素 数 の は な し

小川 裕之 (大阪大学大学院 理学研究科)

x1. 素数は無数にあります

自然数 a が自然数 m で割り切れるとき, a は m の **倍数**, m は a の **約数** といいます. 1 より大きい自然数で, 1 と自分自身以外の約数を持たないものを **素数** といいます. 約数の中で素数であるものを **素因数** といい, 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. m が自然数 a, b の両方の約数であるとき, m 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. a と b の最大公約数が 1 であるとき a と b は **互いに素** といいます. $12 = 2£2£3$ や $15 = 3£5$ 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. すべての自然数は, ただ一通りの仕方で素因数分解されます. **(整数論の基本定理)** 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なのです.

さて, 素数はいく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 種類の証明法を紹介します.

x2. 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 $p_1, p_2, ¢¢¢, p_n$ から, それらと異なる素数を作り出すことができれば, いくらでも好きなだけ新しい素数をみつけることができます. つまり, 素数が無数にあることが証明されるのです.

2.1. ユークリッド (Euclid) の証明

$N = p_1£p_2£¢¢¢£p_n + 1$ は $p_1, p_2, ¢¢¢, p_n$ では割り切れないので, N の素因数 p は $p_1, p_2, ¢¢¢, p_n$ とは異なる素数です.

2.2. クンマー (Kummer) の証明 (1878 年)

$N = p_1£p_2£¢¢¢£p_n ¡ 1$ は $p_1, p_2, ¢¢¢, p_n$ では割り切れないので, N の素因数 p は $p_1, p_2, ¢¢¢, p_n$ とは異なる素数です.

2.3. スティルチェス (Stieltjes) の証明 (1890 年)

$p_1£p_2£¢¢¢£p_n = L£M$ と 2 数の積に分ける. $N = L + M$ は $p_1, p_2, ¢¢¢, p_n$ では割り切れません.

2.4. メトロ (M¶trod) の証明 (1917 年)

$M = p_1£p_2£¢¢¢£p_n$ とする. $N = M=p_1 + ¢¢¢ + M=p_n$ は $p_1, p_2, ¢¢¢, p_n$ では割り切れません.

x3. 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法をたどることで, 新しい素数を次々と作り出していくことができます. 実際にユークリッドの証明 (2.1) をたどって, 順々に新しい素数をみつけてみましょう. まずは $p_1 = 2$ からはじめます.

1. $p_1 = 2$
2. $p_1 + 1 = 2 + 1 = 3$ は素数なので $p_2 = 3$
3. $p_1£p_2 + 1 = 2£3 + 1 = 7$ も素数 $p_3 = 7$
4. $p_1£p_2£p_3 + 1 = 2£3£7 + 1 = 43$ も素数 $p_4 = 43$

§ $p_1£p_2£p_3£p_4 + 1 = 2£3£7£43 + 1 = 1807 = 13£139$ 小さい方の素数をとって $p_5 = 13$

¶ $p_1£p_2£p_3£p_4£p_5 + 1 = 23479 = 53£443$ 小さい方の素数をとって $p_6 = 53$

· $p_1£p_2£p_3£p_4£p_5£p_6 + 1 = 1244335$ 素因数分解は面倒そう. でも ¢¢¢ $p_7 = 5$

¸ $p_1£p_2£p_3£p_4£p_5£p_6£p_7 + 1 = 6221671$ 最小素因数は ¢¢¢ ?

実は 6221671 は素数でなので 8 つ目に来る素数は $p_8 = 6221671$ です. 次の 9 つ目に来る素数はいくつでしょうか ? 答えは 14 桁の素数 38709183810571 です. 更にこの次, 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 ?

何となくもれがありそうですが, まだ証明されていません. 最小でなく, 最大素因数を選ぶようにアレンジした場合には, 現れない素数があるのですが, そのような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)

実際に電卓などで計算してみるとわかる (困ってしまう) のですが, 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 ?

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 $F_m = 2^{2^m} + 1$ $(m \geqq 0)$

$F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ は素数です. フェルマーは F_m がすべて素数であろうと予想しました. オイラー (Euler, 1732) は F_5 が 641 で割り切れることを見出し, その後, 多くの研究で素数にならないフェルマー数が沢山みつかっていますが, 上の 5 つ以外に素数であるものはみつかっていません.

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. $M_{11} = 2047 = 23£89$ は素数ではありませんが, M_{13}, M_{17}, M_{19} は素数 (メルセンヌ素数) です. メルセンヌ素数が無数にあるかどうかわかっていません. 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 44 個のメルセンヌ素数がみつかっています. 35 番目からの 10 個は, 1996 年に始まった GIMPS (`http://www.mersenne.org/prime.htm`) というプロジェクトの成果です. 今年の 9 月 6 日にみつかったメルセンヌ素数 $M_{32582657}$ は 980 万 8358 桁の自然数で, 現在知られている最も大きな素数です.

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/`) をご覧ください.

x4. フルビッツ (Hurwitz) の問題

前節でふれたフェルマー数 F_m は次の関係式を満たします.

$$F_m - 2 = F_0£F_1£¢¢¢£F_{m-1}$$

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 年) $m > n$ とすると, 上の関係式より F_m を F_n で割ったあまりは 2 です. フェルマー数は奇数なので, F_m と F_n は互いに素です. p_0 を F_0 の素因数, p_1 を F_1 の素因数, p_2 を F_2 の素因数とし以下同様に, F_m の素因数 p_m をひとつずつ選ぶと, それらはすべて異なる素数です. 無数に多くの素数をみつけることができました.

どの 2 つのフェルマー数をとっても互いに素であることが, この証明の本質的な部分です. フルビッツは次のように問題を設定しました.

4.2. **フルビッツ** (Hurwitz) **の問題** (1891 **年**)

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.

この問題の自然数の系列 $A_1, A_2, \cdots$ のそれぞれから素因数をひとつずつ選べば, それらはすべて異なるので, 素数が無数にあることがわかります.

4.3. **エドワーズ** (Edwards) **の証明** (1964 **年**)

a, B_0 を互いに素な自然数とし, 自然数 $n \geqq 1$ に対して $B_n = B_{n-1}(B_{n-1} - a) + a$ とおきます. $m \neq n$ に対して B_m と B_n は互いに素になり, フルビッツの要求する自然数の系列になります. $a = 2, B_0 = 3$ とすると B_n はフェルマー数 F_n です. C_0 を奇数, $C_n = C_{n-1}^2 - 2$ $(n \geqq 1)$ 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, フルビッツの要求する自然数の系列になっています.

4.4. **ベルマン** (Bellman) **の定理** (1947 **年**)

$f(x)$ 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) 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 つをとっても互いに素になる.

$f(x) = (x-1)^2+1$ 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, $f(k) = 2^2+1 = F_1$, $f(f(k)) = (2^2)^2 + 1 = 2^{2^2} + 1 = F_2$, $f(f(f(k))) = (2^{2^2})^2 + 1 = 2^{2^3} + 1 = F_3, \cdots$ フェルマー数が現われます. ベルマンの定理を使っても 2 つのフェルマー数が互いに素であることがわかります. こうしてゴールドバッハの証明が, フルビッツの問題をベルマンの定理で解くことに帰着されました.

問題 $f(x)$ をどのようにとれば, ベルマンの定理の系列に, エドワーズの自然数の系列 $B_0, B_1, B_2, \cdots$ が現われるでしょうか？ $C_0, C_1, C_2, \cdots$ はどうでしょうか？

問題 $f(x) = x(x-1) + 1$ を使って素数が無数にあることを示してください.

x5. **オイラー** (Euler) **の証明**

5.1. **オイラー** (Euler) **の証明**

素数の逆数の和 $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \cdots$ を考える. 素数が有限個しかないならこの和は計算でき, 有限の値に定まるはずなのですが, 実際に足し算を続けていくと値が幾らでも大きくなる. この和は有限の値に定まらない (収束しない) ことが証明され, 素数は有限個ではない.

素数の逆数の和を考えるというオイラーの証明は, 素数を次々にみつけていくユークリッドの証明に比べ, 不自然に思えます. 素数の世界を知るのに解析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.

4.2. **ディリクレの算術級数定理** (1837 **年**)

$d \geqq 2$, a を互いに素な自然数とする. 初項 a 公差 d の等差数列

$a, a + d, a + 2d, a + 3d, \cdots$ の中には素数が無数に現われる.

初項 a 公差 d の等差数列の一般項は $a + d(n-1)$ ですから n の一次式です. ディリクレの定理は, 『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 二次式で与えられる数の列の場合はどうなのでしょうか？

二次式が因数分解されると素数は全然出てこなくなるので, 上の問題は既約な二次式で考えるべきです. 実は, $x^2 + 1$ のような簡単な二次式の場合でさえ, 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

ないのです. 難しい解析を使いこなせるだけの知識が必要ですが, 二次以上の次数の多項式で表される数の系列に含まれる素数の逆数の和は有限の値に定まる (収束してしまう) ので, オイラーの方法が使えないのです. オイラーの方法の使えない自然数の系列に素数が無数に含まれるかどうか, 現在の数学では判定できないのです.

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, ¢¢¢ 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. ところが 1919 年にブラン (Brun) は, 双子素数の逆数の和 $(\frac{1}{3}+\frac{1}{5})+(\frac{1}{5}+\frac{1}{7})+(\frac{1}{11}+\frac{1}{13})+$¢¢¢ が有限の値に定まる (収束する) ことを証明しました. この和はブランの定数と呼ばれ, 近似値は 1:902160577783278¢¢¢ (Nicely, Kutrib-Richstein, 1995) です. これもやはりオイラーの方法が使えず, 双子素数が無数にあるのかどうかわかっていないのです.

x6. 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 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

現在知られているデータを表にします.

x	$\pi(x)$	$(\pi(x)=x)$
10^{1}	4	(40%)
10^{2}	25	(25%)
10^{3}	168	(17%)
10^{4}	1 229	(12%)
10^{5}	9 592	(10%)
10^{6}	78 498	(7.8%)
10^{7}	664 579	(6.6%)
10^{8}	5 761 455	(5.8%)
10^{9}	50 847 534	(5.1%)
10^{10}	455 052 511	(4.6%)
10^{11}	4 118 054 813	(4.1%)

x	$\pi(x)$	$(\pi(x)=x)$
10^{12}	37 607 912 018	(3.8%)
10^{13}	346 065 536 839	(3.5%)
10^{14}	3 204 941 750 802	(3.2%)
10^{15}	29 844 570 422 269	(3.0%)
10^{16}	279 238 341 033 925	(2.8%)
10^{17}	2 623 557 157 654 233	(2.6%)
10^{18}	24 739 954 287 740 860	(2.5%)
10^{19}	234 057 667 276 344 607	(2.3%)
10^{20}	2 220 819 602 560 918 840	(2.2%)
10^{21}	21 127 269 486 018 731 928	(2.1%)
10^{22}	201 467 286 689 315 906 290	(2.0%)

この表を見てどう感じますか ? 思ったより多い ? 思ったより少ない ? 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. 次の桁 10^{23} も計算しようとしていたのですが, 少しプログラムミスがあって計算できなかったそうです.

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 個の割合で素数を見つけることができるのです. 10^{22} の欄をみると約 2 % が素数です. 適当に 22 桁の数を思い浮かべると 50 個に 1 個の割合で素数になります. 素数って結構沢山あると思いませんか.

でも素数の割合はだんだん少なくなっているようです.

問題 素数の割合 $(\pi(x)=x)$ はどの位なのでしょうか ?
x をどんどん大きくすると, どんどん小さくなるのですが ¢¢¢