = a_4 - a_3,$$

$$h_1 = a_1 a_2 + a_2 a_3 + a_3 a_4 + a_4 a_5 + a_5 a_6 + a_6 a_1,$$

$$h_2 = a_2 a_4 + a_4 a_6 + a_6 a_1 + a_1 a_3 + a_3 a_5 + a_5 a_2,$$

$$h_4 = a_4 a_1 + a_1 a_5 + a_5 a_2 + a_2 a_6 + a_6 a_3 + a_3 a_4$$

なる量 $f_1, f_2, f_4, g_1, g_2, g_4, h_1, h_2, h_4$ を定め、さらに

$$\begin{aligned} 12t = & (f_1 + f_2 + f_4)^2 + 7(g_1 + g_2 + g_4)^2 \\ & + 14(f_1^2 + f_2^2 + f_4^2 - f_1 f_2 - f_2 f_4 - f_4 f_1 \\ & + g_1^2 + g_2^2 + g_4^2 - g_1 g_2 - g_2 g_4 - g_4 g_1) \end{aligned}$$

と置く。右辺は 12 の倍数であるから、整数 t が定まる。また

$$x = 2h_1 - h_2 - h_4,$$

$$y = 2h_2 - h_4 - h_1,$$

$$z = 2h_4 - h_1 - h_2$$

と置き

$$27\zeta_1 = t^3 + 7t(xy + xz + yz) + 7(x^2y + y^2z + z^2x + 2xyz)$$

とする。右辺は必ず 27 の倍数で、上式から正・整数 ζ_1 が求められる。

D. $\zeta_1, \zeta_2, \zeta_3$ の最大公約数 δ を求める。

E. $\delta = 0$ であるかないかが才 1 の要点である。 $\delta = 0$ である
と新しい等差集合の生ずる可能性がある。 $\delta \neq 0$ であるとき
それは“例外的な”等差集合を与えるにすぎない。しかし
 $\delta \neq 0$ ならば δ を 8 で割れるだけ割り、その商を 7 で割れる
だけ割って、その最後の商を δ_0 とする。

$\delta_0 = 1$ ならばそのままよいが、 $\delta_0 > 1$ ならば、それを

$$14k+1 \quad (k=2, 3, \dots)$$

の形の因数に分解する。

以上で計算を終り、 $\delta = 0$ か否か、 $\delta > 0$ ならば δ_0 及び
その因数を出力させる。

6. 計算の規模の推定.

以下大ざっぱに推定をしてみると, 行列 L, M, N の成分は絶対値において $\leq 10^4$ であろう. P, Q, R のノルム S_1, S_2, S_3 は (正であって) $\leq 10^{40}$ と推定される. $\delta \neq 0$ の時の δ_0 は最も把握し難い量だが $145 \times 7 = 1015$ の場合のうち 90% までは -1 になるものと思われる. 最悪の場合 $\delta_0 > 1$ であっても $\delta_0 \leq 10^{20}$ ぐらいで, δ_0 を完全に分解するのに莫大な時間がかかるようだったら, それは途中までに止めなければならぬ.

手で計算してみると, 最初のデータ系列が 0 の場合

$$s=0: \quad S_1=64, \quad S_2=1911 \ 02976, \quad S_3=2 \ 62144.$$

$$s \geq 1: \quad S_1=307 \ 06649, \quad S_2=322 \ 68853, \quad S_3=99 \ 98311$$

で $\delta_0=1$ がえられる.

なお比較の為に言えば $e=12$ の際, データ 0 の場合のノルムの最大値 5 桁, 一般の場合のノルムの最大値は 12 桁であるが, 問題の拡大体の次数が $e=12$ の際の 4 に対して $e=14$ では 6 になっているので, S_1, S_2, S_3 の最大値を

$$\frac{10}{5} \times 12 \times \frac{6}{4} = 36 \text{ 桁} \text{ と推定するのである.}$$

以上

文献

L.D. Baumert : Cyclic difference sets, *Lecture Notes in Mathematics*, vol. 182, 1971.

K. Yamamoto : On Jacobi sums and difference sets, *J. Combinatorial Theory*, vol. 3 (1967), pp.146-181