中学生のための玉原数学教室　　東京大学玉原国際セミナーハウス
講義 (2)　桂　利行　　2008年9月28日

「素数さん、こんにちは」

1　素数とは

整数の集合を $\mathbf{Z}$ と書く:

$$\mathbf{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$$

整数のことを**有理整数**ということもある. 1以上の整数を**自然数**と呼ぶ. $1, 2, 3, \cdots$ と続く数列に属する数のことである. **自然数**の集合を $\mathbf{N}$ と書く:

$$\mathbf{N} = \{1, 2, 3, \cdots\}$$

整数 $a, b \in \mathbf{Z}$ に対し, ある整数 q が存在して

$$b = aq$$

となるとき, a は b を**割り切る**, あるいは a は b の**約数**であるという. b を主体にいえば, b は a で**割り切れる**, あるいは b は a の**倍数**であるという. a が b を**割り切る**ことを $a|b$ と表す. a が b を割り切る時, $-a$ も b を割り切るから, 約数といった場合には正の約数を意味するものとする.

整数 a, b に対し, a と b の共通の約数を**公約数**という. a と b の公約数のうちで最大のものを a と b の**最大公約数**といい, $\gcd(a, b)$ と書く. a と b の最大公約数が1になるとき, a と b は**互いに素**であるという. a と b が互いに素であるとは, 共通の約数が1しかないということである.

例 1.1 $\gcd(4, 6) = 2$ である. また, 8と9は互いに素である.

1と自分自身以外の約数を**真の約数**という. 2以上の整数が真の約数をもたないとき, **素数**という. 素数は

$$2, 3, 5, 7, 11, 13, 17, \cdots$$

と続き, 無限個存在することが知られている. 2以上の整数が真の約数を持つとき**合成数**という.

$$4, 6, 8, 9, 10, \cdots$$

などは合成数である. 素数の世界には不思議な現象が数多くあり, 多くの研究者の興味を惹いている. 素数に関する興味ある結果をご紹介しておこう.

(1) （**ディリクレの定理**）a, k を互いに素な自然数とすれば,

$$kn+a \quad (n=1,2,\cdots)$$

の中に素数が無限に存在する. たとえば, $4n+1$ $(n=1,2,\cdots)$ には素数が無限個含まれている.

(2) （**チェビシェフの定理**）$a>1$ とすれば, $a<p<2a$ なる素数 p が必ず存在する.

(3) いくらでも大きな区間でその間に素数が存在しない区間が存在する.

(4) 素数 p が適当な整数 x, y を用いて

$$p=x^2+y^2$$

と表示できるための必要十分条件は, $p=2$ または p を 4 で割って 1 余ることである.

素数に関する未解決の問題を２つご紹介しよう.

双子素数

3 と 5, 5 と 7, 11 と 13, 17 と 19 のように, 偶数をはさむ２つの素数を**双子素数**という. 双子素数は無限個存在すると予想されているが証明されていない.

ゴールドバッハの予想

4 以上の偶数は２つの素数の和として表されると予想されている. $4=2+2, 6=3+3, 8=5+3, 10=7+3, 12=7+5$ $14=7+7, 16=11+5$ など.

2 約数の数

任意の自然数は素数の積に因数分解されるという大事な性質がある.

命題 2.1 任意の合成数は素数の積に分解することができる. また, その分解は積の順序を除いて一意的である

例 2.2 72 は $72=2^3\cdot 3^2$ と因数分解される.

n を素因数分解したとき, 同じ素数はひとつにまとめて次のように書く.

$$n=p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}$$

ここに, p_i $(i=1,2,\cdots,t)$ は相異なる素数である.

自然数 n の約数が何個あるか数えてみよう. まず, 感じをつかむために例をあげよう.

例 2.3 $72 = 2^3 \cdot 3^2$ の約数は $2^a \cdot 3^b$ $(0 \leq a \leq 3, 0 \leq b \leq 2)$ の形をしている．a の取り方は 4 通り，b の取り方は 3 通りだから，約数の個数は

$$4 \times 3 = 12$$

である．

一般の自然数

$$n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$$

の約数は，p_i $(i = 1, 2, \cdots, t)$ の積で，各 p_i は e_i 回以下現れるものである．したがって，p_i の現れる回数は，0 から e_i の $1 + e_i$ 通りである．よって全体では

$$(1 + e_1)(1 + e_2) \cdots (1 + e_t)$$

通りの約数が存在する．それでは，それらの約数の全ての和を計算してみよう．そのために，次のような式を考える:

$$(1 + p_1 + p_1^2 + \cdots + p_1^{e_1})(1 + p_2 + p_2^2 + \cdots + p_2^{e_2}) \cdots (1 + p_t + p_t^2 + \cdots + p_t^{e_t})$$

この式を展開すれば，その項の中に n の約数が 1 度ずつ出て来る．したがって，この式の値が n の約数すべての和と等しくなる．この式を $S(n)$ と書けば

$$S(n) = \frac{p_1^{e_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{e_2+1} - 1}{p_2 - 1} \cdots \frac{p_t^{e_t+1} - 1}{p_t - 1}$$

となる．

3 完全数とメルセンヌ素数

自然数 n は自分自身を除く約数の和が n になるとき**完全数**という．例えば，6 の自分自身を除く約数は

$$1, 2, 3$$

の 3 個で，その和は 6 になるから，6 は完全数である．また，28 の自分自身を除く約数は

$$1, 2, 4, 7, 14,$$

の 5 個であるが、その和は 28 になるから，28 は完全数である．それでは，少し高級な話になるが，完全数がどのくらいあるか調べてみよう．$S(n)$ には自分自身も約数の 1 つとして足してしまっているから，n が完全数となるための必要十分条件は

$$S(n) = 2n$$

ということになる．偶数の完全数はオイラーが証明した次の定理によって完全に決定できる．

定理 3.1 $n = 2^{\ell-1}(2^\ell - 1)$ において $2^\ell - 1$ が素数であるならば, n は完全数である. 逆に, 偶数の完全数は素数になる $2^\ell - 1$ をとって, すべてこの形で与えられる.

前半を示すには, 実際に約数すべての和を計算する. $p = 2^\ell - 1$ とおけば, p が素数であることから, $n = 2^{\ell-1}(2^\ell - 1)$ の約数は 2^i または $2^i p$ の形である. すべての約数の和は

$$\begin{aligned} S(n) &= \textstyle\sum_{i=0}^{\ell-1} 2^i + \sum_{i=0}^{\ell-1} 2^i p \\ &= (2^\ell - 1) + (2^\ell - 1)p \\ &= (2^\ell - 1)(p+1) \\ &= 2^\ell(2^\ell - 1) = 2n \end{aligned}$$

となる. よって, n は完全数である.

逆に n を偶数の完全数とし,

$$n = 2^{\ell-1}m,\ \ell > 1,\ m \text{ は } 2 \text{ で割り切れない}$$

とおく. n は完全数だから

$$S(n) = 2n = 2^\ell m$$

となる. 一方,

$$S(n) = S(2^{\ell-1})S(m) = (1 + 2 + 2^2 + \cdots + 2^{\ell-1})S(m) = (2^\ell - 1)S(m)$$

であるから,

$$2^\ell m = (2^\ell - 1)S(m)$$

となる. よって,

$$S(m) = m + m/(2^\ell - 1)$$

を得る. この左辺は整数であるから $m/(2^\ell - 1)$ は整数でなければならない. また, $\ell > 1$ を考えれば $m/(2^\ell - 1)$ は m より真に小さく, したがって, $m/(2^\ell - 1)$ は m の真の約数である. $S(m)$ は m の約数すべての和だが, 右辺をみれば m の約数は 2 個しかないから, n の約数は 2 個しかないはずで, m は素数でなければならない. よって,

$$m/(2^\ell - 1) = 1$$

となる. ともかく, このことから $2^\ell - 1 = m$ は素数となる. 以上で, 偶数の完全数はすべて

$$n = 2^{\ell-1}(2^\ell - 1) \quad (\text{ただし } 2^\ell - 1 \text{ は素数})$$

の形となる.

奇数の完全数は一つも知られておらず, もし存在したとしても大変大きな数になることが知られている.

ここで, 自然数 $2^\ell - 1$ を調べてみよう. 自然数 $2^\ell - 1$ が素数であるためには ℓ が素数でなければならない.

なぜならば, $\ell = ab$ と 2 以上の 2 つの自然数 a, b の積に書ければ,

$$2^\ell - 1 = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1)$$

となって因数分解されてしまうからである.

$\ell = 2$ なら $2^\ell - 1 = 3$ は素数で対応する完全数は $2^{\ell-1}(2^\ell - 1) = 6$,

$\ell = 3$ なら $2^\ell - 1 = 7$ は素数で対応する完全数は $2^{\ell-1}(2^\ell - 1) = 28$

となる. これらが完全数であることはすでに述べた.

ℓ が素数でも $2^\ell - 1$ が素数になるとは限らないが, $2^\ell - 1$ の形に書ける素数を**メルセンヌ素数**という. コンピュータによる素数判定によって 2007 年末現在, 44 個のメルセンヌ素数が発見されている. その中で最大のメルセンヌ素数は

$$2^{32582657} - 1$$

であり, その桁数は 9808358 桁である. このメルセンヌ素数が 2007 年末現在具体的に知られている最大の素数である. また, メルセンヌ素数と偶数の完全数は 1 対 1 に対応するから, 完全数は 2007 年末現在 44 個知られていることになる.

参考文献

高木貞治著「初等整数論講（第 2 版）」(共立出版, 1971)

完全数とメルセンヌ素数

メルセンヌ素数 $M(\ell) = 2^{\ell} - 1$
完全数 $M(\ell) = 2^{\ell-1}(2^{\ell} - 1)$

No	ℓ	$M(\ell)$ 桁数	$P(\ell)$ 桁数	発見者
1	2	1	1	---- ----
2	3	1	2	---- ----
3	5	2	3	---- ----
4	7	3	4	---- ----
5	13	4	8	1456 anonymous
6	17	6	10	1588 Cataldi
7	19	6	12	1588 Cataldi
8	31	10	19	1772 Euler
9	61	19	37	1883 Pervushin
10	89	27	54	1911 Powers
11	107	33	65	1914 Powers
12	127	39	77	1876 Lucas
13	521	157	314	1952 Robinson
14	607	183	366	1952 Robinson
15	1279	386	770	1952 Robinson
16	2203	664	1327	1952 Robinson
17	2281	687	1373	1952 Robinson
18	3217	969	1937	1957 Riesel
19	4253	1281	2561	1961 Hurwitz
20	4423	1332	2663	1961 Hurwitz
21	9689	2917	5834	1963 Gillies
22	9941	2993	5985	1963 Gillies
23	11213	3376	6751	1963 Gillies
24	19937	6002	12003	1971 Tuckerman
25	21701	6533	13066	1978 Noll & Nickel
26	23209	6987	13973	1979 Noll
27	44497	13395	26790	1979 Nelson & Slowinski
28	86243	25962	51924	1982 Slowinski
29	110503	33265	66530	1988 Colquitt & Welsh
30	132049	39751	79502	1983 Slowinski
31	216091	65050	130100	1985 Slowinski
32	756839	227832	455663	1992 Slowinski & Gage et al.
33	859433	258716	517430	1994 Slowinski & Gage
34	1257787	378632	757263	1996 Slowinski & Gage
35	1398269	420921	841842	1996 Armengaud, Woltman, et al. (GIMPS)
36	2976221	895932	1791864	1997 Spence, Woltman, et al. (GIMPS)
37	3021377	909526	1819050	1998 Clarkson, Woltman, Kurowski et al. (GIMPS, PrimeNet)
38	6972593	2098960	4197919	1999 Hajratwala, Woltman, Kurowski et al. (GIMPS, PrimeNet)
39	13466917	4053946	8107892	2001 Cameron, Woltman, Kurowski et al. (GIMPS, PrimeNet)
??	20996011	6320430	12640858	2003 Shafer, Woltman, Kurowski et al. (GIMPS, PrimeNet)
??	24036583	7235733	14471465	2004 Findley, Woltman, Kurowski et al. (GIMPS, PrimeNet)
??	25964951	7816230	15632458	2005 Nowak, Woltman, Kurowski et al. (GIMPS, PrimeNet)
??	30402457	9152052	18304103	2005 Cooper, Boone, Woltman, Kurowski et al. (GIMPS, PrimeNet)
??	32582657	9808358	19616714	2006 Cooper, Boone, Woltman, Kurowski et al. (GIMPS, PrimeNet)