講義資料 (5): 素数 (1)

5.1 素数

本節は，教科書 3.1 節の中程 (pp.106–113) に対応する．なお，特に断らない限り，本節では正整数のみを取り扱うとする．

定義 5.1 2 以上の正整数 p は，1 と p 自身のほかに正の約数を持たないとき，**素数** (prime number) と呼ばれる．2 以上の素数でない正整数は**合成数** (composite number) と呼ばれる．なお，1 は素数でも合成数でも無いと考える． □

定義 5.2 整数 n が $n = n_1 n_2$ のように表されたとする．このとき，各 n_i の事を n の**因数** (factor) と呼び，特に n_i が素数ならば**素因数** (prime factor) とも呼ぶ． □

補題 5.3 任意の素数 p に対し，$p|a_1 a_2 \cdots a_n$ ならば，ある i が存在して $p|a_i$.

証明 n に関する帰納法で示す．$n = 1$ の場合は明らか．$n > 1$ とする．(p, a_1) は p の正の約数でもあるので $(p, a_1) = 1$ または $(p, a_1) = p$．$(p, a_1) = p$ のときは題意成立．$(p, a_1) = 1$ のときは，補題 4.11 より $p|a_2 \cdots a_n$．よって，帰納法の仮定より，ある i (≥ 2) が存在して $p|a_i$. □

定理 5.4 ((初等) 整数論の基本定理) 2 以上の正整数 n は，いくつかの素数 $p_1, \ldots, p_k$ の積として

$$n = p_1 p_2 \cdots p_k$$

の形に表すことができる．さらに，その表し方は $p_1 \leq p_2 \leq \cdots \leq p_k$ のように小さい順に並べることにすれば只 1 通りである．

証明

(表現可能性) 任意の 2 以上の整数 n に対して，ある素数 $p_1, \ldots, p_k$ が存在して $n = p_1 p_2 \cdots p_k$ となることを，n に関する帰納法で証明する．

Basis　$n = 2$ とする．$p_1 = 2$ とすると $n = p_1$.

I.S.　$n > 2$ とする．n が素数のときは $p_1 = n$ とすれば良い．n が合成数の場合を考える．仮定より，1 でも n でもない正整数 n_1, n_2 が存在して $n = n_1 n_2$．ここで，$2 \leq n_i < n$ $(i = 1, 2)$ であるので各 i に帰納法の仮定が適用できて，ある素数 p'_i $(i = 1, \ldots, k_1)$ と p''_j $(j = 1, \ldots, k_2)$ が存在して $n_1 = p'_1 p'_2 \ldots p'_{k_1}$ かつ $n_2 = p''_1 p''_2 \ldots p''_{k_2}$．よって，$n = p'_1 p'_2 \ldots p'_{k_1} p''_1 p''_2 \ldots p''_{k_2}$.

(表現の一意性) n を 2 以上の任意の整数とし，$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$ かつ $p_1 \leq \cdots \leq p_k$ かつ $q_1 \leq \cdots \leq q_m$ とする．このとき，$k = m$ かつ各 i で $p_i = q_i$ となることを，n に関する帰納法で示す．

Basis $n = 2$ とする．この場合は $k = m = 1$ かつ $p_1 = q_1 = 2$ となり題意が成立．

I.S. $n > 2$ とする．

- $p_1 \neq q_1$ とする．一般性を失う事なく $p_1 < q_1$ とする．補題5.3より，ある i で $p_1|q_i$．ここで，p_1, q_i は共に素数なので $p_1 = q_i$．よって，$p_1 < q_1 \leq q_i = p_1$ となり矛盾．よってこの場合はあり得ない．
- $p_1 = q_1$ とする．このとき，$p_2 \cdots p_k = q_2 \cdots q_m$．帰納法の仮定より $k = m$ かつ各 i (≥ 2) で $p_i = q_i$．よって，題意が成立． □

系 5.5 2以上の正整数 n は，いくつかの素数の巾 $p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}$ の積として

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

の形に表すことができる．さらに，その表し方は各 i で $\alpha_i > 0$ かつ $p_1 < p_2 < \cdots < p_k$ のように小さい順に並べることにすれば只1通りである． □

命題 5.6 正整数 m, n の最小公倍数を l，最大公約数を d とする．

(1) m, n の任意の公約数 k に対し $k|d$

(2) m, n の任意の公倍数 k に対し $l|k$

(3) $mn = dl$

証明 系 5.5 を考えて，$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ かつ $n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ かつ各 i で $\alpha_i + \beta_i > 0$ となる素因数分解が一意に存在する．各 i で $d_i = \min(\alpha_i, \beta_i)$, $l_i = \max(\alpha_i, \beta_i)$ とする．

(1) k は公約数なので $k = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$ となる γ_i $(\leq d_i)$ が存在する．よって，$k|d$.

(2) k は公倍数なので $k = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$ となる γ_i $(\geq l_i)$ が存在する．よって，$l|k$.

(3) 明らかに $d = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$ かつ $k = p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k}$ となる．各 i で $d_i + l_i = \max(\alpha_i, \beta_i) + \min(\alpha_i, \beta_i) = \alpha_i + \beta_i$ なので $mn = dl$. □

NOTE: この定理は容易に一般の整数 m, n を取り扱えるように拡張でき，これが定理 4.13 に一致．一方，本定理の証明は素因数分解の概念を利用する事によって定理 4.13 の証明に比べ非常に見通しが良くなっている．

5.2 エラトステネスの篩

アルゴリズム 5.7 エラトステネスの篩 (Eratosthenes's sieve) とは，以下のように定義される与えられた上限までの素数を全て求めるアルゴリズムである．

(1) 求める素数の上限値を n とする．最初に，2から n までのリストを作成．

(2) リストに残っている印のついていない最小の整数を探す．見つかった整数 k に ◯ 印を付け，k 以外の k の倍数全てに × 印を付ける．

(3) (2) の作業をリストに残っている印のついていない最小の整数が $\sqrt{n}$ より大きくなるまで繰り返し実行.

(4) 最終的に ◯ 印がついた整数と印がついていない整数は全て素数であり, × 印が付いた整数は全て合成数であると判定する. □

例 5.8 30 までの素数をエラトステネスの篩で調べてみよう.

Step 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~~

Step 2

	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~~

Step 3

	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~~

ここで, $7 > \sqrt{30}$ であるので Step 4 は存在しない. よって, 2,3,5,7,11,13,17,19,23,29 が 30 以下の全ての素数の並べ挙げであることが分かる. □

補題 5.9 どんな合成数 n も, ある $\sqrt{n}$ 以下の素数の倍数である.

証明 明らか □

命題 5.10 与えられた正整数 n に対しエラトステネスの篩を実行したとする. このとき, エラトステネスの篩は素数探索法として完全である, すなわち, 素数と判定された整数は素数であり, 合成数と判定された整数は合成数である. さらに, 有限時間で必ず出力を返す.

証明 (概略のみ示す) 各ステップで必ず一つ印が付けられるので, 有限時間で出力を返すことは明らか.
任意の整数 i $(2 \leq i \leq \sqrt{n})$ に対し, ◯ 印がついた i 以下の整数全体が i までの素数全体に一致する事は, i に関する帰納法で示すことができる. よって, $\sqrt{n}$ 以下の整数には ◯ 印か × 印が付けられており, $\sqrt{n}$ より大きい整数には × 印が付けられているか印が付けられてないかである事に注意して, エラトステヌスの篩の健全性を示すことができる. □

NOTE: エラトステネス (Eratosthenes) は紀元前 3 世紀に活躍したアレクサンドリア図書館の館長. 地球の周囲の長さをきわめて正確に測定した事で有名. なお, 彼のアダナは「β(ベータ)」であった. このアダナの由来には二つの説がある. 一つ目は, プラトンに続いて古代で 2 番目に賢い人物という意味であり, 二つ目は, 彼は当時のありとあらゆる学

問に通じており，どの分野でもその 2 番以内であったという説である．どちらにせよ，とんでもない男であったのは間違いない．
ちなみにアレクサンドリア図書館とは，紀元前 290 年頃に建設が始まり蔵書が 70 万巻にも上ったという当時の世界の “知” の中心．紀元前 48 年にカエサルのアレクサンドリア戦争で焼失した…，とされるがこのときは何とか復興できたようです．しかし，テオドシウス 1 世 (統一ローマ帝国を 1 人で支配した最後の皇帝) が異教 (三位一体派からみた異端を含む) の弾圧を大々的に行なったそうでして (古代オリンピックの廃止もこのとき)，391 年の神殿破壊の許可に伴い熱狂的なキリスト教信者達によって破壊し尽くされたそうです．なお，このときも辛うじて命脈を繋げたが，642 年にアラブの将軍アムルによるエジプト遠征で完全に破壊されたという説もあるらしい．

5.3 いろいろな素数

本節は，教科書 3.1 節の中程 (pp.109–110) に対応する．

5.3.1 メルセンヌ素数

定義 5.11 正整数 n を用いて 2^n-1 という形で表される数を**メルセンヌ数** (Mersenne number) と呼ぶ．特に，素数であるメルセンヌ数を**メルセンヌ素数** (Mersenne prime number) と呼ぶ．なお，n 次のメルセンヌ数 2^n-1 を M_n で記す． □

NOTE: 2 進法で記述すると，メルセンヌ数とは 1 だけが並ぶ数になる $(1, 11, 111, 1111, \ldots)$.

NOTE: なお，メルセンヌ素数が無限個存在するかどうかは現在に至ってもいまだ分かっていない．

命題 5.12 メルセンヌ数 M_n が素数になるのは n が素数の場合に限る．

証明 対偶を示す．n を合成数とし $n = ks$ $(1 < k < n)$ とする．このとき，

$$2^n - 1 = (2^k)^s - 1 = (2^k - 1)(2^{k(s-1)} + 2^{k(s-2)} + \cdots + 2^{k\cdot 1} + 2^{k\cdot 0})$$

よって，$2^n - 1$ も合成数になる． □

NOTE: では逆に，n が素数ならば M_n は素数になるであろうか？実際，かっては，n が素数のときはいつでもメルセンヌ数 M_n が素数になると考えられていた．しかしながら，1536 年に M_{11} が合成数であることが発見された $(M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89)$.

命題 5.13 (ルカスの方法) 数列 S_i を $S_0 = 4$ かつ $S_{i+1} = S_i^2 - 2$ で定義する．このとき $n \geq 2$ に対し以下の関係が成立．

$$M_n\text{が素数} \iff M_n \mid S_{n-2}$$ □

この証明は，初等的に証明できるものの，あまりに膨大な量になるために割愛する．

NOTE: ルカス (Lucas) は上記の命題 (厳密にはちょっと違う) を利用して 1876 年に

$$M_{127} = 170141183460469231731687303715884105727$$

すなわち，170 澗 1411 溝 8346 穣 469 僊 2317 垓 3168 京 7303 兆 7158 億 8410 万 5727 が素数であることを発見した．これは計算機が開発され，より大きな素数を発見するまで人類が知る最大の素数の栄誉を担った．なお，現在でもメルセンヌ数は巨大素数の発見に利用されている．
ちなみに現在 (本資料作成) の時点で知られているメルセンヌ素数はたったの 48 個．そのうち最大のメルセンヌ素数は 2013 年の 1 月 25 日に発見された $M_{57885161}$ である (何と 17425170 桁)．ちなみに，このメルセンヌ素数は GIMPS(Great Internet Mersenne Prime Search) と言う巨大メルセンヌ素数の発見だけを目的として立ち上げられたマニアックなプロジェクトによって発見された．

命題 5.14 M_n をメルセンヌ素数とすれば，$\frac{M_n(M_n+1)}{2}$ は完全数である． □

本題からそれまくってきたので，証明は割愛する．

NOTE: ここで，完全数 (perfect number) とは，自分自身と異る約数の総和が元の数に等しくなる数のことである．例えば，6 は完全数である ($6 = 1+2+3$)．なお，この命題はエウクレイデスの『原論』にすでに示されていた．当時 (紀元前 4 世紀) すでに $6, 28, 496, 8128$ が完全数であることが知られていた．なお，この 2000 年後にオイラーによって，偶数の完全数が全てメルセンヌ素数 M_n を用いて $\frac{M_n(M_n+1)}{2}$ と記せることが証明された．一方，奇数の完全数は一つも知られていない ($4k+3$ の形の完全数が無いことは知られている)．

5.3.2 フェルマー素数

定義 5.15 自然数 n を用いて $2^{2^n}+1$ という形で表される数を**フェルマー数** (Fermat number) と呼ぶ．特に，素数であるフェルマー数を**フェルマー素数** (Fermat prime number) と呼ぶ．なお，n 次のフェルマー数 $2^{2^n}+1$ を F_n で記す． □

NOTE: フェルマー数は「フェルマーの大定理」で有名なフェルマーが考えた素数生成列 (と当人は考えていた)．実際，$n = 0, 1, 2, 3, 4$ に対して $F_n = 3, 5, 17, 257, 65537$ は全て素数である．だが残念ながら F_5 は合成数になる ($F_5 = 641 \times 6700417$)．この反例はオイラーが 1732 年に示した．オイラーは，フェルマー数 F_n の因数が $k2^{n+2}+1$ の形になることを利用して F_5 の素因数分解を行った．なお，フェルマー素数は F_0, F_1, F_2, F_3, F_4 の 5 つしか知られていない．さらに言うと，これら以外のフェルマー素数が存在するかどうかもいまだ分かっていない．

命題 5.16 正 n 角形が作図可能であるための必要十分条件は，n が異なるフェルマー素数の積と 2 の巾の積であることである． □

この命題は，講義の最後の方で行う「群論」の概念をマスターし，さらにその先にある数学で最も美しい理論の一つと言われる「ガロア理論」を習得し，さらにガロア理論を自由自在に使いこなして初めて証明できる．というわけで，証明は割愛する．

NOTE: 作図問題とは定規 (与えられた 2 点を通る任意長の線分を描ける) とコンパス (与えられた 2 点の長さを計り，その長さを半径とする円を任意の点を中心に描ける) だけで作図を試みる問題であり，古代ギリシアで非常に活発に研究された．古代ギリシアの三大作図問題として以下のような問題がある．

- 与えられた円と等しい面積をもつ正方形の作図 (円積問題)
- 与えられた立方体の体積の 2 倍に等しい体積をもつ立方体の作図 (立方体倍積問題)
- 与えられた角を三等分する (角の三等分問題)

古代ギリシア時代より，この 3 つの問題は長い間数学者を悩ませてきた．これらの問題は全て作図不能であるのだが，その証明は 19 世紀になりガロア理論の登場を待つ必要があった．

NOTE: ガウスが 19 才のときに正 17 角形の作図法を発見して，喜びのあまり，生涯を数学に捧げようと決心したことは有名．なお私もこの作図法を読んでみたが，あまりに複雑で途中で投げ出してしまった…….

演習課題

問 5.1 素数が無限個存在する事を示せ．