高校生のための現代数学講座　　東京大学
「素数の世界」　　玉原国際セミナーハウス
講義 (1)　桂　利行　　2009 年 7 月 25 日

「素数, 倍数, 約数, 因数分解」

１から始まり, １ずつ増える数列 $\{1, 2, 3, \cdots\}$ に含まれる数を**自然数**という. 自然数とそのマイナスの数および 0 のなす集合を $\mathbf{Z}$ と書き, $\mathbf{Z}$ に属する数を**整数**という：

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

状況をより明確にしたい場合には整数のことを**有理整数**という.

次の定理は整除性の基本となる.

定理 0.1 a を自然数, b を整数とするとき

$$b = qa + r, \quad 0 \leq r < a$$

となるような整数 q, r がただ一組存在する.

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 b は a で**割り切れる**, あるいは a は b の**約数**である, 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. b が a で割り切れない時, $a \not| b$ と書く. 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. 2 で割り切れる整数を**偶数**, ２で割り切れない整数を**奇数**という. 1 と自分自身以外では割り切れない自然数を**素数**という.

素数が無限個あることは古代ギリシャから知られていた. 証明は背理法で行う. 素数が有限個しかないとして, それらのすべてを p_1, p_2, $\cdots$, p_m とする. 自然数 $n = p_1 p_2 \cdots p_m + 1$ を考える. どんな自然数も素数の積に分解するから, n はある素数で割り切れるはずである. しかし, n は $p_1, \cdots, p_m$ のいずれでも割り切れないから矛盾である. よって素数は無限個なければならない.

後に述べるように大きな素数は暗号に応用することができるため, 大きな素数を見つけることは重要な問題である. 先に示したように素数は無限に存在するから, いくらでも大きな素数が存在するはずである. しかし, 具体的に大きな素数を見つけることは大変難しい問題である. 2006 年 6 月現在知られている最大の素数は $2^{30402457} - 1$

であり, その桁数は約 915 万桁. コンピュータを用いた計算によって, 素数であることが示された. この素数のように, $2^n - 1$ の形の素数を**メルセンヌ** (M. Mersenne) **素数**という. この形の整数は素数になるものを多く含んでおり, 2006 年 6 月現在, 素数になる n が 43 個知られている.

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. ここでは, 未解決の問題を 2 つご紹介しておこう.

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.

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. $4 = 2 + 2$, $6 = 3 + 3$, $8 = 5 + 3$, $10 = 7 + 3$, $12 = 7 + 5$ など. この予想は**ゴールドバッハ** (Goldbach) **の予想**と呼ばれている.

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.

任意の自然数は一意的に素因数分解される. すなわち, 任意の自然数 n に対し相異なる有限個の素数 $p_1, p_2, \cdots, p_k$ と自然数 $e_1, e_2, \cdots e_k$ が存在して

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

と, 積の順序を除いて一意的に表示される.