高校生のための現代数学講座　　東京大学
「素数と暗号」　　玉原国際セミナーハウス
講義 (1)　坪井　俊　　2017 年 7 月 15 日

「素数とふるい」

自然数. 人類の祖先が数えるということを始めて以来、自然数は親から子へと教えられてきたものです。

$$\{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ \ldots\}$$

というものです。

人類と自然数のかかわりの中では、歴史で学ぶべきことも多くあります。例えば、数の記法（位取り、60 進数、10 進数、2 進数）、（辺の長さが 3, 4, 5 などの）直角三角形の発見、零の発見（自然数といえないかもしれません、整数の発見）、実数の発見（有理数、無理数の発見）、（19 世紀の終わりころになっての）自然数の定義、などなどです。

ユークリッドの「原論」という書物が、紀元前 3 世紀に編纂されたと言われており、その内容は、アラビア語、ラテン語に翻訳されたものが、現代に伝えられています。その中には、自然数についても沢山のことが整理されています。ユークリッドの「原論」は 13 巻からなるものとされています。幾何を扱っていますが、7, 8, 9, 10 巻では、自然数についての議論が展開されています。「山口大学　ユークリッド原論」で検索すると、渡邉正先生が渡邉研究室のウェブページに公開されている日本語訳を見ることができます。

倍数と約数. 自然数の足し算は、数えることの延長上にあります。5 を数えて、それから、３つ数えると、6, 7, 8 となり、$5 + 3 = 8$ ということになります。

2 から 2 つずつ数えていくと、2, 4, 6, 8, 10, 12, 14, 16, 18, 20, ... のようになり、5 から 5 つずつ数えていくと、5, 10, 15, 20, 25, 30, ... のようになります。これらは 2 の倍数、5 の倍数と呼ばれます。2 の倍数同士の和は 2 の倍数となり、5 の倍数同士の和は 5 の倍数となります。私たちは、十進法を使っているので、2 の倍数、5 の倍数は、1 位の桁を見るとわかります。

私たちは、一般の自然数を m, n のように表すことを知っています。

自然数 m を何度も足し合わせると、自然数 m の**倍数**が得られます。足し合わせた回数を n とするとき、その自然数 N は $N = m \times n = mn$ または $N = n \times m = nm$ と書かれます。掛け算の答は**順序によりません**から、どちらで書いてもよいです。自然

数 N が自然数 m の倍数であれば、$m \leqq N$ となります。m の倍数の和は m の倍数となります。

自然数 N が自然数 m の倍数であるときに、$N = mn$ となる自然数 n がありますから、N を m で割ると自然数 n となります。このとき自然数 m を自然数 N の**約数**と言います。$N = mn$ ならば自然数 n も自然数 N の約数です。自然数 m が自然数 N の約数であれば、当然 $m \leqq N$ となります。

異なる 2 つの自然数 a, b $(b < a)$ に対しては、a が b の倍数、あるいは同じことですが、b が a の約数となるとは限りません。そのときは、

$$a = qb + r$$

となる自然数 q で最大のものを探します。$b < 2b < 3b < \cdots$ と増加し、やがて a よりも大きくなりますから、このような q は存在すると考えられます（アルキメデスの公理と呼ばれます）。最大の q に対しては、$0 \leqq r < b$ となっていて、このような q はただ 1 つです。従って r もただ 1 つ定まります。a を b で割ったときの**商**は q、**余り**は r であると言います。余りが 0 のときに、a は b で**割り切れる**と言いますが、このとき、a は b の倍数であり、b は a の約数です。

どんな自然数 n も 1 と n を約数に持ちますから、約数を持たないということは起きません。1 と異なる自然数 n の約数が 1 と n だけのとき、n を**素数**と呼び、n の約数が 1 と n 以外にもあるとき、n を**合成数**と呼びます。

素因数分解. 715 の約数は、1, 5, 11, 13, 55, 65, 143, 715 の 8 個です。

$$715 = 5 \times 11 \times 13$$

と素数の積に書き表し、その素数を使うか使わないかという $2 \times 2 \times 2$ 通りを数えたものです。どのような自然数 N も素数の累乗の積として（素数を小さいものから並べれば）**一意的に**書かれます。

$$N = {p_1}^{a_1} {p_2}^{a_2} \cdots {p_k}^{a_k}$$

ここで、$a_1, a_2, \ldots, a_k$ は自然数、$p_1, p_2, \ldots, p_k$ は素数で、$p_1 < p_2 < \cdots < p_k$ を満たすものです。このことを**素因数分解の一意性**と呼びます。証明が必要な事柄です。時間のある人はどうすれば証明できるか考えてみてください。$N = {p_1}^{a_1} {p_2}^{a_2} \cdots {p_k}^{a_k}$ ならば、N の約数は $(a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$ 個あります。

エラトステネスのふるい. 素数は、合成数ではない自然数だから、自然数の表があれば、その中から、2 以外の 2 の倍数、3 以外の 3 の倍数、5 以外の 5 の倍数、7 以外の 7 の倍数、…と順に合成数を取り除けば、残った自然数は、素数であることにな

ります。これはエラトステネスのふるいと呼ばれます。合成数 N の約数には、1 以外に $\sqrt{N}$ 以下のものがあるので、表の自然数の平方根までの素数の倍数を取り除けばよいことになります。

【演習】　次の表の中の素数だけを残せ。

	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	100
101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170	172	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200
201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220
221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240
241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260
261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280
281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300

素数の個数. 素数は上に見るように、1〜60 に 17 個、61〜120 に 13 個、121〜180 に 11 個、181〜240 に 11 個、241〜300 に 10 個、というように分布しています。素数の割合は、大きな自然数の周辺では、約数の候補が増えるので少なくなっていると考えられます。

実際、100 個連続して素数がないこともかならず起ります。（上の表の中では 13 個合成数が連続しているところがあります。）例えば、$100! = 1\times2\times\cdots99\times100$（!は階乗と読む) という自然数を考えれば、$100!+2$ から $100!+100$ の間の自然数、$100!+k$ は、k を約数に持つ合成数です（これは 99 個連続でした)。ただし、$100!$ は、十進法で 157 桁の数です。そういうところで 100 個くらい合成数が並んでいても驚くことではないかもしれません。157 桁の数はかなり大きな数です。アボガドロ数は 23 桁の数で、宇宙にある原子の個数は 80 桁程度の数と考えられています。

だんだんと素数が現れにくくなると、ついには素数が現れなくなることも考えら

れますが、そんなことはないこと（素数は無限個あること）が、すでにユークリッドの原論に書かれています。

その書きぶりは以下のようです（前述の渡邉研究室の日本語訳を少しアレンジしてあります）。

【ユークリッド原論第９巻命題２０】　素数（の個数）は、任意に決められた素数の個数よりも多い。

【証明】　**A**、**B**、**C** を決められた素数とせよ。**A**、**B**、**C** より多く素数があると主張する。

A、**B**、**C** によって割り切られる最小の数 **D** をとる。**D** に **1** を加え、**F** とする。そのとき、**F** は素数か、そうでないかのどちらかである。

まず、**F** が素数とする。そのとき、素数 **A**、**B**、**C**、**F** が **A**、**B**、**C** より多く見つけられた。

次に、**F** が素数でないとする。そのとき、**F** はある素数によって割り切られる。**F** が素数 **G** によって割り切られるとせよ。**G** は **A**、**B**、**C** のどれとも同じでないと主張する。

（どれかと）同じであるとせよ。**A**、**B**、**C** は **D** を割り切る。それゆえに、**G** もまた **D** を割り切る。しかし、**1** も割り切る。**G** は（**1** より大きな）数であり、**1** を割り切り、これは不合理である。それゆえに、**G** は **A**、**B**、**C** のどれとも同じではない。そして、仮定から **G** は素である。

それゆえに、素数 **A**、**B**、**C**、**G** が決められた **A**、**B**、**C** の個数より多く見つけられた。

それゆえに、素数は、任意に決められた素数の個数よりも多い。

現代の証明の書き方ならば以下のようになります。

素数が有限個（k 個）とし、それらを $p_1, \ldots, p_k$ とする。$f = p_1 \cdots p_k + 1$ とおく。f が素数ならば、k 個よりも多くの素数があることになる。f が合成数ならば f を割り切る素数 g があるが、g が $p_1, \ldots, p_k$ のどれかと一致すれば、g は 1 を割り切る素数となり不合理。g が $p_1, \ldots, p_k$ と異なれば、k 個よりも多くの素数があることになり、仮定に反する。従って素数は無限個存在する。

双子素数. 前のページの表の中の素数の分布をみると、5 と 7、11 と 13、17 と 19、29 と 31、41 と 43、59 と 61、71 と 73、101 と 103、107 と 109、137 と 139、149 と 151、179 と 181、191 と 193、197 と 199、227 と 229、239 と 241、281 と 283 というように、2, 3 以外の素数の中に、隣り合う奇数の素数が、$62 - 2 = 60$ 個中 $16 \times 2 = 32$ 個も現れています。（6 以上の自然数で 6 で割って 2, 3, 4 が余るものは、2 または 3 の倍数だから、双子素数は 6 で割って、5 と 1 が余るものの組となっています。）このような素数の組を**双子素数**と呼びます。双子素数が無限個あるかどうかは、**未解決問題**です。素数の逆数の和が発散することはオイラーが示していますが、双子素数の逆数の和は収束することが知られています。2016 年 9 月に知られている最大の双子素数は $2996863034895 \cdot 2^{1290000} \pm 1$ ということです。

双子ではありませんが、2013 年に Zhang Yitang が 7×10^7 以下の差を持つ素数の

組は無限個あることを示し、その年のうちに 246 以下の差を持つ素数の組が無限個あることが示されています。これは世界の数学研究者の間で話題となりました。新聞等で読まれた方も多いと思います。[Bulletin (N. S.) of the American Mathematical Society Vol.52, No. 2, April 2015, Pages 171–222.]

知られている最も大きな素数. ある自然数が素数であることを示すのは困難です。

素数 p に対し、$2^p - 1$ の形の自然数が素数であるとき、$2^p - 1$ は、メルセンヌ素数と呼ばれます。メルセンヌ素数 $2^p - 1$ に対しては、$2^{p-1}(2^p - 1)$ の自分自身以外の約数は、$1, 2, \ldots, 2^{p-1}, (2^p - 1), 2(2^p - 1), \ldots, 2^{p-2}(2^p - 1)$ で、それらの和は $2^p - 1 + (2^{p-1} - 1)(2^p - 1) = 2^{p-1}(2^p - 1)$ となります。自分自身以外の約数の和が自分自身と一致する自然数は**完全数**と呼ばれ、研究されてきました。コンピュータによる大きな素数の探索もメルセンヌ素数を対象にしているものが多くあります。2017 年 7 月 7 日現在の知られている最も大きな素数は、2016 年 1 月に得られた $2^{74,207,281} - 1$ で、22, 338, 618 桁の自然数です。[The List of Largest Known Primes Home Page (https://primes.utm.edu/primes/home.php) Last modified: 07:20:25 AM Saturday May 20 2017 UTC: New record prime: $2^{74,207,281} - 1$ with 22, 338, 618 digits by Cooper, Woltman, Kurowski, Blosser & GIMPS (7 Jan 2016).]

素数にまつわる未解決問題. 素数にまつわる未解決問題は、上にあげた双子素数の問題を含め、簡単に述べられるものがたくさんあります。上の Home Page にいくつか書かれています。ゴールドバッハの予想は、「6 以上の偶数は 2 つの素数の和になる」というものですが、未解決です。

公約数と公倍数. 自然数 a, b に対し、a, b の両方の約数になっている自然数を a, b の**公約数**と言います。1 は常に公約数ですから公約数がないということは起きません。a, b の公約数が 1 しかないとき、a, b は**互いに素**であると言います。公約数のなかで最大のものを、**最大公約数** (greatest common divisor) といい、$\mathrm{GCD}(a, b)$ と書きます。

自然数 a, b に対し、a, b の両方の倍数になっている自然数を a, b の**公倍数**と言います。ab という公倍数がありますから公倍数がないということは起きません。公倍数のなかで最小のものを、**最小公倍数** (least common multiplier) といい、$\mathrm{LCM}(a, b)$ と書きます。

a, b の素因数分解がわかっていれば、$\mathrm{GCD}(a, b), \mathrm{LCM}(a, b)$ は、素因数分解に現れる各素数についての、a および b の素因数分解に現れる少ないほうの累乗の積、多いほうの累乗の積となります。従って、関係式 $\mathrm{GCD}(a, b)\mathrm{LCM}(a, b) = ab$ が成立します。

実際に、最大公約数を求めるためには、**ユークリッドの互除法**という素晴らしい（計算量の少ない）アルゴリズムがあります。