素 数 の は な し

小川 裕之　(大阪大学大学院 理学研究科)[†]

§1.　素数は無数にあります

自然数 a が自然数 b で割り切れるとき, a は b の **倍数**, b は a の **約数** といいます. 1 より大きい自然数で, 1 と自分自身以外に約数を持たないものを **素数** といい, 約数の中で素数であるものを **素因数** といいます. 最も小さい素因数を **最小素因数**, 最も大きい素因数を **最大素因数** といいます. 自然数 a, b の両方の約数となる自然数を a, b の **公約数** といい, 最も大きい公約数を **最大公約数** といいます. 自然数 a, b について, 最大公約数が 1 となるとき, **互いに素** といいます. $12 = 2\times2\times3$ や $15 = 3\times5$ のように, 自然数を素数の積に表すことができます. これを **素因数分解** といいます.

整数論の基本定理　すべての自然数は, ただ一通りの仕方で素因数分解される.

物質における原子のように, 素数は数の世界の最も基本的な構成要素です. その役割はとても重要です. さてその原子というべき素数は, いったい幾つあるのでしょうか？

定理　無数に多くの素数がある.

記録にある最初の証明は, ギリシャ時代のユークリッドのもので, 今では数えきれないくらい多くの種類の証明があります. 今日はその中から 3 種類の証明を紹介します.

§2.　ユークリッド (Euclid) の証明

最初に紹介する証明は, ユークリッドによるものとその類似形です. あらかじめ用意した n 個の素数 $p_1, p_2, \ldots, p_n$ に対して, それらで割り切れない自然数を作れば整数論の基本定理により新しい素数が得られます. 幾らでも新しい素数がみつかるので, 素数が無数にあることがわかります.

2.1. ユークリッド (Euclid) の証明

$N = p_1\times p_2\times\cdots\times p_n + 1$ は $p_1, p_2, \ldots, p_n$ で割り切れない.

2.2. クンマー (Kummer) の証明 (1878)

$N = p_1\times p_2\times\cdots\times p_n - 1$ は $p_1, p_2, \ldots, p_n$ で割り切れない.

2.3. スティルチェス (Stieltjes) の証明 (1890)

$p_1\times p_2\times\cdots\times p_n = L\times M$ と 2 数に分ける. $N = L + M$ は $p_1, p_2, \ldots, p_n$ で割り切れない.

2.4. メトロ (Métrod) の証明 (1917)

$M = p_1\times p_2\times\cdots\times p_n$ とする. $N = M/p_1 + \cdots + M/p_n$ は $p_1, p_2, \ldots, p_n$ で割り切れない.

§3.　ユークリッドの証明に沿って素数を沢山作ってみましょう

ユークリッドらの証明手順に従って, 新しい素数をみつけることができます. 実際にユークリッドの証明 (2.1) をたどってみましょう. $p_1 = 2$ からはじめましょう.

① $p_1 = 2$
② $p_1 + 1 = 2 + 1 = 3$ は素数なので　$p_2 = 3$
③ $p_1\times p_2 + 1 = 2\times3 + 1 = 7$ も素数　$p_3 = 7$
④ $p_1\times p_2\times p_3 + 1 = 2\times3\times7 + 1 = 43$ も素数　$p_4 = 43$
⑤ $p_1\times p_2\times p_3\times p_4 + 1 = 2\times3\times7\times43 + 1 = 1807 = 13\times139$ 小さい方の素数をとって　$p_5 = 13$
⑥ $p_1\times p_2\times p_3\times p_4\times p_5 + 1 = 23479 = 53\times443$ 小さい方の素数をとって　$p_6 = 53$

[†] 〒 560-0043　大阪府豊中市待兼山町 1-1　ogawa@math.sci.osaka-u.ac.jp
2014 年 11 月 10 日　於　奈良県立奈良高等学校

⑦ $p_1{\times}p_2{\times}p_3{\times}p_4{\times}p_5{\times}p_6+1=1244335$　素因数分解は面倒そう. でも $\cdots$　$p_7=5$

⑧ $p_1{\times}p_2{\times}p_3{\times}p_4{\times}p_5{\times}p_6{\times}p_7+1=6221671$　最小素因数は $\cdots$?

実は 6221671 は素数でなので 8 つ目の素数は $p_8=6221671$ です. 9 つ目の素数はいくつでしょうか ? 答えは 14 桁の素数 38709183810571 です. では, 10 番目の素数はいくつでしょうか ?

問題　こうしてすべての素数を見つけることができるのだろうか ?

最小素因数でなく, 最大素因数を選んだ場合には, 現れない素数があることが示されていますが, 現れない素数が無数にあるかどうはわかっていません (Cox–van der Poorten, 1968). このようなことを確かめるために, 実際に計算してみようとするとすぐに困難に出会います. 素数を沢山掛けるのも大変ですが, それに 1 を足した数を素因数分解するのはもっともっと大変です.

問題　素因数分解しなくてもいいような, 素数が沢山出てくる系列をつくれないだろうか ?

3.1.　フェルマー (Fermat) はフェルマー数という系列を考えました.

フェルマー数　$F_m=2^{2^n}+1$　$(n\geqq 0)$

$F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$, $F_4=65537$ は素数です. フェルマーは, すべてのフェルマー数が素数であろうと予想しました (1650). ところがオイラー (Euler) は F_5 (= 4294967297) が 641 で割り切れることを見出しました (1732). 計算機のない時代に大きい数の素因数を求めるのはとても難しく, 超一流の数学者オイラーによって到達しえた金字塔です. 現在では多くのフェルマー数が素数でないことが計算されています. 素数は他にみつかっていません. 素数のフェルマー数はこの 5 つだけであろうと考えられています. ガウス (Gauss) は, 正 17 角形の作図 (1796) から, 素数のフェルマー数が正多角形の作図問題の解答であることを指摘し, 整数論の進むべき方向を指し示しました.

3.2.　メルセンヌ (Mersenne) 数という系列もあります.

メルセンヌ数　$M_q=2^q-1$　(q は素数)

$M_2=3$, $M_3=7$, $M_5=31$, $M_7=127$ は素数です. 素数のメルセンヌ数をメルセンヌ素数と言います. $M_{11}=2047=23{\times}89$ は素数ではありませんが, M_{13}, M_{17}, M_{19} は素数です. メルセンヌ素数が無数にあるかどうかも, 素数にならないメルセンヌ数が無数にあるかどうかもわかっていません. 現在 48 個のメルセンヌ素数がみつかっています. 35 番目からの 14 個は, 1996 年に始まったプロジェクト GIMPS (`http://www.mersenne.org/primes/`) の成果です. 2013 年 1 月 25 日にみつかったメルセンヌ素数 $M_{57885161}$ は 1742 万 5170 桁の素数で, 現在知られている最大の素数です.

歴史や記録など素数について興味のあるかたは, The Prime Pages (`http://primes.utm.edu/`) が参考になるでしょう.

§4.　フルビッツ (Hurwitz) の問題

前節でふれたフェルマー数 F_n は次の関係式を満たします.

$$F_n-2=F_0{\times}F_1{\times}\cdots{\times}F_{n-1}$$

因数分解の公式 $x^2-1=(x-1)(x+1)$ を繰り返し使って証明できます.

4.1. ゴールドバッハ (Goldbach) の証明 (1730)

$n>m$ とすると, 上の関係式より F_n を F_m で割ったあまりは 2 です. フェルマー数は奇数なので, F_n と F_m は互いに素です. フェルマー数 F_n から素因子 p_n をひとつずつ選ぶと, p_1, p_2, ... と無数に多くの異なる素数が得られます.

4.2. フルビッツ (Hurwitz) の問題 (1891)

1 より大きな自然数の系列 A_1, A_2, $\cdots$ で, どの 2 つをとっても互いに素になるものをみつけよ.

フェルマー数がこの自然数の系列の一例で, A_1, A_2, $\cdots$ のそれぞれから素因数をひとつずつ選べば, 無数に多くの異なる素数が得られます.

4.3. エドワーズ (Edwards) の解 (1964)

a, B_0 を互いに素な自然数とし, 自然数 $n \geqq 1$ に対して $B_n = B_{n-1} \times (B_{n-1} - a) + a$ とおきます. $n \neq m$ に対して B_n と B_m は互いに素です. 特に $a = 2$, $B_0 = 3$ とすると, フェルマー数 F_n が現れます. C_0 を奇数とし, $C_n = C_{n-1}^2 - 2$ $(n \geqq 1)$ とおきます. $m \neq n$ に対して C_m と C_n は互いに素になります.

4.4. ベルマン (Bellman) の定理 (1947)

$f(x)$ を定数でない多項式で次の条件 (i) (ii) を満たすものとする.

(i) 整数 k が $f(0)$ と互いに素ならば $f(k)$ と $f(0)$ も互いに素.

(ii) $f(f(0)) = f(0)$

$f(0)$ と互いに素な k について, k, $f(k)$, $f(f(k))$, $f(f(f(k)))$, $\cdots$ のどの 2 つも互いに素になる.

$f(x) = (x-1)^2+1$ はベルマンの定理の条件 (i) (ii) をみたします. $k = 3$ ととれば, $f(3) = 2^2+1 = F_1$, $f(f(3)) = (2^2)^2 + 1 = 2^{2^2} + 1 = F_2$, $f(f(f(3))) = \cdots = F_3$ となりフェルマー数が現われます. 同様にエドワーズの系列 B_0, B_1, B_2, $\cdots$ や C_0, C_1, C_2, $\cdots$ をベルマンの定理の系列として与える多項式が簡単に見つかります.

4.5. ショルン (Schorn) の証明 (1988)

自然数 n について, $(n!) + 1$, $(n!)2 + 1$, $\cdots$, $(n!)(n-1) + 1$ はどの 2 つをとっても互いに素である. それぞれから素因数を 1 つずつ選んで n 個の異なる素数が得られる.

§5. オイラー (Euler) の証明

5.1. オイラー (Euler) の証明 (1737/1748)

素数の逆数の和 $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \cdots$ を考えます. 素数が有限個しかないならこの和は原理的に計算でき, 有限の値に定まるはずです. 実際にはこの和は幾らでも大きくなることが証明されるので, 素数は有限個ではないことがわかります.

素数の逆数の和を考えるというオイラーの着想は, 代数的に定義された素数を知るのに解析学を使った最初のもので, 整数論で最も重要な考え方のひとつです. オイラーの考え方を発展させて, ディリクレ (Dirichet) は次の定理を証明しました.

5.2. ディリクレ (Dirichet) の算術級数定理 (1837)

互いに素な自然数 $d \geqq 2$, a について, a, $a + d$, $a + 2\,d$, $\cdots$ の中に素数が無数に現われる.

a, $a + d$, $a + 2d$, $\cdots$ は一般に $a + d\,(n - 1)$ $(n \geqq 1)$ と n の一次式で表されます. ディリクレの算術級数定理は, 『一次式で与えられる数の系列の中に素数が無数に現われる』と言いかえられます.

問題 二次以上の次数の多項式で与えられる数の系列の場合はどうなのでしょうか ?

多項式が因数分解されると素数は全然出てこなくなるので, 上の問題は既約な多項式で考えることになります. $n^2 + 1$ の場合でさえ, その中に素数が無数に現われるかどうか全くわかっていません. 一次式以外の系列で素数が無数に出てくるものは現在ひとつもみつかっていません.

5.3. 双子素数というものがあります. 3 と 5, 5 と 7, 11 と 13, 17 と 19, $\cdots$ のように, p も $p + 2$ も素数になる組のことです. 双子素数が無数にあるのかどうかまだわかっていません. 1919 年にブラン (Brun) は, 双子素数の逆数の和 $(\frac{1}{3} + \frac{1}{5}) + (\frac{1}{5} + \frac{1}{7}) + (\frac{1}{11} + \frac{1}{13}) + \cdots$ が有限の値に定まることを証明しました. この和はブラン定数と呼ばれ, 最新の近似値は 1.902160583104 (Sebah, 2002) です.

2013 年, 素数の間隔について張益唐 (Zhang Yitang) により驚くべき結果が得られました. 素数の間隔が 7000 万以下のものが無数に多く存在することが示されました (Ann. of Math. 2014). 双子素数の問題 (素数の間隔が 2) に比べるとまだまだ大きな開きがありますが, 手掛かりの乏しかった双子素数の問題が一気に手が届くところに来たという印象があります. 今世紀中には何とかなるのではないでしょうか. Zhang の結果は研究者にとって真に驚くべきものなのです.

§6. 素数はどのくらい沢山あるのでしょうか？

ともかく素数は無数にあるのですが, 実際にどのぐらいあるのか個数を数えてみましょう. 正の数 x に対して,

$$\pi(x) = (x \text{ 以下の素数の個数})$$

とおきます. “素数が無数にある” と言うのは, “x をどんどん大きくすると $\pi(x)$ もいくらでも大きくなる” と言うことです. 素数をみつけていくには, エラトステネス (Eratosthenes) のふるいという方法が簡単です. この方法で 100 以下の素数を求めると, 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 の 25 個です.

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

エラトステネスのふるい

素数の個数 $\pi(x)$ の値について, 現在知られているデータを表にします.

x	$\pi(x)$	$(\pi(x)/x)$	x	$\pi(x)$	$(\pi(x)/x)$
10^1	4	(40%)	10^{14}	3 204 941 750 802	(3.2%)
10^2	25	(25%)	10^{15}	29 844 570 422 269	(3.0%)
10^3	168	(17%)	10^{16}	279 238 341 033 925	(2.8%)
10^4	1 229	(12%)	10^{17}	2 623 557 157 654 233	(2.6%)
10^5	9 592	(9.6%)	10^{18}	24 739 954 287 740 860	(2.5%)
10^6	78 498	(7.8%)	10^{19}	234 057 667 276 344 607	(2.3%)
10^7	664 579	(6.6%)	10^{20}	2 220 819 602 560 918 840	(2.2%)
10^8	5 761 455	(5.8%)	10^{21}	21 127 269 486 018 731 928	(2.1%)
10^9	50 847 534	(5.1%)	10^{22}	201 467 286 689 315 906 290	(2.0%)
10^{10}	455 052 511	(4.6%)	10^{23}	1 925 320 391 606 803 968 923	(1.9%)
10^{11}	4 118 054 813	(4.1%)	10^{24} *	18 435 599 767 349 200 867 866	(1.8%)
10^{12}	37 607 912 018	(3.8%)	10^{25}	176 846 309 399 143 769 411 680	(1.7%)
10^{13}	346 065 536 839	(3.5%)			

最先端の研究者達がプロジェクトを組んでやっと求めたのがこの表です. 10^9 の欄をみると約 5 % が素数です. 適当に 9 桁の数を思い浮かべるとそのうち 20 個に 1 個の割合で素数になります. 素数でないとすぐにわかる偶数や 3 の倍数, 5 の倍数を除くと素数に出会う確率はもっと高くなります. 10^{22} の欄をみると約 2 %, つまり 50 個に 1 個の割合で素数になります. 10^{25} の欄をみると約 1.7 % が素数です. どのように感じますか. 思ったより多い? 少ない? 素数って結構沢山あると思いませんか.

素数の割合 $\pi(x)/x$ はどの位の大きさなのでしょうか. x をどんどん大きくすると, $\pi(x)/x$ はだんだん少なくなります. ガウス (1790's) やルジャンドル (Legendre, 1798) が予想し, アダマール (Hadamard) とド・ラ・ヴァレ・プーサン (de la Vallée-Poussin) が 1896 年に独立に証明しました.

素数定理 $\pi(x)/(x/\log(x))$ は x をどんどん大きくすると限りなく 1 に近づく.

上の表で星印のある $\pi(10^{24})$ の値は, リーマン予想を仮定して得られました. リーマン予想とは, 1859 年にリーマン (Riemann) が素数の割合を調べる過程で仮定した, とても強力な予想です. 多くの研究者はリーマン予想は成り立つだろうと考えているので, $\pi(10^{24})$ の値は正しいと思われます. もし誤りだったなら, リーマン予想が成立しないという驚くべき結果を導きます.

リーマン予想をもとにすると, 素数定理よりも遙かに詳しく $\pi(x)$ の振る舞いがわかります. 素数定理自体にはリーマン予想ほど強力な予想を仮定しなくてもよいのです. リーマンの着想がもとになり, 解析学の進展によりリーマン予想を経ずに素数定理が証明されました.

数学に限らず学問の進展は連続的ではありません. 今回は素数の無限性を題材に, ユークリッド, フェルマー, オイラー, ガウス, リーマンと言った超一流の数学者たちが時代を切り開き, 一つ上の高みに数学が進展していく様を垣間見ました.