整数と素数の不思議の世界

谷口隆

概 要

整数というのは、1,2,3,4,5, ··という数 (とそのマイナス) のことでとても身近なものと考えておられることと思います。でもこの素朴な数の列には、特に素数を中心として、不思議な規則が実にたくさん隠れています。それを研究する『整数論』と呼ばれる数学の研究分野があって、そこでは大の大人が整数の秘密を解き明かそうと躍起になって研究を続けています。(中には解くと１億円もらえる懸賞金のかかった問題まであります！)

また、整数を研究する歴史の中で、ゼータ関数と呼ばれる関数が発見されました。整数のようにぽつぽつぽつと一つずつ離れているものが、関数のようにつながったものと関係するのは、意外なことと思われるかもしれません。しかしこのゼータ関数と素数の結びつきはとても深く、上に述べた懸賞金の問題はいずれもゼータ関数と関わっています。

ここでは、その不思議な世界を垣間見てみたいと思います。

（本稿は、神戸大学サイエンスセミナー「整数と素数の不思議な世界」(2009 年 7 月 26 日) の配布資料に若干加筆をしたものです。）

目 次

1　素数の並び方

素数とは、1 と自分自身以外に正の約数をもたない数のことでした。たとえば $2, 3, 5$ は素数で、$6 = 2 \times 3$ は素数ではありません。始めに、素数を小さい順にいくつか書き出してみましょう。

$$2,\quad 3,\quad 5,\quad 7,\quad 11,\quad 13,\quad 17,\quad 19,\quad 23,\quad 29,$$
$$31,\quad 37,\quad 41,\quad 43,\quad 47,\quad 53,\quad 59,\quad 61,\quad 67,\quad 71,\quad \cdots$$

20 番目まで書いてみました。さて、この操作はいつか終わりが来るのでしょうか、それともいつまでも続くのでしょうか？これは実は、素数が無限にあるためにどこまでも続けていくことができます。

定理 1　素数は無限に存在する。

(証明) 背理法で示す。素数が有限個しかなかったとして、それらを小さい順に $p_1, p_2, p_3, \ldots, p_n$ とおく。

$$N = p_1 \times p_2 \times p_3 \times \cdots \times p_n + 1$$

という数を考える。すると N は最大の素数 p_n よりも大きな数だから素数ではない。一方で N は p_1 の倍数に 1 を足した数だから p_1 では割り切れない。同じように考えると $p_2, p_3, \ldots, p_n$ いずれでも割り切れない。今素数は $p_1, p_2, \ldots, p_n$ ですべてと仮定したのだから、N はどのような素数で割ることもできない。これは矛盾である。よって素数は無限に存在する。　(証明終)

素数を書き出す作業をもっと続けると次のようになります。

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,　(25 個)
101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199,　(21 個)
211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293,　(16 個)
307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397,　(16 個)
401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499,　(17 個)
503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599,　(14 個)
601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691,　(16 個)
701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797,　(14 個)
809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887,　(15 個)
907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997,　(14 個)
1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049, 1051, 1061, 1063, 1069, 1087, 1091, 1093, 1097,　(16 個)
1103, 1109, 1117, 1123, 1129, 1151, 1153, 1163, 1171, 1181, 1187, 1193,　(12 個)
1201, 1213, 1217, 1223, 1229, 1231, 1237, 1249, 1259, 1277, 1279, 1283, 1289, 1291, 1297,　(15 個)

1301, 1303, 1307, 1319, 1321, 1327, 1361, 1367, 1373, 1381, 1399, (11 個)
1409, 1423, 1427, 1429, 1433, 1439, 1447, 1451, 1453, 1459, 1471, 1481, 1483, 1487, 1489, 1493, 1499, (17 個)
1511, 1523, 1531, 1543, 1549, 1553, 1559, 1567, 1571, 1579, 1583, 1597, (12 個)
1601, 1607, 1609, 1613, 1619, 1621, 1627, 1637, 1657, 1663, 1667, 1669, 1693, 1697, 1699, (14 個)
1709, 1721, 1723, 1733, 1741, 1747, 1753, 1759, 1777, 1783, 1787, 1789, (12 個)
1801, 1811, 1823, 1831, 1847, 1861, 1867, 1871, 1873, 1877, 1879, 1889, (12 個)
1901, 1907, 1913, 1931, 1933, 1949, 1951, 1973, 1979, 1987, 1993, 1997, 1999, (13 個)

素数の仕組みについてもう少し考えてみましょう。上では、2000 以下の素数を 100 ごとに区切ってその個数を数えてみました。個数を考えてみると、緩やかに少しずつ減っているようにみえます。素数の並びといえば、$1327, 1361$ のように間隔が大きく空いたものもあれば、$1481, 1483, 1487, 1489$ のように短い間隔でたくさん現れることもあって、なにか秩序だった規則をみつけることは難しいようにみえます。しかし、その個数については実は不思議な法則があることが発見されました。

$$\pi(x) = (x \text{ 以下の素数の個数})$$

という関数を考えます。
Q： $\pi(10)$ と $\pi(11)$ を求めてください。$\pi(100), \pi(200), \pi(1000)$ はいくつでしょうか。
A： 10 以下の素数は $2, 3, 5, 7$ だから $\pi(10) = 4$, 11 以下なら 11 も加わるので $\pi(11) = 5$ です。$\pi(100)$ なら 100 以下の素数を求める必要がありますが、上の表によればそれは 25 個なので $\pi(100) = 25$、同様に $\pi(200) = 25 + 21 = 46$, $\pi(1000) = 25 + \cdots + 14 = 168$ となります。

関数 $\pi(x)$ は $x \to \infty$ のときどんな挙動をするか、そのことについて次のような定理があります。

定理 2 (素数定理)

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

ここで $\log x$ の底は自然対数 $e = 2.71828\ldots$ です。この式が何を意味するのか、まず少し考えてみましょう。分母の関数を

$$g(x) = \frac{x}{\log x}$$

とします。$x = 10^n$ のときの $g(x)$ の値はどうなるでしょうか。まず、

$$g(10^n) = \frac{10^n}{\log_e 10^n} = \frac{10^n}{n} \cdot \frac{1}{\log_e 10} = \frac{10^n}{n} \cdot \log_{10} e$$

ここで、$e \fallingdotseq 2.7 = 3^3/10$ と考えれば、$\log_{10} 3 \fallingdotseq 0.4771$ だったので、

$$g(10^n) \fallingdotseq \frac{10^n}{n} \cdot \log_{10} \frac{3^3}{10} \fallingdotseq \frac{10^n}{n}(3\log_{10} 3 - 1) \fallingdotseq \frac{10^n}{n} \cdot 0.43$$

1 億 $(=10^8)$ 以下の素数の個数、つまり $\pi(10^8)$ を求めるのは大変な手間です。でも素数定理によれば、$\pi(10^8)$ はだいたい $g(10^8)$ ぐらいで、上の計算から $g(10^8) \fallingdotseq 10^8 \cdot \frac{0.43}{8}$ だから、約 540 万個ぐらいと見積もることができます。実際には $\pi(10^8) = 5761455$ なので、6%程度の誤差で見積もれていることになります。100 億 $= 10^{10}$ ならばどうでしょうか。上の式で $n = 10$ とすると、$g(10^{10}) \fallingdotseq 10^7 \times 0.43$ =4 億 3 千万はたちまち計算できます。これは $\pi(10^{10}) = 455052511$ と 4.8%の誤差です。(100 億以下の素数を求めるには、1 億以下の素数を調べるその手間の、少なくとも 100 倍はかかることに注意してください！)

x	10^8	10^{10}
$g(x)$	5428681	434294482
$\pi(x)$	5761455	455052511
誤差	約 6%	約 4.8%

ある程度誤差はあるものの、手間をかけずに近似値が計算できることが、$g(x)$ と $\pi(x)$ の関係の不思議なところです。

実際には、

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\log t}\, dt$$

という関数があり、$g(x)$ を $\mathrm{Li}(x)$ で置き換えても、素数定理と同じ公式

$$\lim_{x\to\infty} \frac{\pi(x)}{\mathrm{Li}(x)} = 1$$

が成り立ちます。しかも、数値実験で見ると、$\mathrm{Li}(x)$ は $\pi(x)$ をもっと、とんでもない精度で近似していることが観察できます。たとえば $\mathrm{Li}(10^8) \fallingdotseq 5762209$ は $\pi(10^8) = 5761455$ と 0.013%程度の差、$\mathrm{Li}(10^{10}) \fallingdotseq 455055615$ は $\pi(10^8) = 455052511$ と 0.0007%程度の差！

x	10	10^2	10^3	10^4	10^5	10^6	10^7	10^8	10^9	10^{10}	10^{11}
$\pi(x)$	4	25	168	1229	9592	78498	664579	5761455	50847534	455052511	4118054813
$\mathrm{Li}(x)$	5.1	29	177	1245	9629	78627	664917	5762208	50849234	455055614	4118066400
$x/\log x$	4.3	22	135	1086	8686	72382	620421	5428681	48254942	434294482	4287977972

不規則で値を求めるのが大変な関数 $\pi(x)$ が $x/\log x$ や $\mathrm{Li}(x) = \int_2^x (dt/\log t)$ のようなシンプルな関数で近似できるのは不思議なことではないでしょうか。

素数定理の証明はいろいろな試行錯誤ののち、1896 年にアダマールとデ・ラ・バレ・プーサンによって与えられました。(110 年か 120 年前ぐらいです。結構最近ですね。) その証明はやや複雑でここには紹介できませんが、その証明ではゼータ関数と呼ばれる関数が活躍します。ここでそのゼータ関数を定義しておきましょう。

定義

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots + \frac{1}{n^s} + \cdots$$

と定め、リーマン (Riemann) のゼータ関数という。

これは次のような素数の積への分解を通して、素数とつながっています。

定理 3 (オイラー積)

$$\zeta(s) = \prod_{p:\text{すべての素数}} \frac{1}{1-\frac{1}{p^s}} = \frac{1}{1-\frac{1}{2^s}} \cdot \frac{1}{1-\frac{1}{3^s}} \cdot \frac{1}{1-\frac{1}{5^s}} \cdot \frac{1}{1-\frac{1}{7^s}} \cdots$$

(証明) 次のような無限積を考える。

$$\left(1+\frac{1}{2^s}+\frac{1}{2^{2s}}+\frac{1}{2^{3s}}+\cdots\right)\cdot\left(1+\frac{1}{3^s}+\frac{1}{3^{2s}}+\frac{1}{3^{3s}}+\cdots\right)\cdot\left(1+\frac{1}{5^s}+\frac{1}{5^{2s}}+\frac{1}{5^{3s}}+\cdots\right)$$
$$\times\left(1+\frac{1}{7^s}+\frac{1}{7^{2s}}+\frac{1}{7^{3s}}+\cdots\right)\cdot\left(1+\frac{1}{11^s}+\frac{1}{11^{2s}}+\frac{1}{11^{3s}}+\cdots\right)\cdots$$

この展開を考えると、素因数分解の一意性から、すべての自然数 n の $\frac{1}{n^s}$ がちょうど一度ずつ現れる。よってこの式は $\zeta(s)$ に等しい。一方で、無限等比級数の公式から

$$1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\frac{1}{p^{3s}}+\cdots=\frac{1}{1-\frac{1}{p^s}}$$

である。よって示された。 (証明終)

素数定理は証明されましたが、では $\mathrm{Li}(x)$ は $\pi(x)$ をどの程度よく近似しているのでしょうか。これに関する次の予想が、100 万ドル (＝約 1 億円!) の懸賞金がかかった問題です。

未解決問題 (リーマン予想)　$\pi(x)$ と $\mathrm{Li}(x)$ の差は、ほぼ $\pm\sqrt{x}\log x$ のオーダーの範囲内に収まる。(厳密にいえば、ある正の定数 C が存在して、常に $|\pi(x)-\mathrm{Li}(x)| < C\sqrt{x}\log x$ が成り立つ。)

これはゼータ関数を使って言い換えることができ、それは『$\zeta(s)$ は s を複素変数の関数として考えたとき、s の実部が $1/2$ より大きい範囲では 0 にならない』となります。(ただし、実際には $\zeta(s)$ を定義する級数は s の実部が 1 以下のときは収束しないので、関数をうまく解析的に延長して (専門用語では解析接続して) 考えることになります。)

2　素数と平方和

素数表に戻って、個数以外の規則について考えてみましょう。
Q：2 以外の素数を、ある単純なルールによって 2 つに分けます。以下は 100 以下の素数ですが、そのルールが分かるでしょうか？

グループ A　5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97
グループ B　3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83

A：4で割った余りで分けています。2以外の素数は奇数なので、余りは1か3です。グループAは4で割った余りが1, グループBは4で割った余りが3です。

ここで、素数pを$p=\square^2+\triangle^2$のように、平方数の和としてかけるかどうかを考えてみます。たとえば、$5, 13$はそのように表せます。

$$5=4+1=2^2+1^2, \qquad 13=9+4=3^2+2^2$$

一方で、少し考えると分かるように、$3, 7, 11$などはそのように表すことはできません。

$$3\neq\square^2+\triangle^2, \quad 7\neq\square^2+\triangle^2, \quad 11\neq\square^2+\triangle^2$$

しばらく試していって感じられる規則は、グループAに属する数(4で割って1余る素数)は必ずそのように表すことができ、グループBに属する数(4で割って3余る素数)は必ずそのように表すことができないということです。実はこのことは一般に成り立ちます。

定理4 (素数と平方和)　奇素数pについて、$p=x^2+y^2$ (x, yは整数) と表されるのはpを4で割った余りが1のときである。

この定理のうち、4で割って3余る素数pがx^2+y^2と表せないことの証明は実はそれほど難しくありません。なぜなら$p=x^2+y^2$ならばx, yは一方が奇数, 他方が偶数となりますが、$x=2m+1, y=2n$とおくと、$x^2+y^2=4m^2+4m+1+4n^2=4(m^2+m+n^2)+1$だから4で割って3余る数にはなりえないからです。問題はこの逆です。たとえば21は4で割ると1余りますが、21はx^2+y^2とは表せません。

$$21\neq\square^2+\triangle^2$$

したがって定理が証明できるとするなら、素数であるという条件をどこかでうまく使わなければなりません。$p=x^2+y^2$のx, yをpで表す単純な公式もありません。たとえば$709=22^2+15^2$という式の$15, 22$は見つかるまで探していくしかないのです。

この定理の証明も、大学数学科の2年生か3年生ぐらいの知識が必要になってしまい、ここで紹介することはできません。それでも、大切なポイントをひとつだけ述べておきましょう。それは、この証明には複素数が使われるということです。大変意外だと思われるかもしれませんが、複素数を使う証明がいちばん分かりやすいのです。

複素数が活躍する理由は、等式

$$x^2+y^2=(x+yi)(x-yi)$$

によります。これをあてはめると、$p=x^2+y^2$と表される数たちは、

$$5=(2+i)(2-i), \quad 13=(3+2i)(3-2i), \quad 17=(4+i)(4-i),$$
$$29=(5+2i)(5-2i), \quad \ldots \quad 709=(22+15i)(22-15i), \quad \ldots$$

と分解されることになります。この素数たちは二つの数の積に分解されたので、もはや素数ではありません(!!)。この『数の範囲を複素数まで広げたときに、4で割って1余

る素数はその広がった数の世界では素数でなくなる』という考え方が証明の基礎になります。

少し問題をアレンジしてみましょう。今度は $p = x^2 + xy + y^2$ という形に素数が書けるかどうかを考えてみます。すると次のような定理が成り立ちます。

定理 5　3 でない素数 p について、$p = x^2 + xy + y^2$ $(x, y$ は整数$)$ と表されるのは p を 3 で割った余りが 1 のときである。

今度の証明では 1 の 3 乗根 ω が活躍します。$x^2 + xy + y^2 = (x - y\omega)(x - y\omega^2)$ と分解されるからです。i は 1 の 4 乗根で ω は 1 の 3 乗根、それぞれに対応する定理が 4 で割った余りと 3 で割った余りになっているのも実は偶然ではありません。しかし、この話題もあまり長く続ける代わりに類似の次の定理を述べて一旦終わりにし、また別の視点から素数を眺めることにしたいと思います。

定理 6　p を 2 でない素数とする。
(1)　$p = x^2 + y^2$ $(x, y$ は整数$)$ と書ける $\Longleftrightarrow$ p を 8 で割った余りが 1 か 5
(2)　$p = x^2 + 2y^2$ $(x, y$ は整数$)$ と書ける $\Longleftrightarrow$ p を 8 で割った余りが 1 か 3
(3)　$p = x^2 - 2y^2$ $(x, y$ は整数$)$ と書ける $\Longleftrightarrow$ p を 8 で割った余りが 1 か 7

（この (1) は先の定理 4 と等価ですが、定理 6 においては (1),(2),(3) は一つのセットになった内容なので再録しました。）

3　素数が作る無限積の公式

また別の面から素数の不思議な性質を紹介します。まず、次の式に注目しましょう。

定理 7

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \cdots = \frac{\pi}{4}$$

(証明) 積分 $\displaystyle\int_0^1 \frac{dx}{1+x^2}$ を考える。$x = \tan\theta$ と置換すると、

$$\int_0^1 \frac{dx}{1+x^2} = \int_0^{\pi/4} \frac{d(\tan\theta)}{1+\tan^2\theta} = \int_0^{\pi/4} \frac{d\theta}{(1+\tan^2\theta)\cos^2\theta} = \int_0^{\pi/4} d\theta = \frac{\pi}{4}$$

となる。一方で $1 - x^2 + x^4 - x^6 + x^8 - x^{10} + \cdots$ は $0 \leq x < 1$ の範囲で収束する無限等比級数でその和は $\frac{1}{1-(-x^2)} = \frac{1}{1+x^2}$ となるから、

$$\begin{aligned}\int_0^1 \frac{dx}{1+x^2} &= \int_0^1 (1 - x^2 + x^4 - x^6 + x^8 - x^{10} + \cdots)dx \\ &= \left[x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \frac{x^9}{9} - \frac{x^{11}}{11} + \cdots\right]_0^1 = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \cdots\end{aligned}$$

よって示された。 (証明終)

一方でこの左辺の和は

$$\prod_{p:2\text{ 以外の素数}} \frac{1}{1-\frac{\chi(p)}{p}} = \frac{1}{1-\frac{-1}{3}}\cdot\frac{1}{1-\frac{+1}{5}}\cdot\frac{1}{1-\frac{-1}{7}}\cdot\frac{1}{1-\frac{-1}{11}}\cdot\frac{1}{1-\frac{+1}{13}}\cdot\frac{1}{1-\frac{+1}{17}}\cdots$$

と等しくなります。ここに、$\chi(p)$ は p の 4 で割った余りが 1 であるか 3 であるかに応じて $1, -1$ とします。等しくなるのはリーマンゼータ関数の場合と同様で、今回は

$$\left(1-\frac{1}{3}+\frac{1}{3^2}-\frac{1}{3^3}+\cdots\right)\cdot\left(1+\frac{1}{5}+\frac{1}{5^2}+\frac{1}{5^3}+\cdots\right)\cdot\left(1-\frac{1}{7}+\frac{1}{7^2}-\frac{1}{7^3}+\cdots\right)$$
$$\times\left(1-\frac{1}{11}+\frac{1}{11^2}-\frac{1}{11^3}+\cdots\right)\cdot\left(1+\frac{1}{13}+\frac{1}{13^2}+\frac{1}{13^3}+\cdots\right)\cdots$$

の展開を考えるとできます。このことから、素数の積に関するこんな公式が得られました。

定理 8

$$\frac{1}{1-\frac{-1}{3}}\cdot\frac{1}{1-\frac{+1}{5}}\cdot\frac{1}{1-\frac{-1}{7}}\cdot\frac{1}{1-\frac{-1}{11}}\cdot\frac{1}{1-\frac{+1}{13}}\cdot\frac{1}{1-\frac{+1}{17}}\cdots=\frac{\pi}{4}$$

このように、素数に関する積[1]に忽然と円周率のような値が姿を現します。そして、p の 4 で割った余りが 1 であるか 3 であるかというのは、定理 4 の $p=\square^2+\triangle^2$ と表せるかどうかという問題に現れた条件そのものでした。実は、あのような素数の分解法則に一つ一つに応じて素数の積に関する整った公式が一つ対応する、という**類体論**と呼ばれる理論があります。たとえば $p=x^2+xy+y^2$ の場合は次の公式になります。

定理 9

$$\frac{1}{1-\frac{-1}{2}}\cdot\frac{1}{1-\frac{-1}{5}}\cdot\frac{1}{1-\frac{+1}{7}}\cdot\frac{1}{1-\frac{-1}{11}}\cdot\frac{1}{1-\frac{+1}{13}}\cdot\frac{1}{1-\frac{-1}{17}}\cdots=\frac{\pi}{3\sqrt{3}}$$

今度は $\frac{\pm1}{p}$ の分子は、p を 3 で割った余りが $1, 2$ に応じて $1, -1$ としています。

4 三角関数の不思議な公式

次のような公式をご覧になったことがあるでしょうか。

定理 10

$$\sin\frac{2\pi}{7}+\sin\frac{4\pi}{7}+\sin\frac{8\pi}{7}=-\left(\sin\frac{6\pi}{7}+\sin\frac{10\pi}{7}+\sin\frac{12\pi}{7}\right)=\frac{\sqrt{7}}{2}$$

[1]なお、$L(s,\chi)=\prod_{p:2\text{ 以外の素数}}\frac{1}{1-\frac{\chi(p)}{p^s}}$ とおくと、定理の左辺は $L(1,\chi)$ になります。$L(s,\chi)$ はディリクレの L 関数とよばれるもので、これもゼータ関数の一種です— 定理 3 の $\zeta(s)$ の式と比べてみてください。

$\sin\frac{2\pi}{7}, \sin\frac{4\pi}{7}$ などの一つ一つの値は複雑ですが、うまく 3 つを選んで和をとると、突然 $\sqrt{7}/2$ とシンプルな値になってしまうという定理です。

証明を紹介しましょう。証明には、ド・モアブルの定理

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$$

を使います。この式は、n に関する帰納法で証明できます。また、n が負の整数のときも成り立ちます。

(定理 10 の証明) $a = \cos\dfrac{2\pi}{7} + i\sin\dfrac{2\pi}{7}$ とおくと、ド・モアブルの定理から

$$a^2 = \cos\frac{4\pi}{7} + i\sin\frac{4\pi}{7}, \quad a^3 = \cos\frac{6\pi}{7} + i\sin\frac{6\pi}{7}, \quad a^4 = \cos\frac{8\pi}{7} + i\sin\frac{8\pi}{7},$$
$$a^5 = \cos\frac{10\pi}{7} + i\sin\frac{10\pi}{7}, \quad a^6 = \cos\frac{12\pi}{7} + i\sin\frac{12\pi}{7}, \quad a^7 = \cos 2\pi + i\sin 2\pi = 1$$

である。よって

$$A = a + a^2 + a^4, \quad B = a^3 + a^5 + a^6$$

とおくと、

$$A = \left(\cos\frac{2\pi}{7} + \cos\frac{4\pi}{7} + \cos\frac{8\pi}{7}\right) + i\left(\sin\frac{2\pi}{7} + \sin\frac{4\pi}{7} + \sin\frac{8\pi}{7}\right)$$

などから、A, B の虚部を求めることになる。ここで $A+B, AB$ を計算してみよう。$a^7 - 1 = 0$ を因数分解すると $(a-1)(a^6 + a^5 + a^4 + a^3 + a^2 + a + 1) = 0$ であり、$a \neq 1$ だから $a^6 + a^5 + a^4 + a^3 + a^2 + a + 1 = 0$ である。よって、

$$\begin{aligned} A + B &= a + a^2 + a^3 + a^4 + a^5 + a^6 = -1, \\ AB &= (a + a^2 + a^4)(a^3 + a^5 + a^6) = a^4(1 + a + a^3)(1 + a^2 + a^3) \\ &= a^4(1 + a + a^2 + 3a^3 + a^4 + a^5 + a^6) \\ &= a^4((1 + a + a^2 + a^3 + a^4 + a^5 + a^6) + 2a^3) = a^4 \cdot 2a^3 = 2a^7 = 2 \end{aligned}$$

である。したがって解と係数の関係から、A, B は 2 次方程式 $t^2 + t + 2 = 0$ の解である。よって $A, B = \dfrac{-1 \pm \sqrt{7}i}{2}$ となる。ここで、$\sin\dfrac{2\pi}{7}, \sin\dfrac{4\pi}{7} > 0$, $\sin\dfrac{8\pi}{7} < 0$ だが、図を書くと $\sin\dfrac{4\pi}{7} + \sin\dfrac{8\pi}{7} > 0$ が分かるので、

$$\mathrm{Im}(A) = \sin\frac{2\pi}{7} + \left(\sin\frac{4\pi}{7} + \sin\frac{8\pi}{7}\right) > 0 + 0 = 0$$

となる。よって $A = \dfrac{-1 + \sqrt{7}i}{2}, B = \dfrac{-1 - \sqrt{7}i}{2}$ となり、これらの虚部を考えると等式が得られた。 (証明終)

この計算の (ほとんど唯一つの) ポイントは、$\{a, a^2, a^3, a^4, a^5, a^6\}$ を $\{a, a^2, a^4\}$ と $\{a^3, a^5, a^6\}$ の二つに分けたところです。言い方を変えれば

$$\{1, 2, 3, 4, 5, 6\} = \{1, 2, 4\} \cup \{3, 5, 6\}$$

という分け方だと言ってもよいでしょう。実は、これ以外の分け方では計算がうまくいきません。例えば、

$$A' = a + a^2 + a^3, \quad B' = a^4 + a^5 + a^6$$

というのも 3 個ずつ二つへの分け方ですが、これだと $A' + B' = -1$ はよくても、$A'B'$ の計算で a が残ってしまいます。

このような三角関数の特別な公式は、7 以外の素数でもあります。少し例を挙げると、例えば素数 11 については、

$$\sin\frac{2\pi}{11} + \sin\frac{6\pi}{11} + \sin\frac{8\pi}{11} + \sin\frac{10\pi}{11} + \sin\frac{18\pi}{11} = \frac{\sqrt{11}}{2}$$

が成り立ちます。ここでは $\{1, 2, 3, \ldots, 10\} = \{1, 3, 4, 5, 9\} \cup \{2, 6, 7, 8, 10\}$ という分け方をしたことがポイントです。(証明は同じ方法でできるので、是非やってみて下さい。) 13 の場合なら、

$$\cos\frac{2\pi}{13} + \cos\frac{6\pi}{13} + \cos\frac{18\pi}{13} = \cos\frac{8\pi}{13} + \cos\frac{20\pi}{13} + \cos\frac{24\pi}{13} = \frac{-1+\sqrt{13}}{4}$$

$$\cos\frac{4\pi}{13} + \cos\frac{10\pi}{13} + \cos\frac{12\pi}{13} = \cos\frac{14\pi}{13} + \cos\frac{16\pi}{13} + \cos\frac{22\pi}{13} = \frac{-1-\sqrt{13}}{4}$$

$$\sin\frac{2\pi}{13} + \sin\frac{6\pi}{13} + \sin\frac{18\pi}{13} = -\left(\sin\frac{8\pi}{13} + \sin\frac{20\pi}{13} + \sin\frac{24\pi}{13}\right) = \frac{1}{2}\sqrt{\frac{13-3\sqrt{13}}{2}}$$

$$\sin\frac{4\pi}{13} + \sin\frac{10\pi}{13} + \sin\frac{12\pi}{13} = -\left(\sin\frac{14\pi}{13} + \sin\frac{16\pi}{13} + \sin\frac{22\pi}{13}\right) = \frac{1}{2}\sqrt{\frac{13+3\sqrt{13}}{2}}$$

などです。このような分け方の一般的な法則は、ガウスによって 1796 年に発見され、それによって正 17 角形は作図可能であることが証明されました。

定理 11 (ガウスの定理) 正 17 角形は作図可能である。具体的には、

$$\cos\frac{2\pi}{17} = \frac{-1+\sqrt{17}}{16} + \frac{1}{8}\sqrt{\frac{17-\sqrt{17}}{2}} + \frac{1}{4}\sqrt{\frac{17+3\sqrt{17}}{4} - \frac{1}{2}\sqrt{\frac{17-\sqrt{17}}{2}} - \sqrt{\frac{17+\sqrt{17}}{2}}}$$

と計算され、定木とコンパスを用いると、四則及び開平が作図可能なので、作図可能となる。また、正 257 角形、正 65537 角形も作図可能である。

正 5 角形については、

$$\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}, \quad \sin\frac{2\pi}{5} = \frac{1}{2}\sqrt{\frac{5+\sqrt{5}}{2}}$$

に相当する式は紀元前から知られていたことから、正5角形は作図可能と分かっていましたが、7以上の素数個の頂点をもつ正多角形は作図可能ではないのではないかと考えられていました。正5角形以来の世界記録を2000年ぶりに更新したガウスの研究は、当時の数学界においてかなりセンセーショナルな事件だったようです。

話を素数7の場合 (定理10) に戻します。実は定理10も、素数の2次式による表示やゼータ関数の値と関係しています。$p \neq 7$ に対して、$\chi_7(p)$ を

$$\chi_7(p) = \begin{cases} 1 & p \text{を} 7 \text{で割った余りが} 1,2,4 \\ -1 & p \text{を} 7 \text{で割った余りが} 3,5,6 \end{cases}$$

とおきましょう。これが定理10とその証明にでてきた $\{1,2,3,4,5,6\} = \{1,2,4\} \cup \{3,5,6\}$ という分け方に対応したものであることは一目瞭然でしょう。これについて次の定理が成り立ちます。

定理12 (1) p を7以外の素数とするとき、$p = x^2 + xy + 2y^2$ (x, y は整数) と表せる条件は、p を7で割った余りが $1,2,4$ のいずれかになること、つまり $\chi_7(p) = 1$ である。

(2)
$$\prod_{p:7 \text{ 以外の素数}} \frac{1}{1 - \frac{\chi_7(p)}{p}} = \frac{1}{1-\frac{+1}{2}} \cdot \frac{1}{1-\frac{-1}{3}} \cdot \frac{1}{1-\frac{-1}{5}} \cdot \frac{1}{1-\frac{+1}{11}} \cdot \frac{1}{1-\frac{-1}{13}} \cdot \frac{1}{1-\frac{-1}{17}} \cdots = \frac{\pi}{\sqrt{7}}$$

11の場合も対応する定理があります。$p \neq 11$ に対して、$\chi_{11}(p)$ を

$$\chi_{11}(p) = \begin{cases} 1 & p \text{を} 11 \text{で割った余りが} 1,3,4,5,9 \\ -1 & p \text{を} 11 \text{で割った余りが} 2,6,7,8,10 \end{cases}$$

とおきます。

定理13 (1) p を11以外の素数とするとき、$p = x^2 + xy + 3y^2$ (x, y は整数) と表せる条件は、$\chi_{11}(p) = 1$ である。

(2)
$$\prod_{p:11 \text{ 以外の素数}} \frac{1}{1 - \frac{\chi_{11}(p)}{p}} = \frac{1}{1-\frac{-1}{2}} \cdot \frac{1}{1-\frac{+1}{3}} \cdot \frac{1}{1-\frac{+1}{5}} \cdot \frac{1}{1-\frac{-1}{7}} \cdot \frac{1}{1-\frac{-1}{13}} \cdot \frac{1}{1-\frac{-1}{17}} \cdots = \frac{\pi}{\sqrt{11}}$$

つまり、定理10のような三角関数の特別な公式は、ただそれだけで存在しているのではなく、素数を2次式で表す条件や、素数が作る無限積 (＝ゼータ関数) の値が円周率 π などによる整った数で表されることと繋がって現れてくるものなのです。これらの関係は、すべて類体論という理論によって統合されています。

5　おわりに

短い間にたくさんの公式を紹介しましたが、いかがだったでしょうか。個人的な経験になりますが、私は子供のころ、算数や数字は好きでしたが、素数のことは実はあまり

好きにはなれませんでした。あまりにも秩序がなくてんでばらばらで、例えば $\frac{1}{8} = 0.125$ のように割り切れる 8 などの数の方がスッキリしていると思ったからです。でも、素因数分解によって整数の世界の “原子” の役割を持つ素数は、実はそれ自身奥深い調和の取れた法則をたくさん持っています。そのことが発見されたのは早く見積もっても 17 世紀以降のフェルマーの研究以降のことで、本格的な研究は 18 世紀以降になります。複素数や関数など、一見整数とは遠く離れたものたちとの関係が発見されることで、整数論は実り多い豊かな理論になりました。20 世紀以降、整数論は幾何学との関係が特に顕著となり、1995 年に証明されたフェルマーの最終定理も、この関係が基礎になりました。また、最近は佐藤-テイト予想と呼ばれる整数論の大予想が証明されて (2006 年に部分的証明、2009 年に完全な証明)、整数論関係者はびっくりしています。そんな現在でも、素数の法則については分からないことが驚くほどたくさんあり、これらを探求する試みが続いています。今回はこのような話題は紹介できませんでしたが、興味のある方は、以下に紹介する本をお読みいただけたらと思います。

6　数学の本の紹介

私がこれまで読んできて面白いと感じた数学の本を何冊か紹介して、本稿を終わりたいと思います。私の個人的な好みでしかありませんが、何かのご参考になれば幸いです。

6.1　整数論の入門書

整数論の入門的な教科書としては、

・『数論入門』山本 芳彦 著（岩波書店）

がお薦めです。また、

・『数論序説』小野 孝 著（裳華房）

も、『数論入門』より少しレベルは高くなりますが、教育的配慮の行き届いた教科書です。

・『数論〈1〉Fermat の夢と類体論』『数論〈2〉岩沢理論と保型形式』黒川 信重, 斎藤 毅, 栗原 将人 著（岩波書店）

では、非常に幅広い整数論のテーマを多くの具体例を用いて紹介してあります。本稿の内容もすべて『数論〈1〉』に含まれていると言えます。素数定理の証明もあります。

最近の整数論の発展を扱った本としては、

・『フェルマーの最終定理・佐藤 - テイト予想解決への道 (類体論と非可換類体論) 』加藤和也著（岩波書店）

・『数学のたのしみ〈2008 最終号〉フォーラム:現代数学のひろがり 佐藤 - テイト予想の解決と展望 』（日本評論社）

があります。いずれも、入門的な題材が豊富に取り上げてあり、読みやすい本です。また、

・『解決!フェルマーの最終定理―現代数論の軌跡』加藤 和也著 (日本評論社)

は絶版ですが、ユニークな比喩が面白い (例えば “楕円曲線 vs ゴジラ” など!)、そして一見してはそのように見えにくいけれど、実は本格的な内容も随所に散りばめられてあるすばらしい本なので、見かけたら是非手に取ってみてください。

6.2 数学の読み物

・『フェルマーの最終定理』サイモン・シン著（新潮文庫）

360 年の年月を経て証明されたフェルマーの最終定理には多くのエピソードや人間ドラマがあります。それらが生き生きと描かれています。また、現代数学者事情を知るための格好の本とも思われます。著者のサイモンシンさんは優れたサイエンスライターで、『暗号解読』『宇宙創成』（新潮文庫）も非常に面白いと感じました。

・『すうがく博物誌』森 毅 著, 安野 光雅 イラスト（童話屋）

半分絵本みたいな本で、各ページ読みきりの小学生でも楽しめるような本です。それなのに数学のことはとてもよく書けていて、カジュアルながらちゃんと楽しめる数学の本です。

・『放浪の天才数学者エルデシュ』ポール・ホフマン著（草思社）

職も家も家族も持たず、世界中の数学者を訪れては相手が疲れ果てるまでぶっ続けで共同研究をする。そんな人生を本当に生きた 20 世紀の数学者エルデシュの伝記です。とても面白く読みやすく書かれています。

・『無限の天才—夭逝の数学者・ラマヌジャン』ロバート・カニーゲル 著（工作舎）

インドの魔術師とも呼ばれた数学者ラマヌジャンの本格的な伝記です。寝ている間に夢で女神が教えてくれる、と朝起きるたびにノートに書き付けた未知の不思議な公式は、彼の没後以降も長く研究され、数学の進展に大きく寄与することになりました。厚い本格的な本ですが、ラマヌジャンの人物像に興味のある方はぜひお読みいただきたいと思います。

・『偉大な数学者たち』岩田 義一著 (ちくま学芸文庫)

アルキメデスからガロア・アーベルまで、数学の虜となった数学者たちの伝記です。