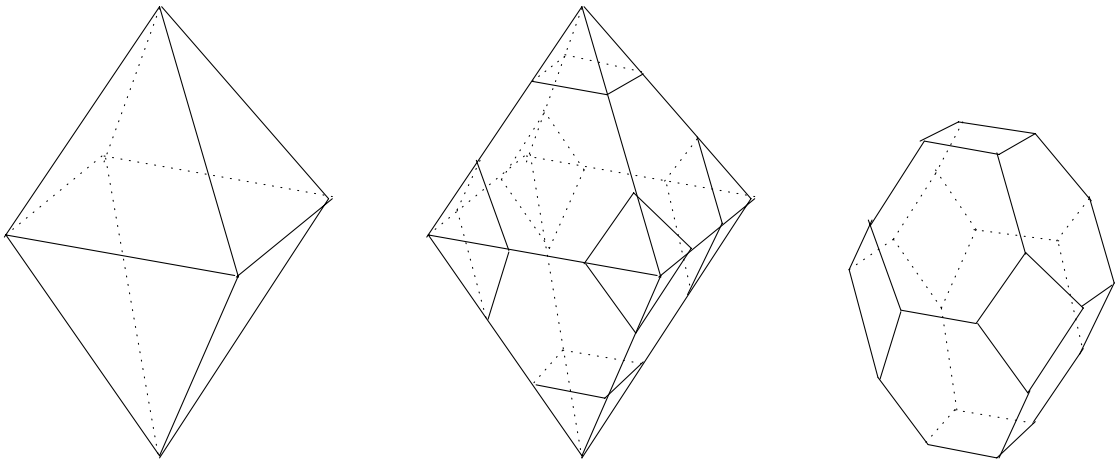
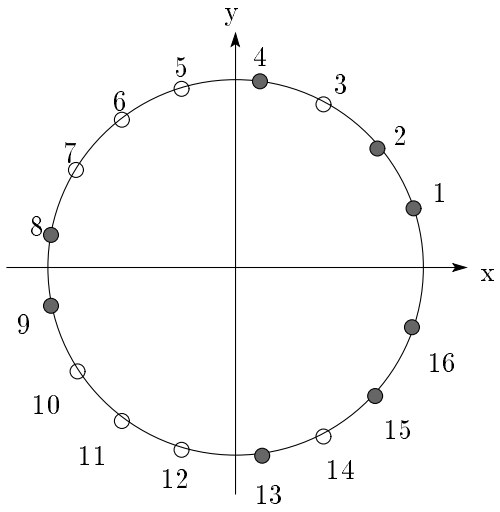
数学のメモ



（「数学　，Ａの指導メモ」，
「数学　，Ｃの周辺についてのメモ」に追加して）

富山県立砺波高等学校

片山　喜美



はじめに

富山県高等学校教育研究会数学部会の発表のため，平成８年度に「数学　，Aの指導メモ」，平成１０年度に「数学　，Cの周辺についてのメモ」をまとめた．それらに含めなかったもの，その後にメモしておいたものをこの時点（２００１年夏）で一度まとめておくことにする．平成１３年度全国理数科教育研究大会の発表原稿に含めた数学の内容で、詳しく説明したものを用意しておく必要もあったので、その他のものとあわせて打ち込んでおいた。

最近は、授業や課題研究に使うエネルギーよりも、分掌の様々な事務的な仕事につかう時間が多くなってきた。そのため、なかなか数学書を読んだり、数学の問題を考えたりする時間が少なくなってしまっている。たまに何かに取り組んだりしても、細切れになり、継続が難しい。今後、これまでのように「メモ」をするくらいに数学を考えられるか少し不安もある。

今回の TeX 打ち込みでは $ams-tex$ を使って可換図式を作成すること、数式の split、ghostscript,dviout の設定による写真の張り込みなどわずかながらも技術を向上させることができた。また、この原稿およびこれまでの発表原稿を自分のホームページに載せるため、TeX からポストスクリプト、さらにＰＤＦのファイルへ変換する作業にも初めて取り組んだ。今後の課題として、emath シリーズが持つ相当な機能を何かの機会に是非マスターしたいものである。　なお，砺波高校数学科の先生方には，日頃からの助言など大変お世話になったことを感謝します.

富山県立砺波高等学校
教諭　　片　山　喜　美
E－mail　ja9nfo@p1.coralnet.or.jp
もしくは ja9nfo@nifty.ne.jp
te6449@tym.ed.jp

目 次

第1章　算数オリンピックのある問題から

平成１１年度の算数オリンピックに次のような問題があった.
「１から順にふえていく整数の列の中には，たとえば１から３までの場合は，１＋２＝３，１から２０までの場合には，１＋２＋３＋ ···· ＋１４＝１５＋１６＋１７＋ ···· ＋２０のように順序を変えないまま，途中でうまく２つのグループに分けて，各グループの数の和を等しくできるものがあります．このような整数の列のうち，上の例以外で，もっとも短いものは１からいくつまででですか.」

この問題は Nifty の数学の会議室で話題になった．少し考えてみると，２次形式を用いて解決することができ，以前課題研究で扱ったピタゴラス数 $x^2+y^2=z^2,\quad |x-y|=1$ と関わりがあることがわかった.

1.1　２次形式を用いた解法

$1+2+3+\cdots\cdots+k=(k+1)+(k+2)+\cdots\cdots+n$　とすると，
$\frac{1}{2}n(n+1)=2\times\frac{1}{2}k(k+1)$
さらに変形して
$(2n+1)^2-2(2k+1)^2=-1$
$X=2n+1, Y=2k+1$　とおくと，２次形式　$X^2-2Y^2=-1$　を解く問題となる.
これについては以前課題研究[1]で生徒が発見した漸化式が正しいことを証明する際に現れたものである．そのときの経過は，平成１０年度高教研発表資料「数学　，Cとその周辺についてのメモ」第４章　ある種のピタゴラス数と２次形式　に書いてあるが，それによると
$X^2-2Y^2=-1$　の自然数解の列は，最小解　$(X_0,Y_0)=(1,1)$
一般解　$\begin{pmatrix} X_n \\ Y_n \end{pmatrix}=\begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}^n\begin{pmatrix} X_0 \\ Y_0 \end{pmatrix}$
で与えられる.
$X_0=1, Y_0=1$　のときは，$n=k=0$　となり，この場合は $0=0$ という解となり，意味をなさない.

$$\begin{pmatrix} X_1 \\ Y_1 \end{pmatrix}=\begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix}=\begin{pmatrix} 7 \\ 5 \end{pmatrix}\qquad \therefore n=3,\ k=2,$$

$1+2=3$

[1] 平成９年度課題研究　「ピタゴラス数」

$$\begin{pmatrix} X_2 \\ Y_2 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 7 \\ 5 \end{pmatrix} = \begin{pmatrix} 41 \\ 29 \end{pmatrix} \qquad \therefore n = 20,\ k = 14,$$

$1 + 2 + \cdots + 14 = 15 + 16 + \cdots + 20$

$$\begin{pmatrix} X_3 \\ Y_3 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 41 \\ 29 \end{pmatrix} = \begin{pmatrix} 239 \\ 169 \end{pmatrix} \qquad \therefore n = 119,\ k = 84,$$

$1 + 2 + \cdots + 84 = 85 + 86 + \cdots + 119$

これが算数オリンピックの解答となる.

$$\begin{pmatrix} X_4 \\ Y_4 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 239 \\ 169 \end{pmatrix} = \begin{pmatrix} 1393 \\ 985 \end{pmatrix} \qquad \therefore n = 696,\ k = 496,$$

$1 + 2 + \cdots + 496 = 497 + 498 + \cdots + 696$

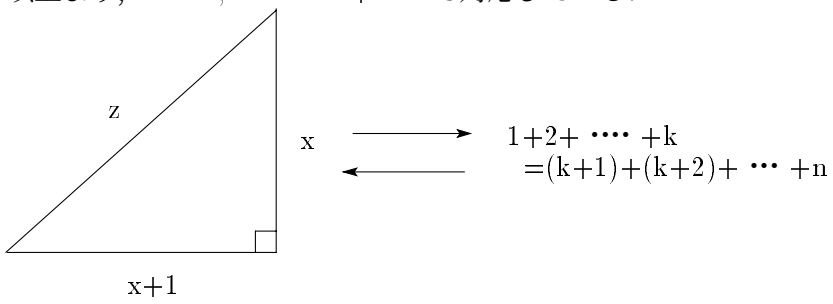
以下，いくらでも作ることができる．ただし，急激に大きな数となる.

1.2 ピタゴラス数 $x^2 + y^2 = z^2, \qquad y = x + 1$ との関係

1. $x^2 + y^2 = z^2, \qquad y = x + 1$ の解は，$X^2 - 2Y^2 = -1$ の解から，$X = 2x + 1, \quad Y = z$ として得られる.

2. $1 + 2 + \cdots + k = (k + 1) + (k + 2) + \cdots + n$ の解は，$X^2 - 2Y^2 = -1$ の解から，$X = 2n + 1, \quad Y = 2k + 1$ として得られる.

以上より，$x = n, \quad z = 2k + 1$ で対応している.



2 次形式は，結構身近なところに応用できて面白いものだ.（Aug.31,1999）

第2章　アミダくじについて

ある大学の数学科の推薦入試の事前課題に「アミダくじを用いるとどのような並び替えも作成可能であることを説明せよ.」という問題が与えられた．他校へ転勤した先生から相談されたので少し考えてみた.

定理 2.1 アミダくじによって $1, \cdots, n$ の任意の並び替えが作成可能である.

1. 高校生向けの証明 ···· 数学的帰納法

(a) $n = 1$ の時は自明.

(b) n の時に正しいと仮定する． $n+1$ の時,

(i) $n+1$ を動かさない並び替えについては，帰納法の仮定から作成可能.

(ii) $k \leq n$ なる k が $n+1$ に移る並び替えについて，以下の図のアミダを考える.

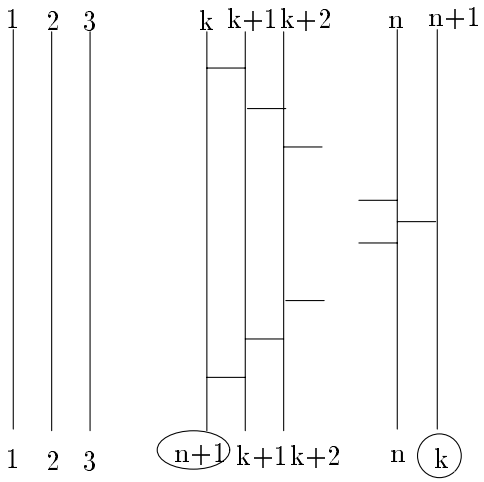


図 2.1:

このアミダによって k と $n+1$ が入れ替わり，残りの数字は自分の場所に来る．従って，k は望み通りの場所に移った．このアミダの下に， 右端を除いた n 個の数で，求める並び替えのアミダを追加すればよいが，それは帰納法の仮定から可能である．以上により $n+1$ の場合も任意の並び替えが可能である.

(iii) 以上により，全ての n についてアミダは任意の並び替えを作成することが出来る．//

2. 置換群の知識によって

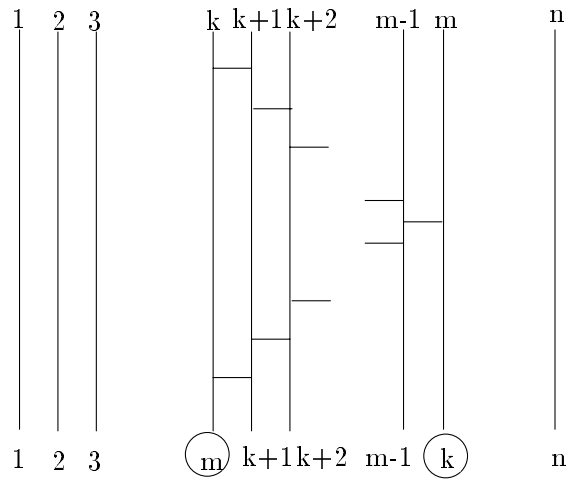


図 2.2:

上図のアミダは k と m の互換を表す．全ての置換は互換によって生成されるので，アミダによって全ての並び替えが可能であるといえる．//

第3章　ユークリッドの互除法が終了するまでの計算回数について

ユークリッドの互除法については、平成４年度の課題研究「数の性質（最大公約数・互除法・連分数）」で、基本的な手法を取り扱った．その後、富山大学教育学部へ進学した教え子から，ユークリッドの互除法が終了するまでにどれだけの計算回数が必要かという問題について相談されたので考えてみた．[1]

3.1　ユークリッドの互除法

$a > b > 0$ を２つの自然数とするとき，その最大公約数を求めるアルゴリズムの１つとして，以下の方法をユークリッドの互除法という．

- $a = q_1 b + r_1, \quad q_1 \in \mathbb{N}, \quad r_1 \in \mathbb{Z}, \quad 0 \leq r_1 < b$
- もし，$r_1 > 0$ ならば続ける．
  $b = q_2 r_1 + r_2, \quad q_2 \in \mathbb{N}, \quad r_2 \in \mathbb{Z}, \quad 0 \leq r_2 < r_1$
- 以降，$r_k > 0$ ならば続ける．
  $r_{k-1} = q_{k+1} r_k + r_{k+1}, \quad q_{k+1} \in \mathbb{N}, \quad r_{k+1} \in \mathbb{Z}, \quad 0 \leq r_{k+1} < r_k$
- $b > r_1 > r_2 > \cdots$ は減少する非負整数の列であるから，$^{\exists}n \quad s.t. \quad r_{n+1} = 0$ ．ここで計算をストップさせる．

命題 ***3.1*** $(a, b) = r_n$ である．

補題 ***3.1*** $(a, b) = (a - qb, b) \qquad (q \in \mathbb{N})$
証明）$(a, b) = d$, $(a - qb, b) = d_1$ とおく．
$d|a$, $d|b$ より，$d|a - qb$.　　よって $d \leq d_1$
$d_1|a - qb$, $d_1|b$ より，$d_1|(a - qb) + qb = a$.　　よって $d_1 \leq d$
以上より，$d = d_1$　　//
この補題により，$(a, b) = (a - q_1 b, b) = (r_1, b)$
同様にして，$(r_1, b) = (r_1, b - q_2 r_1) = (r_1, r_2)$
繰り返して，$(a, b) = (r_1, b) = (r_1, r_2) = (r_3, r_2) = \cdots = (r_{n-1}, r_n)$
作り方 $(r_{n+1} = 0)$により，$r_{n-1} = q_{n+1} r_n$．従って，$(r_{n-1}, r_n) = r_n$．すなわち，$(a, b) = r_n$ と結論できる．以上により命題が証明された．

実際に計算してみる．$a = 332, b = 87$ のとき，$332 = 3 \times 87 + 71, \qquad 87 = 1 \times 71 + 16, \qquad 71 = 4 \times 16 + 7, \qquad 16 = 2 \times 7 + 2, \qquad 7 = 3 \times 2 + 1, \qquad 2 = 2 \times 1 + 0$．従って，$(332, 87) = 1$

[1] 1997 年５月

3.2　互除法が終了するまでの計算回数

$a > b > 0$ を２つの自然数とするとき、互除法により、$a, b, r_1, r_2, \cdots\cdots, r_n = d$（$d = (a, b)$　最大公約数）と剰余の列を作っていく．このとき，b を固定して，a をいろいろ変えていったとき，互除法の列の長さの最大値を b に対する互除法の計算回数と定義し，$N(b)$ と表す．a の値をいろいろ取るとしても，$r_1 = 0, \cdots b-1$ であるから，これらの r_1 で考えれば十分である．b の値に対して，計算回数 $N(b)$ はどのくらいであると見積もることができるであろうか？それが問題である．

主張 ***3.1*** $b < 2^{k+1}$ ならば $N(b) \leq 2k$

証明）$b = q_1 r_1 + r_2 \geq r_1 + r_2 > 2r_2$ であるから，$r_2 < \dfrac{1}{2}b$

同様に，$r_{i+2} < \dfrac{1}{2}r_i$．従って，$r_{2k} < \left(\dfrac{1}{2}\right)^k b.$

$b < 2^{k+1}$ とすると，$r_{2k} < 2$．従って，$r_{2k} = 1$ もしくは，その前に計算は終了している．よって，主張は証明された．

しかし，この主張は少々荒く，ベストな評価とは遠い．$b = 17$ について考えてみる．

$17, 2, 1$	$17, 6, 5, 1$	$17, 10, 7, 3, 1$	$17, 14, 3, 2, 1$
$17, 3, 2, 1$	$17, 7, 3, 1$	$17, 11, 6, 5, 1$	$17, 15, 2, 1$
$17, 4, 1$	$17, 8, 1$	$17, 12, 5, 2, 1$	$17, 16, 1$
$17, 5, 2, 1$	$17, 9, 8, 1$	$17, 13, 4, 1$	

従って，$N(17) = 4$．しかし，$2^4 < 17 < 2^5$ であるから，上の主張では $N(17) \leq 8$ としか言えていない．

そこで，$N(b)$　$(b = 2, 3, 4, \cdots)$ について，計算してみる.（最後の表を参照のこと）注目すべきは，計算回数の最高記録が出る b の値で，

$1, 2, 3, 5, 8, 13, 21, 34, \cdots$

となっている．これは，$f_1 = 1, f_2 = 2,\quad f_{n+2} = f_{n+1} + f_n$ で定められるフィボナッチ数列である．このことは，以下の理由からも予想できた．

$N(b)$ を筆算で計算していくとき，$b, r_1, r_2, r_3, \cdots$ と並べてみると，急に数が小さくなるところがある．それは，$r_k = q_{k+2} r_{k+1} + r_{k+2}$ と次の剰余に移るときに q_{k+2} が大きいときに起こる．そうなると列の長さが短くなってしまうのである．逆に，q_{k+2} が小さいと数の減少が小さく，列が長くなると考えられる．$q_{k+2} = 1$ とすると，$r_{k+2} = r_{k+1} + r_k$ となり，フィボナッチ数列が現れる．さらに，初項と第２項が最小の $1, 2$ とすると最高記録を更新する数 b が得られる．

主張 ***3.2*** $\{f_l\}$ を　$f_1 = 1, f_2 = 2,\quad f_{l+2} = f_{l+1} + f_l$ で定められるフィボナッチ数列であるとする．

このとき，

- $f_l < b < f_{l+1} \quad \Longrightarrow \quad N(b) < l$
- $N(f_{l+1}) = l$

証明）

1. $f_l < b < f_{l+1} \quad \Longrightarrow \quad N(b) < l$ について
   数学的帰納法で証明する．
   $b < a_l$ を満たす b について $N(b) < l-2$ が成立していると仮定する．このとき，
   $a_l < b < a_{l+1} = a_l + a_{l-1}$ なる b について，

   (a) $0 < r_1 < a_l$ のとき，
   $r_1, r_2, \cdots, r_n$ について，r_1 を起点とした列を考えると，帰納法の仮定から $r_2, \cdots, r_n$ の長さは $l-2$ 未満．従って，$n < l-1$ //

   (b) $a_l \leq r_1 < b$ のとき
   $0 \leq b - r_1 \leq b - a_l < (a_l + a_{l-1}) - a_l = a_{l-1}$
   従って，$r_2 = b - r_1 < a_{l-1}$．このとき，r_2 を起点とした列に帰納法の仮定を用いると，その長さは $l-3$ 未満．よって，$r_1, r_2, r_3, \cdots, r_n$ の長さは $l-1$ 未満．//

2. $N(f_{l+1}) = l$ について
   $f_{l+1} < f_{l+2}$ より，上記で示したことから $N(f_{l+1}) < l+1$
   一方，$f_{l+1}, f_l, f_{l-1}, \cdots, f_2, f_1$ という列を持つから $N(f_{l+1}) \geq l$
   以上より，$N(f_{l+1}) = l$ //

課題

この主張により，計算回数 $N(b)$ の上限は定められた．しかし，下限はどうであろうか？徐々に計算回数は多くなっていく．大きな数なのに計算回数が少ないという特異な数は無いように思われる．表から見ると，$b < c \quad \Longrightarrow \quad N(b) < N(c)$ を満たす b を抜き出すと，$1, 2, 6, 10, 24, \cdots$ ．これらの数の規則性は？あるいは，別の方法で下限は見積もれるであろうか？

3.3 資料

3.3.1 資料．計算回数を求める function

$N(b)$ を求めて，TEX の表になるようなテキストを吐き出す簡単なプログラムを作成したが，そこで用いた $N(b)$ を計算する $function$ の部分を以下に記す．都合により，$N(b)$ の代わりに $EuN(b)$ としてある．

```
Function EuN(b)
    Dim k As Integer, n As Integer, l As Integer
    Dim r As Integer, s As Integer

    EuN = 1
    For k = 2 To b - 1
        r = b: s = k: n = 0
        Do While s > 0
            l = r Mod s
            r = s: s = l: n = n + 1
        Loop
    If n > EuN Then
        EuN = n
    End If
    Next k

End Function
```

3.3.2 資料．$N(b)$ の一覧

b	$N(b)$	b	$N(b)$	b	$N(b)$	b	$N(b)$	b	$N(b)$
1	0	21	6	41	6	61	6	81	8
2	1	22	4	42	6	62	6	82	7
3	2	23	5	43	6	63	6	83	7
4	2	24	4	44	6	64	7	84	6
5	3	25	5	45	6	65	7	85	7
6	2	26	5	46	6	66	7	86	7
7	3	27	5	47	7	67	7	87	7
8	4	28	5	48	6	68	7	88	7
9	3	29	6	49	7	69	7	89	9
10	3	30	6	50	7	70	6	90	6
11	4	31	6	51	6	71	7	91	7
12	4	32	5	52	6	72	6	92	7
13	5	33	5	53	6	73	7	93	7
14	4	34	7	54	5	74	7	94	7
15	4	35	5	55	8	75	7	95	7
16	4	36	5	56	6	76	8	96	6
17	4	37	6	57	6	77	6	97	8
18	5	38	5	58	6	78	6	98	7
19	5	39	6	59	6	79	8	99	7
20	4	40	6	60	7	80	8	100	7

b	$N(b)$	b	$N(b)$	b	$N(b)$	b	$N(b)$	b	$N(b)$
101	7	121	8	141	7	161	8	181	9
102	7	122	7	142	8	162	8	182	7
103	8	123	9	143	8	163	8	183	9
104	7	124	7	144	10	164	7	184	8
105	8	125	7	145	8	165	8	185	9
106	7	126	7	146	8	166	8	186	9
107	8	127	8	147	7	167	9	187	9
108	8	128	9	148	8	168	8	188	9
109	8	129	9	149	8	169	9	189	8
110	8	130	8	150	7	170	9	190	8
111	8	131	9	151	8	171	8	191	9
112	8	132	7	152	8	172	8	192	9
113	7	133	8	153	8	173	9	193	9
114	7	134	8	154	8	174	8	194	9
115	8	135	7	155	8	175	9	195	8
116	8	136	7	156	7	176	8	196	9
117	8	137	8	157	9	177	9	197	8
118	8	138	7	158	8	178	9	198	8
119	8	139	8	159	8	179	9	199	10
120	7	140	8	160	8	180	8	200	7

b	$N(b)$	b	$N(b)$	b	$N(b)$	b	$N(b)$	b	$N(b)$
201	8	221	8	241	9	261	9	281	9
202	8	222	9	242	9	262	9	282	9
203	8	223	8	243	9	263	9	283	10
204	8	224	8	244	8	264	9	284	9
205	8	225	9	245	9	265	9	285	9
206	9	226	9	246	9	266	9	286	10
207	10	227	9	247	9	267	9	287	10
208	10	228	8	248	9	268	8	288	10
209	10	229	9	249	9	269	9	289	10
210	8	230	8	250	9	270	10	290	10
211	8	231	9	251	9	271	9	291	9
212	10	232	8	252	8	272	10	292	9
213	8	233	11	253	9	273	9	293	10
214	8	234	8	254	10	274	10	294	8
215	9	235	9	255	9	275	10	295	10
216	8	236	8	256	9	276	9	296	9
217	9	237	9	257	9	277	9	297	10
218	8	238	9	258	9	278	8	298	8
219	8	239	9	259	9	279	9	299	10
220	8	240	8	260	8	280	10	300	8

b	$N(b)$	b	$N(b)$	b	$N(b)$	b	$N(b)$	b	$N(b)$
301	10	321	9	341	9	361	9	381	10
302	10	322	11	342	9	362	9	382	10
303	10	323	9	343	11	363	9	383	10
304	8	324	9	344	9	364	10	384	9
305	10	325	9	345	9	365	10	385	9
306	8	326	9	346	9	366	10	386	9
307	10	327	9	347	9	367	10	387	10
308	10	328	9	348	10	368	9	388	9
309	10	329	9	349	9	369	10	389	10
310	8	330	8	350	9	370	9	390	10
311	10	331	9	351	10	371	10	391	10
312	10	332	9	352	9	372	9	392	9
313	10	333	10	353	9	373	10	393	9
314	9	334	9	354	9	374	10	394	10
315	9	335	11	355	9	375	10	395	10
316	9	336	10	356	9	376	9	396	10
317	10	337	11	357	9	377	12	397	10
318	9	338	11	358	9	378	9	398	10
319	8	339	10	359	10	379	10	399	9
320	9	340	9	360	9	380	9	400	10

b	$N(b)$	b	$N(b)$	b	$N(b)$	b	$N(b)$	b	$N(b)$
401	10	421	9	441	11	461	9	481	10
402	10	422	10	442	8	462	10	482	11
403	10	423	9	443	11	463	11	483	9
404	10	424	10	444	10	464	10	484	10
405	10	425	10	445	11	465	11	485	11
406	10	426	10	446	10	466	11	486	9
407	10	427	10	447	9	467	11	487	11
408	10	428	9	448	10	468	10	488	10
409	9	429	9	449	10	469	11	489	9
410	9	430	10	450	9	470	9	490	11
411	11	431	10	451	10	471	10	491	10
412	10	432	10	452	10	472	10	492	10
413	10	433	10	453	11	473	10	493	11
414	10	434	10	454	9	474	11	494	10
415	10	435	10	455	10	475	9	495	11
416	10	436	10	456	10	476	10	496	10
417	10	437	11	457	10	477	10	497	10
418	10	438	10	458	11	478	11	498	11
419	10	439	9	459	10	479	10	499	11
420	9	440	9	460	10	480	9	500	11

b	$N(b)$	b	$N(b)$	b	$N(b)$	b	$N(b)$	b	$N(b)$
501	10	521	12	541	10	561	10	581	11
502	9	522	10	542	12	562	10	582	9
503	11	523	10	543	10	563	11	583	10
504	10	524	10	544	10	564	9	584	10
505	11	525	9	545	12	565	10	585	10
506	9	526	10	546	12	566	10	586	10
507	11	527	10	547	12	567	10	587	10
508	10	528	10	548	11	568	11	588	10
509	9	529	10	549	10	569	10	589	11
510	9	530	10	550	10	570	9	590	10
511	10	531	10	551	10	571	10	591	11
512	10	532	9	552	10	572	10	592	10
513	11	533	10	553	9	573	10	593	11
514	10	534	10	554	9	574	10	594	11
515	10	535	10	555	12	575	10	595	11
516	9	536	10	556	10	576	10	596	11
517	10	537	10	557	10	577	10	597	10
518	9	538	9	558	9	578	10	598	10
519	10	539	11	559	10	579	10	599	10
520	10	540	10	560	10	580	10	600	11

b	$N(b)$	b	$N(b)$	b	$N(b)$	b	$N(b)$	b	$N(b)$
601	10	621	11	641	11	661	11	681	10
602	10	622	10	642	11	662	10	682	10
603	10	623	10	643	11	663	11	683	11
604	11	624	10	644	11	664	10	684	11
605	11	625	10	645	10	665	12	685	10
606	10	626	11	646	10	666	11	686	11
607	10	627	11	647	11	667	11	687	10
608	11	628	10	648	11	668	11	688	10
609	10	629	11	649	11	669	11	689	11
610	13	630	9	650	9	670	11	690	11
611	10	631	11	651	11	671	11	691	11
612	11	632	11	652	11	672	11	692	10
613	10	633	11	653	11	673	11	693	10
614	10	634	10	654	10	674	11	694	10
615	10	635	11	655	11	675	10	695	11
616	11	636	10	656	10	676	11	696	10
617	10	637	11	657	10	677	11	697	11
618	10	638	10	658	11	678	11	698	11
619	11	639	11	659	11	679	10	699	11
620	10	640	10	660	10	680	10	700	11

b	$N(b)$	b	$N(b)$	b	$N(b)$	b	$N(b)$	b	$N(b)$
701	11	721	11	741	12	761	10	781	12
702	11	722	11	742	10	762	10	782	12
703	11	723	10	743	11	763	11	783	11
704	11	724	11	744	10	764	11	784	11
705	10	725	11	745	11	765	11	785	11
706	10	726	10	746	10	766	10	786	10
707	12	727	11	747	11	767	12	787	12
708	11	728	10	748	10	768	10	788	12
709	11	729	10	749	12	769	10	789	12
710	10	730	11	750	11	770	11	790	10
711	10	731	11	751	11	771	11	791	11
712	10	732	11	752	12	772	11	792	12
713	12	733	12	753	12	773	12	793	12
714	11	734	11	754	12	774	10	794	11
715	12	735	10	755	12	775	11	795	12
716	10	736	11	756	12	776	11	796	10
717	12	737	11	757	11	777	12	797	10
718	11	738	11	758	11	778	11	798	12
719	11	739	10	759	12	779	12	799	11
720	12	740	10	760	11	780	10	800	10

b	$N(b)$	b	$N(b)$	b	$N(b)$	b	$N(b)$	b	$N(b)$
801	11	821	11	841	11	861	11	881	12
802	12	822	11	842	10	862	11	882	13
803	12	823	11	843	13	863	11	883	13
804	10	824	10	844	11	864	11	884	12
805	12	825	10	845	11	865	11	885	13
806	10	826	10	846	10	866	11	886	11
807	12	827	11	847	11	867	11	887	12
808	11	828	11	848	11	868	11	888	11
809	12	829	11	849	11	869	11	889	11
810	10	830	12	850	10	870	10	890	11
811	11	831	11	851	11	871	11	891	10
812	10	832	10	852	10	872	12	892	11
813	10	833	11	853	11	873	10	893	11
814	12	834	10	854	11	874	11	894	11
815	10	835	10	855	11	875	11	895	11
816	10	836	11	856	11	876	10	896	10
817	12	837	11	857	11	877	13	897	10
818	12	838	10	858	10	878	10	898	13
819	10	839	11	859	11	879	11	899	11
820	12	840	10	860	11	880	11	900	11

b	$N(b)$	b	$N(b)$	b	$N(b)$	b	$N(b)$	b	$N(b)$
901	11	921	11	941	11	961	12	981	11
902	11	922	10	942	11	962	11	982	11
903	11	923	11	943	11	963	11	983	12
904	11	924	10	944	11	964	12	984	11
905	11	925	11	945	11	965	12	985	12
906	11	926	11	946	11	966	11	986	11
907	11	927	11	947	11	967	11	987	14
908	11	928	11	948	11	968	11	988	11
909	11	929	11	949	11	969	11	989	12
910	11	930	11	950	11	970	11	990	11
911	12	931	11	951	11	971	12	991	12
912	10	932	11	952	11	972	11	992	11
913	11	933	11	953	12	973	11	993	11
914	11	934	11	954	11	974	11	994	11
915	10	935	11	955	11	975	11	995	11
916	11	936	11	956	12	976	10	996	11
917	11	937	11	957	11	977	12	997	12
918	10	938	11	958	11	978	11	998	11
919	12	939	11	959	12	979	12	999	11
920	11	940	12	960	11	980	11	1000	11

第4章　正多角形の作図について … ガウスの f 項周期

平成１２年度の課題研究では,「正多角形と正多面体」をテーマに生徒と一緒に考えた. そこで扱った正多角形の作図について，課題研究ではどうしても曖昧にせざるを得なかった部分がある．それは，

1. 作図可能とは．そしてそれがどのように代数方程式の解法と関わるのか.
2. 正ｎ角形の作図可能条件　$n = 2^{\lambda} p_1 p_2 \cdots p_k$　　$(\lambda = 0, 1, 2, \cdots,$　　p_i は $Fermat$ 素数 $)$
3. $Gauss$ のアイディアによる正 17 角形の作図について … どうしてうまい数の組み合わせができるのか，その理由.

特に最後の問題が気にかかっていた．高木貞治著「近世数学史談」には計算方法が載っており，その正しさを追うことはできるが，アイディアが理解できない．研究中，随分以前[1]の雑誌「大学への数学」に河合良一郎先生が連載されていた「高校数学の周辺」のコピーを先輩の先生からいただいた．それには以下のような解説があった．$\zeta = \cos\frac{2\pi}{17} + i\sin\frac{2\pi}{17}$ とおき，$\zeta, \zeta^2, \cdots, \zeta^{16}$ に対し，　mod 3 の原始根の１つ 3 をとり，それを指数に作用させて，　$\zeta, \zeta^3, \zeta^9, \zeta^{10}, \zeta^{13}, \zeta^5, \zeta^{15}, \zeta^{11}, \zeta^{16}, \zeta^{14}, \zeta^8, \zeta^7, \zeta^4, \zeta^{12}, \zeta^2, \zeta^6$ を考える．それを１つおきに取って，$a = \zeta + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2,$　　$b =$ 残りの和　とすると，$a + b = -1,$　$ab = -4$ ．従って，$x^2 + x - 4 = 0$　を解く …· とある．少し前進したが，この方法のベースとなっているアイディアはつかめない.

課題研究発表会までには，どうしても時間が取れなかったので，そのあとではあったが手元の本を少し調べてみた.

まず，永田雅宜著「可換体論」(裳華房)．作図問題についての解説もあり，1，2 についてはわかるのであるが，3 については記述がない.

次に，アルティン著「ガロア理論入門」(東京図書)．ガロア理論から 2 については説明してあるが，やはり 3 については記述がない．ただし，この本には「ポストニコフの本を見よ」とかいてあった.

そこで，ポストニコフ「ガロアの理論」(東京図書)．この本は，数学を志したが文系の大学に進学した友人から頂いたものであった．学生時代にはあまり読んでいない．大学での講義が抽象的な代数学であったのに反してこの本は具体的な内容が多かった．そのため，学生時代はこの本ではなく、上記の本などを参考にするのが普通なのではないかと判断したのであった．いかにもロシアのテキストらしい具体的な内容の豊富さである。[2]円周等分多項式に対する１の原始 p 乗根が引き起こす自己同型作用と対応するグループ分

[1] 1974 年?．私が高校生になったのはそれより少しあとであるが，田舎では「大学への数学」をあまり見かけることはなかった

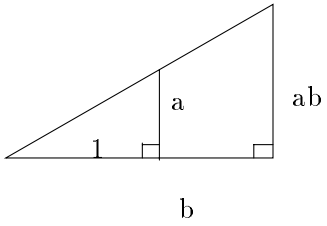
[2] 学生時代の指導教官が「ロシアのテキストは、計算式の変形についても逐一記述している」とおしゃったのが印象に残っている.

け …· ガウスの f 項周期 …· のアイディアが解説されており，3についての疑問が解決された．１．作図の可能性とは，２．作図可能条件とあわせて以下にメモしておく．

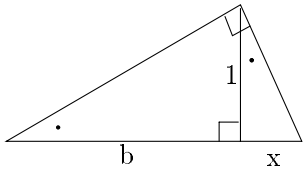
4.1　定規とコンパスによる作図

この節は永田雅宜著「可換体論」（裳華房）による．
作図問題は，与えられた有限個の点から出発して，作図しうる点がどのくらいあるかを考えることになる．直線は通る２点，線分は両端の２点，円は中心と半径によって決定される．定規とコンパスで可能な作図を考えてみる．

補題 ***4.1*** 実数 $1, a, b > 0$ について
$(a) a+b \qquad (b) a-b \qquad (c) ab \qquad (d) \dfrac{a}{b} \qquad (e) \sqrt{a}$
が作図できる．
証明）$(a), (b)$ については簡単．
(c) について

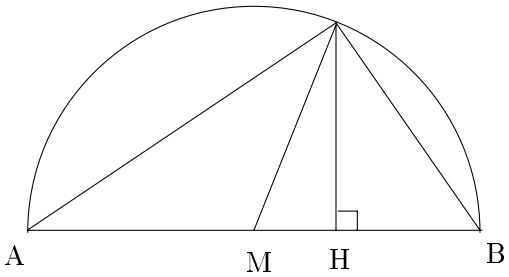


(d) について



$b : 1 = 1 : x$ より $x = \dfrac{1}{b}$ ．　　$\dfrac{1}{b}$ が作図できれば (c) より $\dfrac{a}{b}$ が作図できる．

(e) について



直径 AB=a+b の円で，中心 M,AH=a,HB=b

$$MP = \frac{a+b}{2}, \quad MH = \frac{a-b}{2}, \quad PH = \sqrt{\left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2} = \sqrt{ab}$$

複素平面上の作図としてこのことを考えると，2つの複素数 γ_1, γ_2 の表す点から
$(f)\gamma_1+\gamma_2 \quad (g)\gamma_1-\gamma_2 \quad (h)\gamma_1\gamma_2 \quad (i)\dfrac{\gamma_1}{\gamma_2} \quad (j)\sqrt{\gamma_1}$ の表す点を作図することができる．

定理 4.1　$0, 1, \alpha_1, \alpha_2, \ldots, \alpha_n$ が与えられた点を表す複素数とする．これらから出発して，β の表す点が作図可能な必要十分条件は，$K_0 = \mathbb{Q}(\alpha_1, \cdots, \alpha_n, \bar{\alpha_1}, \cdots, \bar{\alpha_n})$ から出発して，$K_0 \subset K_1 \subset \cdots \subset K_t$ という体の拡大列で

- $\beta \in K_t$
- $[K_i, K_{i-1}] = 2 \quad (i = 1, 2, \cdots, t)$

となるものが存在すること．

（注意．体の拡大の各段階では２次方程式の解を添加して進んでいく．）

証明）
十分性）

- 直線に関する対称点を作図することが可能であるから $\bar{\alpha_i}$ を作図できる．
  $(f), \ldots, (j)$ により $K_0 = \mathbb{Q}(\alpha_1, \cdots, \alpha_n, \bar{\alpha_1}, \cdots, \bar{\alpha_n})$ の元は作図可能である．
- K_{i-1} の元が作図可能であったと仮定する．$[K_i, K_{i-1}] = 2$ であるから，$^{\exists}\beta_i \in K_{i-1} \quad s.t. \quad K_i = K_{i-1}\left(\sqrt{\beta_i}\right)$ ．(j) が作図可能（偏角の 2 等分と $\sqrt{r}$ の作図可能性より）であることから $\sqrt{\beta_i}$ が作図可能．従って，K_0 のときと同様に K_i の元が作図可能であるといえる．
- 数学的帰納法により，$K_0, K_1, \cdots, K_t$ と順にその元が作図可能であることがわかる．//

必要性）既に作図できた点をもとに定規とコンパスで求め得る点は，
　$a)$ 2 直線の交点　$b)$ 直線と円の交点の１つ　$c)$ 円と円の交点の 1 つ
のいずれかである．
$a)$ について
　L_1 を γ_1, γ_2 で定まる直線とすると，$\beta = \gamma_1 + t(\gamma_2 - \gamma_1)$
　L_2 を γ_3, γ_4 で定まる直線とすると，$\beta = \gamma_3 + t(\gamma_4 - \gamma_3)$

$$\begin{cases} \gamma_1 + t(\gamma_2 - \gamma_1) = \gamma_3 + t(\gamma_4 - \gamma_3) & \cdots \quad (i) \\ \bar{\gamma_1} + t(\bar{\gamma_2} - \bar{\gamma_1}) = \bar{\gamma_3} + t(\bar{\gamma_4} - \bar{\gamma_3}) & \cdots \quad (ii) \end{cases}$$

$(i) \times (\bar{\gamma_4} - \bar{\gamma_3}) + (ii) \times (\gamma_4 - \gamma_3)$ より，
$\{(\gamma_1 - \gamma_3)(\bar{\gamma_4} - \bar{\gamma_3}) - (\bar{\gamma_1} - \bar{\gamma_3})(\gamma_4 - \gamma_3)\} + t\{(\gamma_2 - \gamma_1)(\bar{\gamma_4} - \bar{\gamma_3}) - (\bar{\gamma_2} - \bar{\gamma_1})(\gamma_4 - \gamma_3)\} = 0$
ここで，$(\gamma_2 - \gamma_1)(\bar{\gamma_4} - \bar{\gamma_3}) - (\bar{\gamma_2} - \bar{\gamma_1})(\gamma_4 - \gamma_3) = 0$ とすると
$$\frac{\gamma_4 - \gamma_3}{\gamma_2 - \gamma_1} = \frac{\overline{\gamma_4 - \gamma_3}}{\overline{\gamma_2 - \gamma_1}}$$

これは $\gamma_4-\gamma_3//\gamma_2-\gamma_1$ ，すなわち　$L_2//L_1$ を意味するが，今は交点を求めているので不適.

従って，$t=\dfrac{(\gamma_1-\gamma_3)(\bar{\gamma_4}-\bar{\gamma_3})-(\bar{\gamma_1}-\bar{\gamma_3})(\gamma_4-\gamma_3)}{(\bar{\gamma_2}-\bar{\gamma_1})(\gamma_4-\gamma_3)-(\gamma_2-\gamma_1)(\bar{\gamma_4}-\bar{\gamma_3})}$

t がこの形で表されることから，　$\beta\in\mathbb{Q}(\gamma_1,\gamma_2,\gamma_3,\gamma_4,\bar{\gamma_1},\bar{\gamma_2},\bar{\gamma_3},\bar{\gamma_4})$ の元であることが結論される.

$b)$ について

直線 $l:\beta=\gamma_1+t(\gamma_2-\gamma_1)$ ，円 $C:|\beta-\gamma_3|=r$ を連立して，

$\{\gamma_1+t(\gamma_2-\gamma_1)-\gamma_3\}\{\bar{\gamma_1}+t(\bar{\gamma_2}-\bar{\gamma_1})-\bar{\gamma_3}\}=r^2$

これは t の 2 次方程式．従って，解 t は $\mathbb{Q}(\gamma_1,\gamma_2,\gamma_3,\gamma_4,\bar{\gamma_1},\bar{\gamma_2},\bar{\gamma_3},\bar{\gamma_4})$ の 2 次拡大体の元である.

$c)$ について

円 $C_1:|\beta-\gamma_1|=r_1,\qquad C_2:|\beta-\gamma_2|=r_2$ とする.

C_1 から $(\beta_1^{\gamma})(\bar{\beta}-\bar{\gamma_1})=r^2$ ，$|\beta|^2-\beta\bar{\gamma_1}-\bar{\beta}\gamma_1+|\gamma_1|^2=r_1^2\qquad\cdots\quad(i)$

同様にして，$|\beta|^2-\beta\bar{\gamma_2}-\bar{\beta}\gamma_1+|\gamma_2|^2=r_2^2\qquad\cdots\quad(ii)$

$(i)-(ii)\qquad(\bar{\gamma_2}-\bar{\gamma_1})\beta+(\gamma_2-\gamma_1)\bar{\beta}=r_1^2-r_2^2\qquad\bar{\beta}=-\dfrac{\bar{\gamma_2}-\bar{\gamma_1}}{\gamma_2-\gamma_1}\beta+\dfrac{\gamma_1^2-\gamma_2^2}{\gamma_2-\gamma_1}$

(i) に代入

$$-\frac{\bar{\gamma_2}-\bar{\gamma_1}}{\gamma_2-\gamma_1}\beta^2+\frac{\gamma_1^2-\gamma_2^2}{\gamma_2-\gamma_1}\beta-\bar{\gamma_1}\beta+\gamma_1\frac{\bar{\gamma_2}-\bar{\gamma_1}}{\gamma_2-\gamma_1}\beta_1^{\gamma}\frac{\gamma_1^2-\gamma_2^2}{\gamma_2-\gamma_1}+|\gamma_1|^2=r_1^2$$

これは t の 2 次方程式．従って，解 β は $\mathbb{Q}(\gamma_1,\gamma_2,\bar{\gamma_1},\bar{\gamma_2})$ の 2 次拡大体の元である.

以上により，$a),b),c)$ の交点は既知の点が含まれる体の元もしくはその 2 次拡大体の元であることがわかった．従って定理の必要性が証明された//

系 *4.1* $0,1,\alpha_1,\cdots,\alpha_n$ から出発して β が作図されるとき，β の $K_0=\mathbb{Q}(\alpha_1,\cdots,\alpha_n,\bar{\alpha_1},\cdots,\bar{\alpha_n})$ 上の最小多項式の次数は２のべきであることが必要.（十分ではない）

これを利用して正多角形の作図，角の等分の可能性を考える.

正 n 角形 を作図する　$\Longleftrightarrow$　角 $\dfrac{2\pi}{n}$ を作る.

従って１の n 乗根 ζ を求める. 与えられる点は原点と $(1,0)$ であるから，$K_0=\mathbb{Q}$. ζ の最小多項式は n 位の円分多項式 $\Phi_n(x)$ で，その次数は $\phi(n)=^{\#}\{k\,|\,1\le k\le n-1,\,(k,n)=1\}$. 上の系より $\phi(n)=2^e$ とならねばならない．$n=p$ （素数）のときには，$\phi(p)=p-1$ であるから，$p=2^e+1$.

定理 *4.2* p が素数であるとき，

正 p 角形が作図可能　$\Longleftrightarrow$　$p=2^{2^n}+1$　（フェルマー素数）

証明）$e=kl$　（ l は奇数）とすると，$p=2^{kl}+1=\left(2^k\right)^l+1$. しかるに X^l+1 は $X+1$ で割り切れるから，$p=(2^k+1)\times$ 整数　となる．p が素数であることから $l=1$ で

あることが結論される．従って e は1より大きい奇数を因数に持たない．すなわち $e=2^n$ となり，$p=2^{2^n}+1$ （フェルマー素数）となることが必要.

逆に，$p=2^e+1$ のとき，$\mathbb{Q}(\zeta)$ は $\mathbb{Q}$ 上 2^e 次の $Galois$ 拡大．$Gal\,(\mathbf{Q}(\zeta)/\mathbb{Q})$ の位数は2の冪であるから冪」零群で，可解群である．従って，$K_0=\mathbb{Q}\subset K_1\subset\cdots\subset K_t=\mathbb{Q}(\zeta)$ となるものが存在する.（十分）.

定理 *4.3* 正 n 角形の作図ができる $\iff$ $n=2^\lambda p_1p_2\cdots p_r$（ $\lambda=0,1,2,\cdots$, $p_i=2^{2^{e_i}}+1$ 互いに異なるフェルマー素数）

証明）

$\Longleftarrow$) について

角の2等分は可能であるから $\lambda=0$ の時に示せば十分．素数の数 r についての帰納法で示す.

- $r=1$ の時は前定理.
- $r-1$ 以下のときに可能であると仮定して r のときを考える．

$$\zeta_1:=\cos\frac{2\pi}{p_1p_2\cdots p_{r-1}}+i\sin\frac{2\pi}{p_1p_2\cdots p_{r-1}},\quad \zeta_2:=\cos\frac{2\pi}{p_r}+i\sin\frac{2\pi}{p_r}$$

とおく.

$$\arg\zeta_1^t\zeta_2^u=\frac{2\pi}{p_1p_2\cdots p_{r-1}}+\frac{2\pi}{p_r}=\frac{2\pi}{n}\left(p_rt+p_1p_2\cdots p_{r-1}u\right)$$

$p_1p_2\cdots p_{r-1}$ と p_r は互いに素であるから $p_rt+p_1p_2\cdots p_{r-1}u=1$ を満たす $t,u\in\mathbb{Z}$ が存在する．仮定より ζ_1,ζ_2 は作図可能．従って ζ_1^t,ζ_2^u も作図可能．すなわち1の原始 n 乗根が作図可能であるといえる．//

$\Longrightarrow$) について

正 n 角形が作図可能であれば，その約数 n' について，正 n' 角形も作図可能．従って，$n=2^\lambda p_1^{f_1}\cdots p_r^{f_r}$ と素因数分解したとき，各 p_i はフェルマー素数でなければいけない．さらに， $f_i\geq 2$ とならないことを示す．それには各 $p=p_i$ について，正 p^2 角形が作図できないことを示せばよい．$\phi(p^2)=p(p-1)$ であるがそれは2の冪にはならない．作図可能なときには最小多項式の次数が2の冪にならなくてはいけないので，正 p^2 角形は作図不可能である．//

系 *4.2* 各の3等分線は一般には作図できない．一般に，p が奇素数ならば，各の p 等分線は作図できない.

証明）正 p^2 角形が作図できないことから，角 2π の p 等分もしくは 角 $\frac{2\pi}{p}$ の p 等分ができない．例えば，正9角形が作図不可能であることから 角 $\frac{2\pi}{3}$ の3等分ができないことが結論される.

系 *4.3* 角の n 等分が必ずできるのは，n が2の冪のときに限る.

4.2　素冪円分体の構造

円周 n 等分多項式とは，1の n 原始乗根を根に持ち，かつそれだけを根とする多項式のことである．その次数は $\phi(n) =^{\#} \{k \,|\, 1 \leq k \leq n-1, \quad (k,n)=1\}$ である．
$n = p$ ：素数のときは， $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$

補題 *4.2* $\Phi_p(x)$ は既約である．
証明）$\Phi_p(x) = \dfrac{x^p - 1}{x - 1}$ で $x = y + 1$ とおくと
$\Phi_p(x) = \dfrac{(y+1)^p - 1}{(y+1) - 1} = \dfrac{y^p +_p C_1 y^{p-1} +_p C_2 y^{p-2} + \cdots +_p C_{p-1} y + 1 - 1}{y}$
$= y^{p-1} +_p C_1 y^{p-2} + \cdots +_p C_{p-1}$
この y についての $p-1$ 次式は

- 最高次の項の係数は1で， p で割り切れない．
- その他の係数 ${}_pC_1, {}_pC_2, \cdots {}_pC_{p-1}$ は p の倍数である．
- 定数項 ${}_pC_{p-1} = p$ は p^2 で割り切れない．

従って，*Eisenstein* の判定定理により， $\Phi_p(x)$ は既約である．//

作図を問題とするので，基礎体を有理数体 $\mathbb{Q}$ として考える． $\mathbb{Q}$ 上の $\Phi_p(x)$ の分解体は $\mathbb{Q}(\zeta)$ だある．ただし， $\zeta = \cos\dfrac{2\pi}{p} + \sin\dfrac{2\pi}{p}$ とする．既約性により， $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$ ．

補題 *4.3* $\zeta, \zeta^2, \cdots, \zeta^{p-1}$ が $\mathbb{Q}(\zeta)$ の $\mathbb{Q}$ 上の基底をなす．
証明）$\zeta, \zeta^2, \cdots, \zeta^{p-1}$ は拡大次数の $p-1$ 個ある．それが $\mathbb{Q}$ 上1次独立であることを示せばよい．
$a_1\zeta + a_2\zeta^2 + \cdots + a_{p-1}\zeta^{p-1} = 0 \qquad (a_i \in \mathbb{Q}$ が成り立っていると仮定する．
両辺を ζ で割って，$a_1 + a_2\zeta + \cdots + a_{p-1}\zeta^{p-2} = 0$
これは ζ が $p-2$ 次方程式 $a_{p-1}x^{p-2} + \cdots + a_2 x + a_1 = 0$ の解であることを示す．$\Phi_p(x)$ の最小性により，この方程式は恒等的に 0 でなければいけない．従って $\zeta, \zeta^2, \cdots, \zeta^{p-1}$ は $\mathbb{Q}$ 上1次独立である．//

このとき，*Galois* 群 $G = Gal\,(\mathbb{Q}(\zeta)/\mathbb{Q})$ は巡回群となり，その位数は $p-1$ である．
$\sigma \in G$ を G の生成元の1つとすると， $\zeta^\sigma = \zeta^q$ （ q は $\mod p$ のある原始根）．
$i = o, \pm 1, \pm 2, \cdots$ に対して，$\zeta_i := \zeta^{\sigma^i} = \zeta^{qi}$ とする.（ただし， $\zeta_0 := \zeta$ とする）
$\zeta_i^\sigma = \zeta_{i+1}$
$\sigma^n = 1 \qquad \Longleftrightarrow \qquad p-1 \,|\, n \qquad$ より $\zeta_i = \zeta_j \qquad \Longleftrightarrow \qquad i \equiv j \pmod{p-1}$
従って， $\zeta_i \quad (i \in \mathbb{Z})$ の中で相異なるものは $p-1$ 個である．例えば，$\zeta_0, \zeta_1, \cdots, \zeta_{p-2}$ をそれらの代表としてとることができる．これらは $\zeta, \zeta^2, \cdots, \zeta^{p-1}$ を並び替えたものに他ならない．従って， $\mathbb{Q}(\zeta)/\mathbb{Q}$ の基底にすることができる．
Galois 群 G の部分群はまた巡回群であり，その生成元は σ^f （ f は $p-1$ の約数の1つ ）と表せる．逆に $p-1$ の任意の約数 f に対して， σ^f は G のある部分群を生成する．

$$
\begin{array}{ccc}
\mathbb{Q}(\zeta) & \longleftrightarrow & <\sigma^{p-1}>=<1> \\
{\scriptstyle \frac{p-1}{f}次}\uparrow & & \downarrow \\
\mathbb{Q}_f & \longleftrightarrow & <\sigma^f> \\
{\scriptstyle f次}\uparrow & & \downarrow \\
\mathbb{Q} & \longleftrightarrow & <\sigma>=Gal(\mathbb{Q}(\zeta)/\mathbb{Q})
\end{array}
$$

図のように部分体 $\mathbb{Q}_f$ と部分群 $<\sigma^f>$ を対応させる．$\alpha \in \mathbb{Q}_f \quad \Longleftrightarrow \quad \alpha^{\sigma^f}=\alpha$

$\mathbb{Q}_1=\mathbb{Q}, \quad \mathbb{Q}_{p-1}=\mathbb{Q}(\zeta) \quad$ 拡大次数 $[\mathbb{Q}(\zeta):\mathbb{Q}_f]=\dfrac{p-1}{f}, \qquad [\mathbb{Q}_f:\mathbb{Q}]=f$

Gauss の f 項周期

$p-1$ の任意の約数 f に対して，1の p 乗根 $\quad \zeta_0,\zeta_1,\cdots,\zeta_{p-2}$ を f 個のグループに分ける． $q:=\dfrac{p-1}{f}$ とおく．

$\zeta_0,$	$\zeta_f,$	$\zeta_{2f},$	$\cdots \quad \cdots$	$\zeta_{(q-1)f}$
$\zeta_1,$	$\zeta_{f+1},$	$\zeta_{2f+1},$	$\cdots \quad \cdots$	$\zeta_{(q-1)f+1}$
$\zeta_2,$	$\zeta_{f+2},$	$\zeta_{2f+2},$	$\cdots \quad \cdots$	$\zeta_{(q-1)f+2}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\quad \ddots$	$\vdots$
$\zeta_{f-1},$	$\zeta_{2f-1},$	$\zeta_{3f-1},$	$\cdots \quad \cdots$	ζ_{qf-1}

σ^f の作用により各元 ζ_i は表中の右隣の項 ζ_{i+f} にうつる.(ただし，右端の元 $\zeta_{(q-1)f+i}$ は左端の元 ζ_i にうつり，最後の項は ζ_0 にうつるものとする.)

各グループの和を求める．

$$\eta_i^{(f)}:=\sum_{j=0}^{q-1}\zeta_{jf+i}=\zeta_i+\zeta_{f+i}+\zeta_{2f+i}+\cdots+\zeta_{(q-1)f+i}$$

このとき，各 $\eta_i^{(f)}=\eta_i$ は σ^f の作用について不変．すなわち， $\eta_i^{\sigma^f}=\eta_i$ ．これらを **Gauss の f 項周期**という．不変性より $\eta_i \in \mathbb{Q}_f \quad (i=0,1,\cdots,f-1)$ ．

$\eta_0,\eta_1,\cdots,\eta_{f-1}$ の個数 f は拡大次数 $[\mathbb{Q}_f:\mathbb{Q}]$ に等しい．また，それらは $\mathbb{Q}$ 上独立である．従って，$\eta_0,\eta_1,\cdots,\eta_{f-1}$ は $\mathbb{Q}_f/\mathbb{Q}$ の基底となる．

補題 *4.4* 任意の周期 η_i は周期 $\eta=\eta_0$ の有理式で表される．

証明） $\eta=\eta_0 \in \mathbb{Q}_f$ より， $\mathbb{Q}(\eta) \subset \mathbb{Q}_f$ ．そこで， $m:=[\mathbb{Q}(\eta):\mathbb{Q}], \quad f(x) \in \mathbb{Q}[x]$ を η の $\mathbb{Q}$ 上の最小多項式とする．

$\mathbb{Q}(\eta) \subset \mathbb{Q}_f$ より，$m \le f$ ．

一方，$\eta_i=\eta^{\sigma^i} \quad (i=0,1,\cdots,f-1)$ より，

$f(x)=a_mx^m+a_{m-1}x^{m-1}+\cdots+a_1x+a_0 \qquad (a_i \in \mathbb{Q}$

$f(\eta)=a_m\eta^m+a_{m-1}\eta^{m-1}+\cdots+a_1\eta+a_0=0$

上式の両辺に σ^i を作用させて

$a_m\eta_i^m+a_{m-1}\eta_i^{m-1}+\cdots+a_1\eta_i+a_0=0$

従って，$\eta_0,\eta_1,\cdots,\eta_{f-1}$ は全て $f(x)$ の根である．すなわち，$f(x)$ は少なくとも f 個の

相異なる根を持つ．従って，$m \geq f$
以上により，$m = f$ ．これにより，$\mathbb{Q}(\eta) = \mathbb{Q}_f$
従って，$\eta_0, \eta_1, \cdots, \eta_{f-1}$ は全て $\mathbb{Q}(\eta)$ の元であり， η の有理式で表される．//

4.3 円周等分方程式の解法

$p - 1 = q_1 q_2 \cdot \cdots \cdot q_s$ ： 必ずしも相異なるとは限らない素数の積への分解．例えば，$17 - 1 = 2 \cdot 2 \cdot 2 \cdot 2$ ．

$\mathbb{Q}_{f'} \subset \mathbb{Q}_f \quad \Longleftrightarrow \quad f' \mid f$ であるから，$\mathbb{Q}_{(0)} := \mathbb{Q}$, $\mathbb{Q}_{(i)} := \mathbb{Q}_{q_1 q_2 \cdots q_i}$ とすると，$\mathbb{Q} = \mathbb{Q}_{(0)} \subset \mathbb{Q}_{(1)} \subset Q_{(1)} \subset \cdots \subset \mathbb{Q}_s = \mathbb{Q}(\zeta)$ という体の拡大列ができる．
拡大の各ステップ $\mathbb{Q}_{(i)}/\mathbb{Q}_{(i-1)}$ では $^{\exists}\alpha_i \in \mathbb{Q}_{(i)}$ $s.t.$ $\mathbb{Q}_{(i)} = \mathbb{Q}_{(i-1)}(\alpha_i)$, α_iは $\mathbb{Q}_{(i-1)} = \mathbb{Q}(\alpha_1, \alpha_2, \cdots, \alpha_{i-1})$ 上の q_i 次式の根で，$[\mathbb{Q}?(i) : \mathbb{Q}_{(i-1)}] = q_i$ ．
従って円周 p 等分方程式を解くことは，素数 $q_1, q_2, \cdots, q_s$ 次の方程式を順次解いていくことに帰着できる．
4.1 の結果により，定規とコンパスで作図可能となるのは $q_1 = q_2 = \cdots = q_s = 2$ となるときのみである．このとき，$p = 2^{2^n} + 1$ （フェルマー素数）である．フェルマー素数は現在のところ *3,5,17,257,65531* しか見つかっていない．$2^{2^5} + 1$ が合成数であることは *Euler* によって発見された．

4.4 円周１７等分方程式

Gauss の f 項周期のアイディアに基づき，方程式 $x^{16} + x^{15} + \cdots + x + 1 = 0$ を解く．河合良一郎先生の記事に従い，素数１７の原始根として最も簡単な３をとる．$3^n \mod 17$ は $3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1$ と順にならぶ．また，$p - 1 = 2 \cdot 2 \cdot 2 \cdot 2$ より，$\mathbb{Q} \subset \mathbb{Q}_2 \subset \mathbb{Q}_4 \subset \mathbb{Q}_8 \subset \mathbb{Q}_{16} = \mathbb{Q}(\zeta)$ と拡大列ができる．

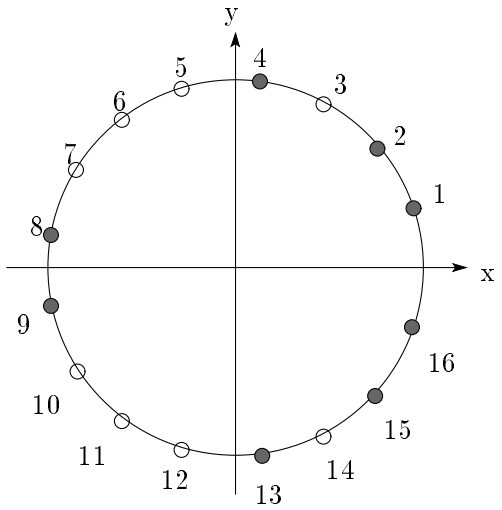


図 4.1:

(1)$f = 2$ のとき

$$\eta = \zeta + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2$$

$$\eta_1 = \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6$$

$$\eta^\sigma = \eta_1$$

$$\eta + \eta_1 = \zeta + \zeta^2 + \cdots + \zeta^{16} = -1 \qquad (\zeta^{16} + \cdots + \zeta + 1 = 0 \text{ より}) \tag{4.1}$$

$$\begin{aligned}
\eta\eta_1 =& \zeta^4 + \zeta^{19} + \zeta^{18} + \zeta^{26} + \zeta^{30} + \zeta^{15} + \zeta^{16} + \zeta^8 \\
& \zeta^{11} + \zeta^{14} + \zeta^{24} + \zeta^{29} + \zeta^{23} + \zeta^{20} + \zeta^{10} + \zeta^5 \\
& \zeta^6 + \zeta^{20} + \zeta^{27} + \zeta^{22} + \zeta^{28} + \zeta^{14} + \zeta^7 + \zeta^{12} \\
& \zeta^{12} + \zeta^{23} + \zeta^{20} + \zeta^{27} + \zeta^{22} + \zeta^{11} + \zeta^{14} + \zeta^7 \\
& \zeta^{15} + \zeta^{16} + \zeta^{25} + \zeta^{21} + \zeta^{19} + \zeta^{18} + \zeta^9 + \zeta^{13} \\
& \zeta^8 + \zeta^{21} + \zeta^{19} + \zeta^{18} + \zeta^{26} + \zeta^{13} + \zeta^{15} + \zeta^{16} \\
& \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^{25} + \zeta^{21} + \zeta^{19} + \zeta^{18} + \zeta^9 \\
& \zeta^7 + \zeta^{12} + \zeta^{23} + \zeta^{20} + \zeta^{27} + \zeta^{22} + \zeta^{11} + \zeta^{14}
\end{aligned}$$

$$\begin{aligned}
=& \zeta^4 + \zeta^2 + \zeta + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 \quad \cdots \quad \eta \\
& \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6 + \zeta^3 + \zeta^{10} + \zeta^5 \quad \cdots \quad \eta_1 \\
& \zeta^6 + \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} \quad \cdots \quad \eta_1 \\
& \zeta^{12} + \zeta^6 + \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 \quad \cdots \quad \eta_1 \\
& \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2 + \zeta + \zeta^9 + \zeta^{13} \quad \cdots \quad \eta \\
& \zeta^8 + \zeta^4 + \zeta^2 + \zeta + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} \quad \cdots \quad \eta \\
& \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2 + \zeta + \zeta^9 \quad \cdots \quad \eta \\
& \zeta^7 + \zeta^{12} + \zeta^6 + \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} \quad \cdots \quad \eta_1
\end{aligned} \tag{4.2}$$

$$= 4(\eta + \eta_1) = -4$$

(4.1),(4.2) より，η, η_1 は 2 次方程式 $x^2 + x - 4 = 0$ の 2 解である．$x = \dfrac{-1 \pm \sqrt{17}}{2}$ ．
円上で考えて（図 *4.1* 参照），$\eta > 0$ ．従って $\eta = \dfrac{-1 + \sqrt{17}}{2}$

(2) $f = q_1 q_2 = 4$ のとき，*4* 項周期は

$$\eta_0^{(4)} = \zeta + \zeta^{13} + \zeta^{16} + \zeta^4$$

$$\eta_1^{(4)} = \zeta^3 + \zeta^5 + \zeta^{14} + \zeta^{12}$$

$$\eta_2^{(4)} = \zeta^9 + \zeta^{15} + \zeta^8 + \zeta^2$$

$$\eta_3^{(4)} = \zeta^{10} + \zeta^{11} + \zeta^7 + \zeta^6$$

$[\mathbb{Q}_{(4)} : \mathbb{Q}_{(2)}] = 2$ について考えるので，$\eta_0^{(4)}$ と $\eta_2^{(4)}$ を用いる．

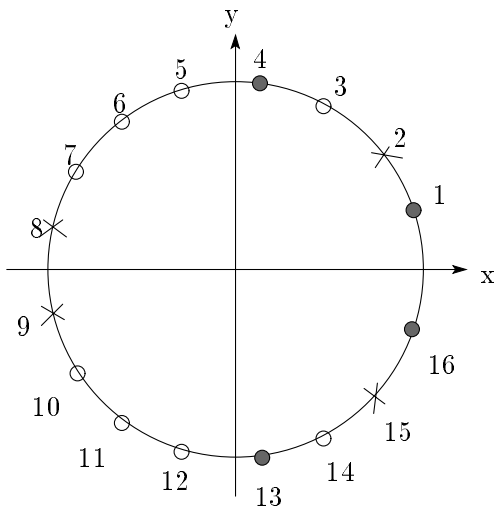


図 4.2:

$$\eta_0^{(4)} + \eta_2^{(4)} = \eta = \frac{-1+\sqrt{17}}{2} \tag{4.3}$$

$$\begin{aligned}
\eta_0^{(4)}\eta_2^{(4)} =& (\zeta + \zeta^{13} + \zeta^{16} + \zeta^4)(\zeta^9 + \zeta^{15} + \zeta^8 + \zeta^2) \\
=& \quad \zeta^{10} + \zeta^{28} + \zeta^{24} + \zeta^6 \\
&+ \zeta^{16} + \zeta^{21} + \zeta^{18} + \zeta^{13} \\
&+ \zeta^9 + \zeta^{15} + \zeta^{25} + \zeta^{19} \\
&+ \zeta^3 + \zeta^{22} + \zeta^{31} + \zeta^{12} \\
\\
=& \quad \zeta^{10} + \zeta^{11} + \zeta^7 + \zeta^6 \quad \cdots \quad \eta_3^{(4)} \\
&+ \zeta^{16} + \zeta^4 + \zeta + \zeta^{13} \quad \cdots \quad \eta_0^{(4)} \\
&+ \zeta^9 + \zeta^{15} + \zeta^8 + \zeta^3 \quad \cdots \quad \eta_2^{(4)} \\
&+ \zeta^3 + \zeta^5 + \zeta^{14} + \zeta^{12} \quad \cdots \quad \eta_1^{(4)} \\
\\
=& \eta_0^{(4)} + \eta_1^{(4)} + \eta_2^{(4)} + \eta_3^{(4)} = -1
\end{aligned} \tag{4.4}$$

従って，$\eta_0^{(4)}$ と $\eta_2^{(4)}$ は 2 次方程式 $x^2 - \dfrac{-1+\sqrt{17}}{2}x - 1 = 0$ の 2 解である．

$$x = \frac{-1+\sqrt{17} \pm \sqrt{34-2\sqrt{17}}}{4}$$

図 *4.2* より，$\eta_0^{(4)} > 0$ ．従って，$\eta_0^{(4)} = \dfrac{-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}}{4}$

(2) $f = q_1 q_2 q_3 = 8$ のとき，*8* 項周期は

$$\begin{aligned} \eta_0^{(8)} &= \zeta + \zeta^{16} & \eta_4^{(8)} &= \zeta^{13} + \zeta^4 \\ \eta_1^{(8)} &= \zeta^3 + \zeta^{14} & \eta_5^{(8)} &= \zeta^5 + \zeta^{12} \\ \eta_2^{(8)} &= \zeta^9 + \zeta^8 & \eta_6^{(8)} &= \zeta^{15} + \zeta^2 \\ \eta_3^{(8)} &= \zeta^{16} + \zeta^7 & \eta_7^{(8)} &= \zeta^{11} + \zeta^6 \end{aligned}$$

$[\mathbb{Q}_{(8)} : \mathbb{Q}_{(4)}] = 2$ について考えるので，$\eta_0^{(8)}$ と $\eta_4^{(8)}$ を用いる．

$$\eta_0^{(8)} + \eta_4^{(8)} = \zeta + \zeta^{16} + \zeta^{13} + \zeta^4 = \eta_0^{(4)} \tag{4.5}$$

$$\begin{aligned} \eta_0^{(8)} \cdot \eta_4^{(8)} =& (\zeta + \zeta^{16})(\zeta^{13} + \zeta^4) = \zeta^{14} + \zeta^{20} + \zeta^5 + \zeta^{29} \\ =& \zeta^{14} + \zeta^3 + \zeta^5 + \zeta^{12} = \eta_1^{(8)} + \eta_5^{(8)} \\ =& \eta_1^{(4)} \end{aligned} \tag{4.6}$$

ここで $\eta_1^{(4)}$ が現れたが，前節の補題からそれは $\eta_0^{(4)}$ の有理式で表すことができるはずである．積 $\eta_0^{(4)}\eta_1^{(4)}$ を作ってみる．

$$\begin{aligned} \eta_0^{(4)}\eta_1^{(4)} =& (\zeta + \zeta^{13} + \zeta^4)(\zeta^3 + \zeta^5 + \zeta^{14} + \zeta^{12}) \\ =& \zeta^4 + \zeta^{18} + \zeta^{30} + \zeta^{16} \\ & \zeta^6 + \zeta^{27} + \zeta^{28} + \zeta^7 \\ & \zeta^{15} + \zeta^{25} + \zeta^{19} + \zeta^9 \\ & \zeta^{13} + \zeta^{16} + \zeta^{21} + \zeta^{18} \end{aligned}$$

$$\begin{aligned} =& \zeta^4 + \zeta + \zeta^{13} + \zeta^{16} \quad \cdots \quad \eta_0^{(4)} \\ & \zeta^6 + \zeta^{10} + \zeta^{11} + \zeta^7 \quad \cdots \quad \eta_3^{(4)} \\ & \zeta^{15} + \zeta^8 + \zeta^2 + \zeta^9 \quad \cdots \quad \eta_2^{(4)} \\ & \zeta^{13} + \zeta^{16} + \zeta^4 + \zeta \quad \cdots \quad \eta_0^{(4)} \end{aligned} \tag{4.7}$$

$$\begin{aligned} =& 2\eta_0^{(4)} + \eta_2^{(4)} + \eta_3^{(4)} = (\eta_0^{(4)} + \eta_1^{(4)} + \eta_2^{(4)} + \eta_3^{(4)}) + \eta_0^{(4)} - \eta_1^{(4)} \\ =& -1 + \eta_0^{(4)} - \eta_1^{(4)} \end{aligned}$$

従って，$(1+\eta_0^{(4)})\eta_1^{(4)} = -1 + \eta_0^{(4)} \qquad \eta_1^{(4)} = \dfrac{-1+\eta_0^{(4)}}{1+\eta_0^{(4)}}$

以上より $\eta_0^{(8)}$ と $\eta_4^{(8)}$ は $x^2 - \eta_0^{(4)} x \dfrac{\eta_0^{(4)} - 1}{\eta_0^{(4)} + 1} = 0$ の 2 解である．

$\eta_0^{(4)} = \xi$ とおくと，$(\xi+1)x^2 - \xi(\xi+1)x + \xi - 1 = 0$

$$x = \frac{\xi(\xi+1) \pm \sqrt{\xi^2(\xi+1)^2 - 4(\xi^2-1)}}{2(\xi+1)} = \frac{(\xi^2+\xi) \pm \sqrt{\xi^4+2\xi^3-3\xi^2+4}}{2(\xi+1)}$$

円上の点で考えると $\eta_0^{(8)} > 0$ がわかる．また，$\eta_0^{(8)} = 2\cos\dfrac{2\pi}{17}$ であり，この値が上で計算できたので正１７角形の作図が可能であると言える．//

4.5 Gauss の方法で積の整理がなぜうまくいくか

$\mathbb{Q}_f = \mathbb{Q}(\eta), \quad \eta = \eta_0^{(f)} = \zeta + \zeta_f + \cdots + \zeta_{(g-1)f} \quad \left(g = \dfrac{p-1}{f}\right)$ ： g 項周期の１つ目．

$f' \mid f$ とすると，$\mathbb{Q}_f = \mathbb{Q}_{f'}(\eta)$

ここで，η を根とする $\mathbb{Q}_{f'}$ 上の既約多項式，すなわち $\mathbb{Q}_{f'}$ 上の η の最小多項式を考える．

そのために次の周期を考える． [3]

$$\eta = \eta_0, \eta_{f'}, \eta_{2f'}, \cdots, \eta_{(h-1)f'} \quad \left(h = \frac{f}{f'}\right) \tag{4.8}$$

$$\begin{aligned} \left(\eta_{kf'}\right)^{\sigma^{f'}} &= \left(\zeta_{kf'} + \zeta_{kf'+f} + \zeta_{kf'+2f} + \cdots + \zeta_{kf'+(g-1)f}\right)^{\sigma^{f'}} \\ &= \zeta_{kf'+f'} + \zeta_{kf'+f+f'} + \zeta_{kf'+2f+f'} + \cdots + \zeta_{kf'+(g-1)f+f'} \\ &= \eta_{(k+1)f'} \end{aligned} \tag{4.9}$$

従って， $f(x) = (x-\eta)(x-\eta_{f'})(x-\eta_{2f'}) \cdot \cdots \cdot (x-\eta_{(h-1)f'})$ は $\mathbb{Q}_f$ 上の多項式である．

そしてその次数は $h = [\mathbb{Q}_f : \mathbb{Q}_{f'}]$ に等しい．よってこれが求める最小多項式である．

この多項式の x^{h-1} の係数 $\times(-1)$ は

$$\begin{aligned} \eta + \eta_{f'} + \eta_{2f'} + \cdots + \eta_{(h-1)f'} &= \sum_{k=0}^{h-1} \eta_{kf'} = \sum_{k=0}^{k-1}\sum_{l=0}^{g-1} \zeta_{kf'+lf} \\ &= \sum_{l=0}^{g-1}\sum_{k=0}^{h-1} \zeta_{f'(k+lh)} = \sum_{j=0}^{g'-1} \zeta_j \quad \left(g' = \frac{p-1}{f'}\right) \end{aligned} \tag{4.10}$$

すなわち，f' に対応する $Gauss$ の g' 項周期 $\eta^{(f')}$ $\eta_0^{(f')}$ と同じ．

他の係数も $\eta_0, \eta_1, \cdots, \eta_{f-1}$ が $\mathbb{Q}_f/\mathbb{Q}$ の基底であることから「任意の $\eta_i\eta_j$ は周期 $\eta_0, \eta_1, \cdots, \eta_{f-1}$ の１次結合で表される」ことが導かれ，それらによって係数が計算できる．

♣ Gauss のアイデア

[3] 注意．実際には $\mathbb{Q} \subset \mathbb{Q}_{(1)} \subset \mathbb{Q}_{(2)} \subset \cdots \subset \mathbb{Q}_{(s)} = \mathbb{Q}(\zeta)$ の拡大の途中を考えているので，$f = q_1 \cdot \cdots \cdot q_{i-1}q_i, \quad f' = q_1 \cdot \cdots \cdot q_{i-1}$ を考えればよい．

積 $\eta_i\eta_j$ を計算するために $Gauss$ は次のような整理の仕方を提案した.

$$\eta_i\eta_j = (\zeta_i + \zeta_{i+f} + \zeta_{i+2f} + \cdots + \zeta_{i+(g-1)f})(\zeta_j + \zeta_{j+f} + \zeta_{j+2f} + \cdots + \zeta_{j+(g-1)f})$$

$$\begin{aligned}
= \quad & \zeta_i\zeta_j + \zeta_{i+f}\zeta_{j+f} + \cdots + \zeta_{i+(g-1)f}\zeta_{j+(g-1)f} \qquad \text{（縦に並んだ項の積）} \\
+ \quad & \zeta_i\zeta_{j+f} + \zeta_{i+f}\zeta_{j+2f} + \cdots + \zeta_{i+(g-1)f}\zeta_j \qquad \text{（相手を１つずつ右へ）} \\
+ \quad & \zeta_i\zeta_{j+2f} + \zeta_{i+f}\zeta_{j+3f} + \cdots + \zeta_{i+(g-1)f}\zeta_{j+f} \qquad \text{（相手を２つずつ右へ）} \\
& \vdots \\
+ \quad & \zeta_i\zeta_{j+(g-1)f} + \zeta_{i+f}\zeta_j + \cdots + \zeta_{i+(g-1)f}\zeta_{j+(g-2)f} \qquad \text{（相手を } g-2 \text{ ずつ右へ）}
\end{aligned} \tag{4.11}$$

このとき，各行に対して σ^f の作用を考えると，各項はその行内の１つ右の項へ移る．ただし，右端の項は左端に移る．また，それぞれは１であるかもしくは１の p 乗根である．従って各行は１ばかりの和で $= g$ となるか，もしくは１の p 乗根からなり，$\eta_0, \eta_1, \cdots, \eta_{f-1}$ のうちの１つであるかである．$\eta_0, \eta_1, \cdots, \eta_{f-1}$ のうちのどれであるかは，行中のどれか１つがわかればよい．従って計算が簡単に実行できるのである．

以上，ポストニコフ著　「ガロアの理論」　（東京図書）による．

4.6　正７角形について

7はフェルマー素数ではないので，定規とコンパスで作図することは不可能．その事情を計算でも確かめてみる.（１）加法定理
$7\theta = 2\pi$ とすると $4\theta = 2\pi - 3\theta$ ．従って，$\cos 4\theta = \cos 3\theta$ ．
$\cos\theta = x$ とおくと，$2(2x^2-1)^2 - 1 = 4x^3 - 3x$　　$8x^4 - 4x^3 - 8x^2 + 3x + 1 - 0$　　$(x-1)(8x^3 + 4x^2 - 4x - 1) = 0$ ．
$x \neq 1$ より，$8x^3 + 4x^2 - 4x - 1 = 0$ ．$2x = X$ とおくと，$X^3 + X^2 - 2X - 1 = 0$ ．この方程式に $X = \pm 1$ を代入しても 0 にならないので，$X^3 + X^2 - 2X - 1$ は $\mathbb{Q}$ 上既約.よって $8x^3 + 4x^2 - 4x - 1$ もそうである．従って３次拡大を作らないと $\cos\dfrac{2\pi}{7}$ が求められない．即ち，定規とコンパスでは作図できない.

（２）相反方程式
$z^7 = 1$ より，$z^7 - 1 = (z-1)(z^6 + z^5 + z^4 + z^3 + z^2 + z + 1) = 0$ ．
$z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0$ で $z \neq 0$ のとき，両辺 $\div z^3$ ．
$\left(z^3 + \dfrac{1}{z^3}\right) + \left(z^2 + \dfrac{1}{z^2}\right) + \left(z + \dfrac{1}{z}\right) + 1 = 0$ ．
$X = z + \dfrac{1}{z}$ とおくと，$(X^3 - 3X) + (X^2 - 2) + X + 1 = 0$　　$X^3 + X^2 - 2X - 1 = 0$ ．
これは先の方程式と同じである.（それは $X = z + \dfrac{1}{z} = 2\cos\dfrac{2\pi}{7}$ であることから当たり前なのであるが）

（３）体の拡大で
$\phi(7) = 7 - 1 = 6 = 2 \times 3$　　$\zeta = \cos\dfrac{2\pi}{7} + i\sin\dfrac{2\pi}{7}$ ．

$\mathbb{Q} \subset \mathbb{Q}_2 \subset \mathbb{Q}_6 = \mathbb{Q}(\zeta)$ もしくは $\mathbb{Q} \subset \mathbb{Q}_3 \subset \mathbb{Q}_6 = \mathbb{Q}(\zeta)$
(i) $\mathbb{Q}_2$ について， mod 7 の原始根として例えば *3*をとると，$3^n \mod 7$ は順に $3, 2, 6, 4, 5, 1$.
3 項周期は，$\eta = \zeta + \zeta^2 + \zeta^4 \qquad \eta_1 = \zeta^3 + \zeta^6 + \zeta^5$
円上で点を取って考えると $Im\ \eta > 0$ がわかるので $\eta = \dfrac{-1+\sqrt{7}i}{2}$ となることに注意する.

$$\eta + \eta_1 = \zeta + \zeta^2 + \zeta^4 + \zeta^3 + \zeta^6 + \zeta^5 = -1 \tag{4.12}$$

$$\begin{aligned} \eta \cdot \eta_1 =& (\zeta^4\text{のある行}) + (\zeta^7\text{のある行}) + (\zeta^6\text{のある行}) \\ =& \eta + 3 + \eta_1 = 2 \end{aligned} \tag{4.13}$$

従って，η, η_1 は $x^2 + x + 2 = 0$ の 2 解. $x = \dfrac{-1 \pm \sqrt{7}i}{2}$.
これらは ζ, ζ^2, ζ^4 の作る三角形および $\zeta^2, \zeta^6, \zeta^5$ の作る三角形の重心を求めていくことに役立つが，それら 1 つずつを求めるには，例えば η からは

$$\zeta\zeta^2 + \zeta^2\zeta^4 + \zeta^4\zeta = \zeta^3 + \zeta^6 + \zeta^5 = \eta_1 \tag{4.14}$$

$$\zeta\zeta^2\zeta^4 = \zeta^7 = 1 \tag{4.15}$$

従って $x^3 - \dfrac{-1+\sqrt{7}i}{2}x^2 + \dfrac{-1-\sqrt{7}i}{2}x - 1 = 0$
これは $\mathbb{Q}(\dfrac{-1+\sqrt{7}i}{2})$ 上で既約となる.

(ii)$\mathbb{Q}_3$ について
2 項周期は，$\eta = \zeta + \zeta^6 \quad \eta_1 = \zeta^3 + \zeta^4 \quad \eta = \zeta^2 + \zeta^5$.

$$\eta + \eta_1 + \eta_2 = \zeta + \zeta^6 + \zeta^3 + \zeta^4 + \zeta^2 + \zeta^5 = -1 \tag{4.16}$$

$$\begin{aligned} \eta \cdot \eta_1 =& (\zeta^4\text{のある行}) + (\zeta^5\text{のある行}) = \eta_1 + \eta_2 \\ \eta_1 \cdot \eta_2 =& (\zeta^5\text{のある行}) + (\zeta^8 = \zeta\text{のある行}) = \eta_2 + \eta \\ \eta_2 \cdot \eta =& (\zeta^3\text{のある行}) + (\zeta^8 = \zeta\text{のある行}) = \eta_1 + \eta \end{aligned} \tag{4.17}$$

従って

$$\eta\eta_1 + \eta_1\eta_2 + \eta_2\eta = 2(\eta + \eta_1 + \eta_2) = -2 \tag{4.18}$$

$$\begin{aligned} \eta\eta_1\eta_2 =& \eta(\eta_2 + \eta) = \eta\eta_2 + (\zeta + \zeta^6)^2 \\ =& (\eta_1 + \eta) + (\zeta^4\text{の行}) + (\zeta^7\text{の行}) \\ =& \eta_1 + \eta + \eta_2 + 2 = 1 \end{aligned} \tag{4.19}$$

従って

$$x^3 + x^2 - 2x - 1 = 0 \tag{4.20}$$

これは既約.

課題　正７角形は折り紙で作図可能であるという．どのように３次拡大を実現しているのか？

もう少し時間を見つけて，$Galois$ 理論の理解をもう少し深め，具体的な方程式の $Galois$ 群を計算してみるとよいのであろう．また，ポストニコフの本には「どのような５次方程式が根号で解けるか」など，おもしろそうな話題も載っている．そこで用いられている５次方程式の標準形と判別式については以前「数学Ⅰ・Aの指導メモ」で少し触れたものである．

５次方程式については，楕円関数を用いた解法も以前からの課題である．学生時代に，$Mumford$ 著「$Tata\ lectures\ on\ theta\ I,II$」（$Birkhauser$）の付録に梅村浩先生の論文があるのを知っていたが，読めずに終わっている．最近梅村先生が「楕円関数論」という本を東京大学出版会から出され，その中にもそのことが書かれている．時間を見つけて読んでみるべきであるが ….

作図問題について，学生時代から曖昧にしていた部分が今回少しすっきりさせることができた.（２００１年2月１１日）

第5章　フラーレンＣ６０からの変形 ••• Ｃ２４とＣ１２

化学の先生が不在であったある日、１年生から「黒鉛は分子か？」という質問を受けた。説明をしているうちにＣ６０フラーレンにも話がおよび、数学の課題研究で生徒が作成したサッカーボール型の模型が職員室にあることを教えた。課題研究以降、教務の仕事がずっと忙しく、そして年度末の整理、新たに進路の仕事に就いてばたばたしているうちあっという間に時間が過ぎていた。課題研究の頃のことが懐かしく思い出された。

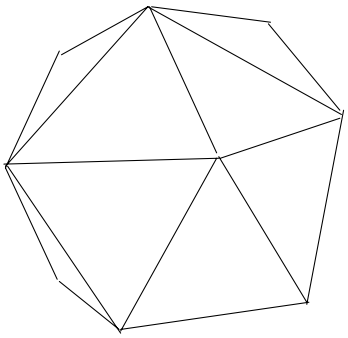
そのしばらく後、名古屋大学が主催している数学コンクールの問題に以下のようなものがあったことを知った。[1]

問題　「Ｃ６０フラーレンの炭素の個数が６０のかわりに２４だったらどのような形状か？」

課題研究の時に生徒がサッカーボールの作り方について報告していたことを思い出したら、その方法でＣ２４の形状が浮かんだ。

5.1　Ｃ６０ ••• サッカーボール

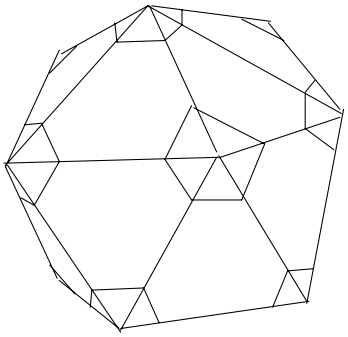
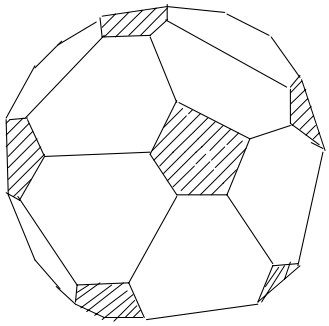
1. 正２０面体を作る。



正三角形が 20 個あり、1 つの頂点に 5 本の辺が集まっている。従って $3 \times 20 \div 5 = 12$ 個の頂点がある。

2. 各頂点を中心に 5 角形を切り取る。

[1] 記事を書いていらっしゃったのは大沢健夫先生である。砺波市出身であり、以前、砺波高校に出張講義に来たいた。またその折り、課題研究で問題となっていた事項について、北岡先生に取り次いでいただいたのであった。

12 個の頂点の分だけ正５角形ができる。この立体の頂点は全て５角形の頂点となっており、また、異なる５角形が頂点を共有することはないから、サッカーボールの頂点は $5 \times 12 = 60$ 個である。

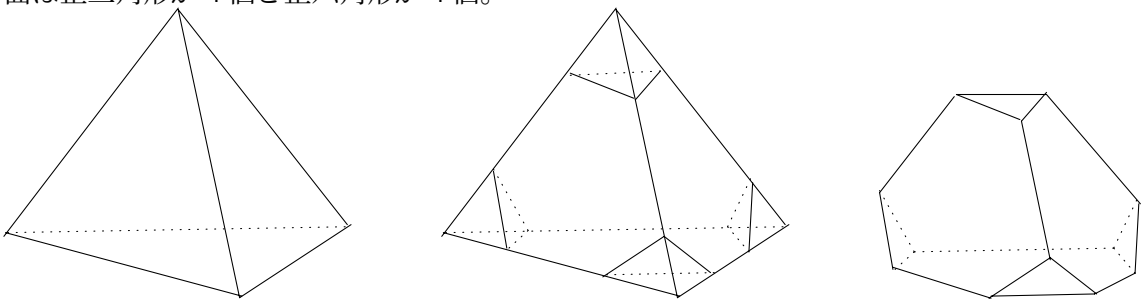
5.2　面取りによるＣ１２，２つのＣ２４、別のＣ６０

その他の正多面体についても、各頂点から面取りをしてみる。

3. 正４面体

　頂点は $3 \times 4 = 12$ 個。従ってＣ１２。

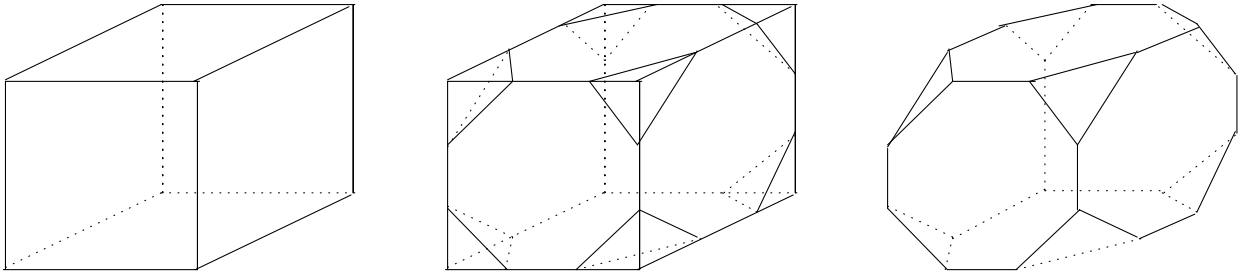
面は正三角形が４個と正六角形が４個。



4. 正６面体（立方体）

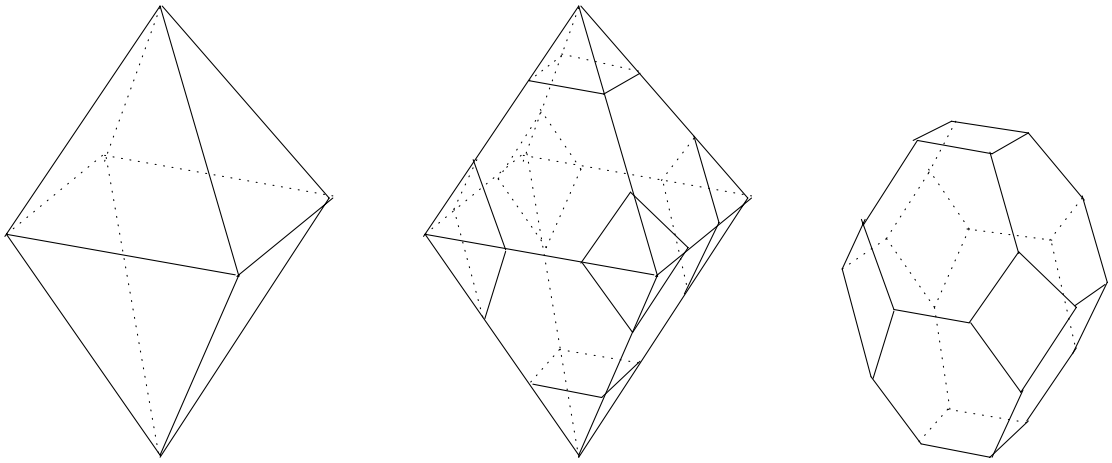
　頂点は $3 \times 8 = 24$ 個。従ってＣ２４。

面は正三角形が８個と正八角形が６個。



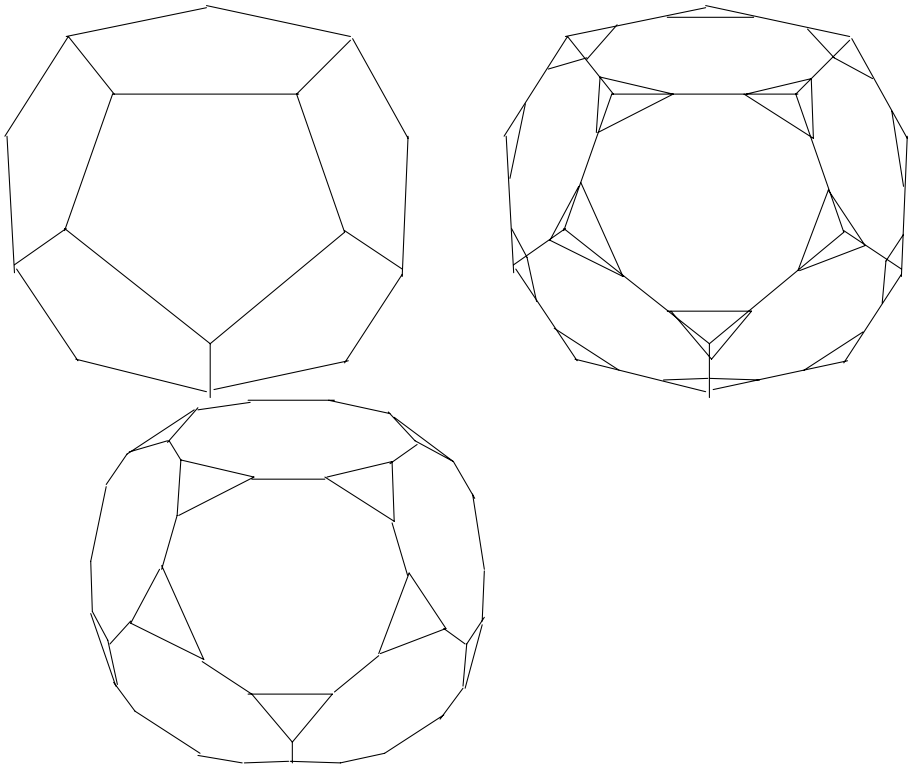
5. 正８面体

頂点は $4 \times 6 = 24$ 個。従ってＣ２４その２。
面は正方形が６個と正六角形が８個。



6. 正１２面体

頂点は $3 \times 20 = 60$ 個。従ってＣ６０その２。
面は正三角形が２０個と正十角形が１２個。



上記の２つのＣ１２が数学コンクールの答えになりうるのだと思う。参加者がどのような答えを出したのか、主催者がどのような解答を用意していたのかはまだ調べていない。上記の構成法があるか否かはよく調べていない。

余談、課題

- 宮池先生「Cからは４本の手が出ていると思うのですが、Ｃ６０の頂点からの辺は３本ずつで１本手が余っていますよね」
  片山「ベンゼンのように２重結合でもう１本手を出しているのでは」
- 上のような図をコンピュータでうまく書くにはどうすればいいか？*Mathemativa*には正多面体の図があったけど。なお、上記の図は *WinTpic* を用いて手書きした。
- 上記のような構造のうち、Ｃ６０フラーレン以外は実際には存在しないそうだけど、それはどうしてか？結合力に対して何かしらの方程式を立てて、その極小条件を考えていくような難しい内容なのであろうか？

(以上、*May 23,2001)*

その後、授業で話題にしたところ、理数科３年の水上君が模型を作ってきてくれた。(それまで私自身は手書きの絵で考えただけであった。) はじめは紙で作ったもの、引き続きマッチ棒をうまく接着した骨格模型で、以下の写真のようなものである。

その立体を眺めてみると、サッカーボール以外のものは頂点から伸びる辺のなす角度がかなりアンバランスなのである。唯一サッカーボールのものは正六角形の内角と正五角形の 120° と 108° であり、その差は許容範囲としてなんとかバランスを保っているのかもしれない。この考えは正しいのかどうか確かめていないが、周囲の人には割と支持してもらえる。実際の立体を見ることによって見えてくることもあるものだ。(２００１年夏)

全国理数科教育研究大会の発表のプレゼンテーション用に，色画用紙で模型を作っておいた.

正２０面体をもとに作成するものが作りにくい．残る１０角形と穴の開く三角形の差が大きい.（２００１年秋）