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 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. 主なものを 3 種類紹介しましょう.

§2. ユークリッド (Euclid, Eukleides) の証明

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 (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. $p_1 = 2$ 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 $p_1 \times p_2 + 1 = 2 \times 3 + 1 = 7$ 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 小さい方の素数をとって　$p_5 = 13$
⑥ $p_1 \times p_2 \times p_3 \times p_4 \times p_5 + 1 = 2 \times 3 \times 7 \times 43 \times 13 + 1 = 23479$ の素因数分解は 53×443 小さい方の素数をとって　$p_6 = 53$
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. 次の 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 ?

実際に電卓などで計算してみるとわかるのですが, 素数を沢山掛けるのも大変ですが, その数を素因数分解するのはもっと大変です.

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

$F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ 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. F_{14}, F_{20}, F_{22} は素数でないことはわかっているのに, 素因数がひとつもみつかっていないのです. F_5 の素因数分解を最初に計算したのは, オイラー (Euler) です. ガウス (Gauss) は, F_m が素数なら正 F_m 角形が定規とコンパスで作図可能であることを証明しました.

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$)$

41 個の素数のメルセンヌ数 (検証中の 2 個を含む) 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 $M_{13466917}$ で 405 万 3946 桁の自然数です. 検証中のも

のでは $M_{24036583}$ で 723 万 5733 桁の自然数です. メルセンヌ数 M_q が素数なら $P_q = 2^{q-1}(2^q - 1)$ は完全数なのですが, $P_{13466917}$ は 810 万 7892 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. 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その個数を数えてみましょう.

$$\pi(x) = (x \text{ 以下の素数の個数}) \qquad (x \text{ は自然数})$$

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.

x	$\pi(x)$		x	$\pi(x)$	
10^1	4	(40%)	10^{10}	455 052 511	(4.6%)
10^2	25	(25%)	10^{11}	4 118 054 813	(4.1%)
10^3	168	(17%)	10^{12}	37 607 912 018	(3.8%)
10^4	1 229	(12%)	10^{13}	346 065 536 839	(3.5%)
10^5	9 592	(10%)	10^{14}	3 204 941 750 802	(3.2%)
10^6	78 498	(7.8%)	10^{15}	29 844 570 422 269	(3.0%)
10^7	664 579	(6.6%)	10^{16}	279 238 341 033 925	(2.8%)
10^8	5 761 455	(5.8%)	10^{17}	2 623 557 157 654 233	(2.6%)
10^9	50 847 534	(5.1%)	10^{18}	24 739 954 287 740 860	(2.5%)

10^9 の欄をみると約 5 % が素数です. 適当に 8 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. 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, 結局は 0 になるのでしょうか ?

§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, 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
> $a,\ a+d,\ a+2\,d,\ a+3\,d,\ \cdots$ 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ことを言っています.

[**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ちゃう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. でも実は, 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, 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.

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.

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. 素数をみつける問題を二次形式で考えてみましょう.

[**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 の x, y に整数を代入したときの値を計算してみましょう. 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,