素数のはなし — 実験数学入門 —

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 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. m が 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. 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. 2 や 3 は素数です. 4 は 2 を約数にもつので素数ではありません. $12 = 2\times2\times3$ や $15 = 3\times5$ のように, 自然数を素数の積に表すことを **素因数分解** といます. 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**) 素因数分解に現れる素数のことを **素因数** といい, 最も小さい素因数を **最小素因数** といいます.

世の中にはどのくらい沢山の素数があるのでしょうか ?

[**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す. 今では数えきれないくらい沢山の種類の証明があります. といっても無数に多くではありませんが $\cdots$ 主なものを 3 種類紹介します.

§2. ユークリッド (Euclid) の証明

最初に紹介するのは, n 個の素数 $p_1, p_2, \cdots, p_n$ から, 新しい素数をみつける方法です. これを繰り返せば, いくらでも好きなだけ素数をみつけることができます.

2.1. ユークリッド (Euclid) の証明

$N = p_1\times p_2\times\cdots\times p_n + 1$ とおくと, N は $p_1, p_2, \cdots, p_n$ では割り切れません. N の素因数 p は $p_1, p_2, \cdots, p_n$ とは異なる新しい素数です.

2.2. クンマー (Kummer) の証明 (1878 年)

$N = p_1\times p_2\times\cdots\times p_n - 1$ とおくと, N は $p_1, p_2, \cdots, p_n$ では割り切れません. N の素因数 p は $p_1, p_2, \cdots, p_n$ とは異なる新しい素数です.

2.3. スティルチェス (Stieltjes) の証明 (1890 年)

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

2.4. メトロ (Métrod) の証明 (1917 年)

$M = p_1\times p_2\times\cdots\times p_n$ とする. $N = M/p_1 + \cdots + M/p_n$ は $p_1, p_2, \cdots, p_n$ では割り切れません.

ユークリッドの証明をたどって, 素数を無数にみつけてみましょう. $p_1 = 2$ からはじめてみましょう.

① $p_1 = 2$
② $p_1 + 1 = 2 + 1 = 3$ は素数なので $p_2 = 3$
③ $p_1 \times p_2 + 1 = 2 \times 3 + 1 = 7$ も素数. $p_3 = 7$
④ $p_1 \times p_2 \times p_3 + 1 = 2 \times 3 \times 7 + 1 = 43$ も素数. $p_4 = 43$
⑤ $p_1 \times p_2 \times p_3 \times p_4 + 1 = 2 \times 3 \times 7 \times 43 + 1 = 1807$ の素因数分解は 13×139 最小素因数をとって $p_5 = 13$
⑥ $p_1 \times p_2 \times p_3 \times p_4 \times p_5 + 1 = 2 \times 3 \times 7 \times 43 \times 13 + 1 = 23479$ の素因数分解は 53×443 最小素因数をとって $p_6 = 53$
⑦ $p_1 \times p_2 \times p_3 \times p_4 \times p_5 \times p_6 + 1 = 2 \times 3 \times 7 \times 43 \times 13 \times 53 + 1 = 1244335$　素因数分解は面倒そう. でも 5 で割りきれるので最小素因数は　$p_7 = 5$
⑧ $p_1 \times p_2 \times p_3 \times p_4 \times p_5 \times p_6 \times p_7 + 1 = \cdots = 6221671$　最小素因数は $\cdots$?

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. この次の 10 個目は $\cdots$ ちょっと計算する気が起こりません. 素数を 9 つ掛けるのも面倒ですが, もっと面倒な素因数分解を計算しないと先に進めません.

[**問題**] 素因数分解しなくてもいいような, 素数ばかりが出てくる系列をつくれないだろうか ?

[**問題**] 素数が無数に現われる系列をつくれないだろうか ?

フェルマーはフェルマー数という系列を考えました.

フェルマー数　　$F_m = 2^{2^m} + 1 \quad (m \geqq 0)$

$F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ は素数です. 残念ながら $m \geqq 5$ で素数であるものはみつかっていません. $F_5, \cdots, F_{11}$ は完全に素因数分解されています. $F_{12}, \cdots, F_{22}$ は素数でないことはわかっているのですが, それぞれ部分的にしか素因数分解されていません. 特に F_{14}, F_{20}, F_{22} は素因数がひとつも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　　$M_q = 2^q - 1 \quad (q$ は素数$)$

38 個の素数のメルセンヌ数 (メルセンヌ素数といいます) がみつかっています. 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. 現在知られている最も大きな素数の記録は, メルセンヌ素数 $M_{6972593}$ で 209 万 8960 桁の自然数です. M_q が素数なら $P_q = 2^{q-1}(2^q - 1)$ は完全数なのですが, $P_{6972593}$ は 419 万 7919 桁の自然数です.

素数の記録など素数について興味のあるかたは, インターネットのページ

The Prime Pages　`http://www.utm.edu/research/primes/`

を見てみて下さい. 素数の歴史から懸賞問題まであります.

§3. フルビッツ (Hurwitz) の問題

3.1. ゴールドバッハ (Goldbach) の証明 (1730 年)

$$F_m - 2 = F_0 \times F_1 \times \cdots \times F_n \times \cdots \times F_{m-2} \times F_{m-1} \quad (m > n)$$

なので 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, フェルマー数 F_m から素因数 p_m をひとつずつ選ぶと, $p_0, p_1, p_2, \cdots$ 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.

3.2. 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. 素数が無数にあることがわかる.

3.3. 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,

$$B_n = B_{n-1} \times (B_{n-1} - a) + a \ (n \geqq 1)$$

$m \neq n$ 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る. $a = 2, B_0 = 3$ とすると B_n はフェルマー数 F_n です.

C_0 を奇数, $C_n = C_{n-1}^2 - 2 \ (n \geqq 1)$ とおく. $m \neq n$ に対して C_m と C_n は互いに素です. これもフルビッツの要求する自然数の系列になっています.

3.4. 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) $f(f(0)) = f(0)$

k を $f(0)$ と互いに素にとるとき, $k, f(k), f(f(k)), f(f(f(k))), \cdots$ のどの 2 つをとっても互いに素である.

$f(x) = (x-1)^2 + 1$ 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. ベルマンの定理より 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 $B_0, B_1, B_2, \cdots$ が現われますか ? $C_0, C_1, C_2, \cdots$ についてはどうですか ?

[**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.

§4. オイラー (Euler) の証明

4.1. オイラー (Euler) の証明

素数の逆数の和 $\displaystyle\sum_{p:\text{素数}} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \cdots$ を考える. 素数が有限個しかないならこの和は計算できる有限の値のはずなのですが, 実際に足し算を続けていくと値が幾らでも大きくなる. つまりこの和は収束しないので, 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, これまでに紹介した素数を並べていく直接的な証明に比べ, 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, $a+d$, $a+2\,d$, $a+3\,d$, $\cdots$ の中には素数が無数に現われる.

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. ところが 1919 年にブラン (Brun) は, 双子素数の逆数の和 $(\frac{1}{3}+\frac{1}{5})+(\frac{1}{5}+\frac{1}{7})+(\frac{1}{11}+\frac{1}{13})+\cdots$ が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 $1.902160577783278\cdots$ (Nicely, Kutrib-Richstein (1995)) です. 収束してしまったのでオイラーの方法は使えません. それでも, 双子素数が有限個であるのかどうかわかっていないのです.

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ことを言っています. (§2. の 2 つめの [問題] を思い出してみてください.)

[**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 ?

いちばん簡単な二次式 x^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. 難しい解析を使いこなせるだけの知識が必要ですが, 一次式以外の系列に含まれる素数の逆数の和は収束してしまうので, オイラーの方法が使えません. 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, 現在の整数論では判定できないのです.

x^2+y^2 のように, どの項も次数が 2 の x と y の多項式を二次形式といいます.

[**問題**] 二次形式で表される整数の中にどのくらい素数が現れるのでしょうか.

次の章で二次形式 x^2+y^2 について調べましょう. x^2+1 と表させる整数の素因数分解との関係を調べてみましょう.

§5. 二次式型素数と二次形式型素数

二次式 x^2+1 に対して, x^2+1 と表される素数について調べましょう. $x=1, 2, 3, 4, \cdots$ と代入して x^2+1 の値とその素因数分解を計算すると,

x	x^2+1	x	x^2+1	x	x^2+1	x	x^2+1
1	2	6	37	11	$122=2\times61$	16	257
2	5	7	$50=2\times5^2$	12	$145=5\times29$	17	$290=2\times5\times29$
3	$10=2\times5$	8	$65=5\times13$	13	$170=2\times5\times17$	18	$325=5^2\times13$
4	17	9	$82=2\times41$	14	197	19	$362=2\times181$
5	$26=2\times13$	10	101	15	$226=2\times113$	20	401

素数が 8 つ現われました.

2, 5, 17, 37, 101, 197, 257, 401

素因数分解も含めて上の表に出てきたすべての素数を小さい順に並べると

2, 5, 13, 17, 29, 37, 41, 61, 101, 113, 181, 197, 257, 401

二次形式 x^2+y^2 に対して, x^2+y^2 と表される素数について調べてみましょう.

$y\backslash x$	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	1	4	9	16	25	36	49	64	81	100	121	144
1	1	*2	*5	10	*17	26	*37	50	65	82	*101	122	145
2	4	*5	8	*13	20	*29	40	*53	68	85	104	125	148
3	9	10	*13	18	25	34	45	58	*73	90	*109	130	153
4	16	*17	20	25	32	*41	52	65	80	*97	116	*137	160
5	25	26	*29	34	*41	50	*61	74	*89	106	125	142	*167

出てきた素数を順に並べると, (* のついているもの)

2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 137, 167

出てきた整数を順に並べると,

0, 1, 2, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, 34, 36, 37, 40, 41, 45, 49,