東京大学玉原国際セミナーハウス
2007 年 9 月 15 日－ 17 日

群馬県教育委員会高校教育課
東京大学大学院数理科学研究科

平成１９年度高校生玉原数学セミナー
「素数」

１．９月１５日　１１：００－１２：００　（関口英子）
整数、素数、有理数、実数、複素数、合同式の使い方

２．９月１５日　１３：３０－１４：３０　（寺杣友秀）
ユークリッドの互除法とその応用

３．９月１５日　１５：００－１６：００　（桂　利行）
いろいろな因数分解法

演習９月１５日　１６：３０－１７：３０　（坪井　俊）
ＰＣ（十進ＢＡＳＩＣ）を用いた演習
エラトステネス (Eratosthenes) の篩（ふるい)、素数の分布

４．９月１６日　　９：００－１０：００　（桂　利行）
いろいろな数、代数学の基本定理、n 次代数方程式、
代数的数と超越数、体の概念、２次体とその応用

演習９月１６日　１０：３０－１１：３０　（坪井　俊）
素数の判定、合同式の計算、ユークリッドの互除法、２進展開

５．９月１６日　１５：００－１６：００　（関口英子）
有限体、フェルマーの小定理とその一般化

演習９月１６日　１６：３０－１７：３０　（坪井　俊）
合同式の解き方、フェルマーの小定理、ＲＳＡ暗号

６．９月１７日　　９：００－１０：００　（桂　利行）
暗号理論（ＲＳＡ暗号の話）

７．９月１７日　１０：３０－１１：３０　（寺杣友秀）
素数とリーマンのゼータ関数

1　整数

自然数の集合:

$$\mathbf{N} = \{1,\ 2,\ 3,\ \cdots,\ \}$$

整数の集合：

$$\mathbf{Z} = \{\cdots,\ -2,\ -1,\ 0,\ 1,\ 2,\ \cdots\}$$

整数のことを**有理整数**ということもある.

次の定理は整除性の基本となる.

定理 1.1 a を自然数, b を整数とするとき

$$b = qa + r, \quad 0 \leq r < a$$

となるような整数 q, r がただ一組存在する.

整数 $a,\ b \in \mathbf{Z}$ に対し, ある整数 q が存在して

$$b = aq$$

となるとき, a は b を**割り切る**, あるいは b は a で**割り切れる**, あるいは a は b の**約数**である, あるいは b は a の**倍数**であるという. a が b を**割り切る**ことを $a|b$ と表す. b が a で割り切れない時, $a \not| b$ と書く. a が b を割り切る時, $-a$ も b を割り切るから, 約数といった場合には正の約数を意味するものとする.

整数 $a,\ b$ に対し, a と b の共通の約数を**公約数**という. a と b の公約数のうちで最大のものを, a と b の**最大公約数**といい, $\gcd(a, b)$ と書く. a と b の最大公約数が 1 になるとき, a と b は**互いに素**であるという.

1 と自分自身以外では割り切れない自然数を**素数**という. 2 は素数であるがそれ以外の素数はすべて奇数である. 素数は,

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ \cdots$$

と続き、無限個あることは古代ギリシャから知られていた.

証明は背理法で行う. 素数が有限個しかないとして, それらのすべてを $p_1, p_2, \cdots, p_m$ とする. 自然数 $n = p_1 p_2 \cdots p_m + 1$ を考える. どんな自然数も素数の積に分解するから, n はある素数で割り切れるはずである. しかし, n は $p_1, \cdots, p_m$ のいずれでも割り切れないから矛盾である. よって素数は無限個なければならない.

素数は無限に存在するから, いくらでも大きな素数が存在するはずである. しかし, 具体的に大きな素数を見つけることは大変難しい問題である. 2007 年 6 月現在知られている最大の素数は

$$2^{32582657} - 1$$

であり, その桁数は約 981 万桁. コンピュータを用いた計算によって, 素数であることが示された. この素数のように, $2^n - 1$ の形の素数を**メルセンヌ** (M. Mersenne) **素数**という. この形の整数は素数になるものを多く含んでおり, 2007 年 6 月現在, 素数になる n が 44 個知られている.

素数の世界には不思議な現象が数多くあり, 多くの研究者の興味を惹いている. ここでは, 未解決の問題を 2 つご紹介しておこう.

双子素数

3 と 5, 5 と 7, 11 と 13, 17 と 19 のように, 偶数をはさむ 2 つの素数を**双子素数**という. 双子素数は無限個存在すると予想されているが証明されていない.

ゴールドバッハの予想

4 以上の偶数は 2 つの素数の和として表されると予想されている. $4 = 2 + 2$, $6 = 3 + 3$, $8 = 5 + 3$, $10 = 7 + 3$, $12 = 7 + 5$ など.

重要な性質として, 任意の自然数は一意的に素因数分解される. すなわち, 任意の自然数 n に対し相異なる有限個の素数 $p_1, p_2, \cdots, p_k$ と自然数 $e_1, e_2, \cdots, e_k$ が存在して

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

と, 積の順序を除いて一意的に表示される.

ここで, よく用いる記号を 1 つ導入する. a, b, m を整数とする. $a - b$ が m で割り切れるとき,

$$a \equiv b \pmod{m}$$

とかく.

たとえば, $17 \equiv 2 \pmod{5}$ である.

$a \equiv b \pmod{m}$ であることは, a を m で割った時の余りと b を m で割った時の余りが等しいことと同値である. このとき, a と b は m を法として**合同**であるといい, この式を**合同式**という.

合同関係に対して次が成立する.

補題 1.2 $a, b, c \in \mathbf{Z}$ とする.

(i) $a \equiv a \pmod{m}$.

(ii) $a \equiv b \pmod{m}$ ならば $b \equiv a \pmod{m}$.

(iii) $a \equiv b \pmod{m}$ かつ $b \equiv c \pmod{m}$ ならば $a \equiv c \pmod{m}$.

証明 (i) は明らか. (ii) は, $a - b$ は m で割り切れれば, $b - a$ も m で割り切れることから従う. (iii) を示す. $a \equiv b \pmod{m}$ より整数 x が存在して $a - b = xm$. $b \equiv c \pmod{m}$ より整数 y が存在して $b - c = ym$. したがって, $a - c = (x + y)m$ となるから, $a - c$ は m で割り切れて $a \equiv c \pmod{m}$ となる. ■

補題 1.3 $a|a_1,\ a|a_2,\cdots,\ a|a_n$ ならば, 任意の整数 $b_1,\ b_2,\ \cdots,\ b_n$ に対し, $a|(a_1b_1 + a_2b_2 + \cdots + a_nb_n)$ となる.

証明 $a|a_1,\ a|a_2,\cdots,\ a|a_n$ だから, $c_1,\ c_2,\ \cdots,\ c_n$ が存在して,

$$a_1 = ac_1,\ a_2 = ac_2,\cdots,\ a_n = ac_n$$

となる. よって,

$$a_1b_1 + a_2b_2 + \cdots + a_nb_n = a(c_1b_1 + c_2b_2 + \cdots + c_nb_n)$$

となり結果を得る. ■

演習問題 n を自然数とし, n 個の整数 $\{a_1, a_2, \cdots, a_n\}$ をとる. このとき始めから適当な連続何個か（0 個も許す）を除き、最後の適当な連続何個か（0 個も許す）を除けば, 1 個以上残した残りの和が n で割り切れるようにすることができる.

n を法とする合同を考え, ディリクレ (Dirichlet) の抽き出し論法（鳩小屋の原理）を用いればよい.

ディリクレ (Dirichlet) の抽き出し論法
n 個の抽き出しに $n+1$ 個のものをいれれば, どれかの抽き出しには
2 個以上入っている.

2 ユークリッドの互除法

a, b を 2 つの整数とするとき, a, b の最大公約数を求める問題を考える.

補題 2.1 q, r を $a = qb + r$ を満たす整数とするとき, a, b の最大公約数は b, r の最大公約数に等しい.

証明 正整数 c が a, b を割り切れば, c は r を割り切る. 逆に, c が b, r を割り切れば, c は a を割り切る. 結果はこのことから従う. ■

0 でない整数 a, b の最大公約数を求めるために次のように順次剰余定理を用いる：

$$\begin{aligned}
&a = m_1b + r_1 \quad 0 \le r_1 \le |b| - 1\\
&b = m_2r_1 + r_2 \quad 0 \le r_2 \le r_1 - 1\\
&r_1 = m_3r_2 + r_3 \quad 0 \le r_3 \le r_2 - 1\\
&\vdots
\end{aligned}$$

このとき, $r_1 > r_2 > r_3 > \cdots \geq 0$ だから自然数 n が存在して $r_n \neq 0$, $r_{n+1} = 0$ となる. このとき

$$r_{n-1} = m_{n+1} r_n$$

となるが, r_n は a, b の最大公約数である.

例 2.2 184 と 40 の最大公約数を計算してみよう.

$$\begin{aligned} 184 &= 4 \times 40 + 24 \\ 40 &= 1 \times 24 + 16 \\ 24 &= 1 \times 16 + 8 \\ 16 &= 2 \times 8 \end{aligned}$$

したがって, 184 と 40 の最大公約数は 8 である.

命題 2.3 a, b を 0 ではない整数とし, a, b の最大公約数を d とすれば,

$$\alpha a + \beta b = d$$

となるような整数 α, β が存在する.

証明には上記の記号を用いて,

$$r_1 = a - m_1 b$$

だから, $p_1 = 1, q_1 = -m_1$ とおけば

$$r_1 = p_1 a + q_1 b$$

となる. また,

$$\begin{aligned} r_2 = b - m_2 r_1 &= b - m_2(p_1 a + q_1 b) \\ &= -m_2 p_1 a + (1 - m_2 q_1) b \end{aligned}$$

だから, $p_2 = -m_2 p_1, q_2 = 1 - m_2 q_1$ とおけば

$$r_2 = p_2 a + q_2 b$$

となる. r_1, r_2 を 3 番目の式に代入すれば同様にして,

$$r_3 = p_3 a + q_3 b$$

の形となる. 以下帰納的に

$$r_i = p_i a + q_i b$$

となるが, $i = n$ の時を考えれば, r_n は a, b の最大公約数 d になるから

$$d = r_n = p_n a + q_n b$$

の形に適当な整数 p_n, q_n を用いて表せることがわかる.
　次の系はとくに重要である.

系 2.4 a, b を互いに素な整数とする. このとき,

$$xa + yb = 1$$

となるような整数 x, y が存在する.

証明　命題 2.3 において, $d = 1$ の場合を考えればよい. ■

例 2.5 $a = 13$, $b = 9$ とする. このとき, $x = -2$, $y = 3$ とすれば

$$xa + yb = 1$$

となる.

[**参考**] 命題 2.3 を示すのに次の補題を用いてもよい.

補題 2.6 a, b を 0 ではない整数とし, a, b の最大公約数を d とする. このとき,

$$I = \{xa + yb \mid x, y \in \mathbf{Z}\}$$

とおけば, I は d の倍数全体と一致する. つまり,

$$I = \{zd \mid z \in \mathbf{Z}\}$$

となる.

証明　$a = 1a + 0b$ より $a \in I$ である. 同様に, $b \in I$ となる. もし, a が負の数なら $-a$ は正の数で, $-a = (-1)a + 0b$ だから $-a \in I$ となる. したがって, I は正の整数を含む. I に含まれる正の整数のうち最小の数を c とする. このとき,

$$c = x_1 a + x_2 b$$

となるような整数 x_1, x_2 が存在する. したがって, 任意の整数 x に対し

$$xc = (xx_1)a + (xx_2)b$$

だから, I は c の倍数をすべて含む. 逆を示すために, I の任意の元 z をとる. このとき, 定理 1.1 から整数 q, r が存在して,

$$z = qc + r, \quad 0 \leq r < c$$

と書ける. $z, qc \in I$ だから $z - qc \in I$ となるが, このとき $r \in I$ となって, もし r が零でないなら, c の最小性に反する. よって, I の元はすべて, c の倍数となる. とくに, I の元はすべて c で割り切れる. したがって, とくに, a, b はともに c で割り切れる. d は a, b の最大公約数だから $c \mid d$ となる. 一方, d は a, b の公約数だから, I のすべての元は d で割り切れる. したがって, c も d で割り切れる. 以上から, $c = d$ となり結果を得る. ■

3 合同式

補題 3.1 $a_1 \equiv a_2 \pmod{m}$, $b_1 \equiv b_2 \pmod{m}$ とすれば,

$$a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod{m}$$
$$a_1 b_1 \equiv a_2 b_2 \pmod{m}$$

が成立する.

証明 仮定から $a_1 - a_2 = xm$, $b_1 - b_2 = ym$ となる整数 x, y が存在する. これを用いて,

$$(a_1 \pm b_1) - (a_2 \pm b_2) = (x \pm y)m$$
$$a_1 b_1 - a_2 b_2 = a_1(b_1 - b_2) + (a_1 - a_2)b_2 = (a_1 y + b_2 x)m$$

を得る. 結果はこのことから従う. ■

整数 m を 1 つ固定して考える. 整数 a に対し,

$$\bar{a} = \{x \in \mathbf{Z} \mid x \equiv a \pmod{m}\}.$$

とおき, a の定める法 m に関する**合同類**という. a を合同類 $\bar{a}$ の代表元という. $\bar{a}$ は, m を法として整数 a と合同な整数全体の集合である. m を法として整数 a と合同な整数はすべて $\bar{a}$ の代表元となる. 法 m に関する合同類全体の集合を $\mathbf{Z}/m\mathbf{Z}$ と書く. a を m で割った余りを r $(0 \leq r \leq m-1)$ とすれば, $a \equiv r \pmod{m}$ だから, $r \in \bar{a}$ であり, $\bar{r} = \bar{a}$ となる. このことから法 m に関する合同類は, m で割った余りの分だけ存在する. 従って,

$$\mathbf{Z}/m\mathbf{Z} = \{\bar{0},\ \bar{1},\ \cdots,\ \overline{m-2},\ \overline{m-1}\}$$

となり, その元は m 個存在する. ここで, 合同類全体の集合に和と積の構造を自然に入れることができることを示そう.

この補題を用いて $\mathbf{Z}/m\mathbf{Z}$ に, 和と積を定義しよう.

$\bar{a}, \bar{b} \in \mathbf{Z}/m\mathbf{Z}$ に対し

$$\text{和} \ : \ \bar{a} + \bar{b} = \overline{a+b}$$
$$\text{積} \ : \ \bar{a} \cdot \bar{b} = \overline{ab}$$

補題 3.1 からこれらの演算はうまく定義できる.

ここに, $\bar{0}$ は零元の役割を果たし, $\bar{1}$ が 1 の役割をはたす. つまり, $\bar{a} \in \mathbf{Z}/m\mathbf{Z}$ に対し,

$$\bar{a} + \bar{0} = \bar{0} + \bar{a} = \bar{a}$$
$$\bar{a}\bar{1} = \bar{1}\bar{a} = \bar{a}$$

が成り立つ. また, 積の記号 $\cdot$ はしばしば省略し, $\bar{a} \cdot \bar{b}$ を $\bar{a}\bar{b}$ と書くことが多い. 1 つ例を挙げておこう.

例 3.2 $\mathbf{Z}/4\mathbf{Z}$ は $\bar{0}$, $\bar{1}$, $\bar{2}$, $\bar{3}$ の 4 個の元からなる. たとえば,

$$\bar{1} + \bar{2} = \bar{3}, \quad \bar{2} + \bar{3} = \bar{5} = \bar{1}$$
$$\bar{2} \cdot \bar{2} = \bar{4} = \bar{0}, \quad \bar{2} \cdot \bar{3} = \bar{6} = \bar{2}$$

が成り立つ.

4 フェルマーの小定理

補題 4.1 a, b, c を整数, m を自然数とし, m と c は互いに素であるとする. このとき, $ac \equiv bc \pmod{m}$ ならば, $a \equiv b \pmod{m}$ が成り立つ.

証明 系 2.4 を用いれば, 整数 x, y で $cx + my = 1$ となるものが存在する. よって,

$$a = acx + amy, \ b = bcx + bmy$$

となる. ゆえに, $a - b = (ac - bc)x + (ay - by)m$ となるが, 仮定からこの右辺は m で割り切れる. 従って, $a - b$ も m で割り切れる. ■

次の定理は重要である.

定理 4.2 (フェルマー (Fermat) の小定理) a を素数 p で割り切れない整数とすれば

$$a^{p-1} \equiv 1 \pmod{p}$$

が成り立つ.

証明 $\mathbf{Z}/p\mathbf{Z}$ の $\bar{0}$ 以外の元の集合を

$$\{a_1, a_2, \cdots, a_{p-1}\}$$

とする. a は p で割り切れないから, 補題 4.1 より, 集合として

$$\{a_1, a_2, \cdots, a_{p-1}\} = \{\bar{a}a_1, \bar{a}a_2, \cdots, \bar{a}a_{p-1}\}$$

となる. ゆえに,

$$\begin{aligned} a_1 \cdot a_2 \cdot \cdots \cdot a_{p-1} &= \bar{a}a_1 \cdot \bar{a}a_2 \cdot \cdots \cdot \bar{a}a_{p-1} \\ &= \bar{a}^{p-1} a_1 \cdot a_2 \cdot \cdots \cdot a_{p-1} \end{aligned}$$

となる. $a_1 \cdot a_2 \cdot \cdots \cdot a_{p-1}$ は $\mathbf{Z}/p\mathbf{Z}$ で零ではないから, 再び補題 4.1 より

$$\bar{a}^{p-1} = \bar{1}$$

となる. これは求める式にほかならない. ■

例 4.3 $p = 71$ は素数, $a = 1666$ は 71 で割り切れない. よって,

$$1666^{70} \equiv 1 \ (mod\ 71)$$

5 因数分解法

必ずうまくいくような高速の因数分解の方法は存在しない（と信じられている）.

1. 試行割算法
   小さな素数から順に割り算を実行して素因子を探す方法.

2. $p-1$ 法
   自然数 n の素因子 p に対して, $p-1$ が小さな素数の積に分解するような場合に有効な方法.

例 5.1 $n = 98093$ の因数分解を考える. $B = 7! = 5040$ とおく. B が $p-1$ の倍数にうまくなっていれば, つまり自然数 ℓ が存在して $B = \ell(p-1)$ であれば, フェルマーの定理によって

$$2^B - 1 = (2^{p-1})^\ell - 1 \equiv 1^\ell - 1 \equiv 0 \ (\mathrm{mod}\ p)$$

となるから, 2^B-1 は p で割り切れる. これを信じて, $2^{5040}-1 \equiv 24840-1 \pmod{98093}$ と 98093 の最大公約数をユークリッドの互除法で計算する. このときは, うまく最大公約数 $d = 421$ が得られる. よって, 因数分解

$$98093 = 421 \times 233$$

を得る. うまくいったのは, $421 - 1 = 420 = 2^2 \times 3 \times 5 \times 7$ と小さな素数の因数分解に（偶然）なっていたからである.

3. モンテ・カルロ法（ρ 法）

1975 年にポラードによって考案された因数分解法. 自然数 n の素因子 p を見つけたいとき,

$$a_0 = 1,\ a_{i+1} \equiv a_i^2 + 1 \pmod{n}$$

で次々に a_i を計算していく.

a_i を p で割った余りは

$$0,\ 1,\ 2,\ \cdots,\ p-1$$

の p 通りしかないので, $a_0, a_1, \cdots, a_p$ の中に p で割ったあまりが同じものがある. つまり, i, j で

$$a_i \equiv a_j \pmod{p}$$

となるものがある. このとき

$$a_{i+1} \equiv a_i^2 + 1 \equiv a_j^2 + 1 \equiv a_{j+1} \pmod{p}$$

なので, a_i 以降は $k = j - i$ 周期であることがわかる. $i \leq k\ell$ となるような整数 $m = k\ell$ をとれば, 周期性から

$$a_m \equiv a_{2m} \pmod{p}$$

となり, $a_{2m} - a_m$ は p を約数にもつ持つ. このようにして, n と $a_{2m} - a_m$ の公約数として, n の真の約数が運がよければ求まるかもしれない. 実際には p がわからないから m もわからない. したがって, s の小さい方から $a_{2s} - a_s$ と n との最大公約数を順に計算し, 幸運を期待するのである.

例 5.2 $n = 35$ とする. a_i を法 35 で計算すると,

$$a_0 = 1,\ a_1 = 2,\ a_2 = 5,\ a_3 = 26,\ a_4 = 12,\ a_5 = 5,\ \cdots,$$

となる. そこで, $a_4 - a_2 = 7$ と $n = 35$ の最大公約数を計算して 7 をうる. よって, 因数分解 $35 = 7 \times 5$ をうる.

4. 2次ふるい法

$n = 3937$ のとき,

$$\sqrt{3937} \fallingdotseq 63$$

だから

$$63^2 - n = 32 = 2^5$$
$$64^2 - n = 159 = 3 \times 53$$
$$65^2 - n = 288 = 2^5 \times 3^2$$
$$66^2 - n = 419$$
$$67^2 - n = 552 = 2^3 \times 3 \times 23$$

1番目の式と3番目の式をかけると

$$(63 \times 65)^2 \equiv (2^5 \times 3)^2 \pmod{n}$$

一般に

$$x^2 - y^2 \equiv 0 \pmod{n}$$

なら, $(x-y)(x+y)$ は n で割り切れるから, うまくいけば $x-y$ と n に公約数があることが期待される. この原理を用いて, $63 \times 65 - 2^5 \times 3 = 3999$ と 3937 の最大公約数をユークリッドの互除法で計算すれば 31 をうる. よって, 因数分解 $3937 = 31 \times 127$ をうる.

6 いろいろな数

2つの整数の商として表される数を**有理数**という. 有理数全体を $\mathbf{Q}$ と書く:

$$\mathbf{Q} = \{-\frac{2}{3}, -1, 0, 4/5, 25/33, \cdots\}$$

有理数を大小順に直線上に並べると, $\sqrt{2}$ のように有理数の間に入る数がある. このように, 有理数の間を埋める数を**無理数**という. 有理数と無理数をあわせて**実数**という. 円周率 π, 自然対数の底 e は無理数であることが知られている. 実数全体の集合を $\mathbf{R}$ と書く:

$$\mathbf{R} \ni -2/3, -1, 0, \sqrt{2}, \pi, e, \cdots$$

2乗して -1 になる数を仮想的に考え $\sqrt{-1}$ とおく. $\sqrt{-1}$ を**虚数単位**という. 虚数単位を $i = \sqrt{-1}$ とおくことが多い. $a, b \in \mathbf{R}$ をとり, $a + b\sqrt{-1}$ なる「数」を考える. これは, 人類が作った想像上の数であり, **複素数**と呼ばれる. a を**実部**, b を**虚部**という. 複素数全体の集合を $\mathbf{C}$ とおく:

$$\mathbf{C} = \{a + bi \mid a, b \in \mathbf{R}, i = \sqrt{-1}\}$$

$\mathbf{C}$ の 2 元 $\alpha_1 = a_1 + b_1 i$, $\alpha_2 = a_2 + b_2 i$ は, $a_1 = a_2$ かつ $b_1 = b_2$ のときに限り相等しい. 実数 a は $a + 0\sqrt{-1}$ によって複素数と見なすことができる. これによって,

$$\mathbf{C} \supset \mathbf{R} \supset \mathbf{Q}$$

となる. 実数でない複素数 $a + bi$ $(b \neq 0)$ を**虚数**, bi の形の複素数を**純虚数**という.

$\mathbf{C}$ の 2 元 $\alpha_1 = a_1 + b_1 i$, $\alpha_2 = a_2 + b_2 i$ に対し, 和を

$$\alpha_1 + \alpha_2 = (a_1 + a_2) + (b_1 + b_2)i,$$

積を

$$\alpha_1 \cdot \alpha_2 = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)i$$

によって定義する. これによって, 有理数全体の集合 $\mathbf{Q}$ や実数全体の集合 $\mathbf{R}$ の場合と同様に, 和（足し算）と積（かけ算）が定義できる. 複素数 $z = a + bi$ に対し, $\bar{z} = a - bi$ とおき, z の**複素共役**という.

定理 6.1 (代数学の基本定理) (Gauss, 1799) 複素数 a_0, a_1, $\cdots$, a_n; $a_0 \neq 0$ を係数とする n 次代数方程式

$$a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n = 0$$

は, 重複を数えて $\mathbf{C}$ に n 個の解をもつ.

ここで, 代数方程式の解の公式について考えてみよう. 2 次方程式

$$x^2 + ax + b = 0$$

の解の公式はすでに学んでいるように

$$x = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

で与えられる. 3 次方程式, 4 次方程式についても, 解は, 係数を用いて, それらの加減乗除とべき根によって具体的に表示されることが１６世紀から知られている. 3 次方程式の解の公式は**カルダノ** (G. Cardano) **の公式**, 4 次方程式の解の公式は**フェラーリ** (L. Ferrari) **の公式**と呼ばれている. このように, 代数方程式の解が, 係数を用いて, それらの加減乗除とべき根によって具体的に表示されるとき, 代数方程式は代数的に解けるという. この言い方を用いれば, 4 次以下の任意の代数方程式は代数的に解くことができる. これに対し 5 次以上の代数方程式の場合には状況が異なっており, 19 世紀前半次のことが示された.

定理 6.2 (Abelの定理) ５次以上の一般代数方程式は, 代数的には解けない. つまり, 係数の加減乗除と巾根だけを用いた解の公式は存在しない.

さて, 有理数全体の集合 $\mathbf{Q}$, 実数全体の集合 $\mathbf{R}$, 複素数全体の集合 $\mathbf{C}$ には, 和と積が定義できるということはすでに述べた. 和と積のみたす性質を抽出すると次のようになる.

定義 6.3 集合 K に和 $+$, 積 $\cdot$ が定義されていて次をみたす時, K を**体**という.

$a, b, c \in K$ とする.

(I) (和 $+$ に関して)

(i) (結合法則) $(a+b)+c = a+(b+c)$

(ii) (零元の存在) 任意の $a \in K$ に対し, $0+a = a+0 = a$ となる元 0 が存在する.

(iii) (和に関する逆元の存在) $a \in K$ に対し $a+a' = a'+a = 0$ となる元 $a' \in K$ が存在する.

(iv) (可換性) $a+b = b+a$

(II) (積 $\cdot$ に関して)

(i) (結合法則) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(ii) (単位元の存在) 任意の $a \in K$ に対し $1 \cdot a = a \cdot 1 = a$ となる元 1 が存在する.

(iii) (積に関する逆元の存在) $b \in K$, $b \neq 0$ に対し $b \cdot b' = b' \cdot b = 1$ となる元 $b' \in K$ が存在する.

(iv) (可換性) $a \cdot b = b \cdot a$

(III) (分配法則)

(i) $(a+b) \cdot c = a \cdot c + b \cdot c$

(ii) $a \cdot (b+c) = a \cdot b + a \cdot c$

積を表す記号 $\times$ や $\cdot$ はしばしば省略され, $a, b \in K$ に対し, $a \cdot b$ をしばしば ab と書く.

有理数全体の集合 $\mathbf{Q}$, 実数全体の集合 $\mathbf{R}$, 複素数全体の集合 $\mathbf{C}$ にはいる和, 積がこれらの条件をみたすことはよく知っている事実である. したがって, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ は体になる. 有理整数全体の集合 $\mathbf{Z}$ は, 先にあげた体の性質のうち, 性質 (II)(iii) 以外の性質をみたす. このような代数系を可換環という.

定義 6.4 先にあげた体の性質のうち, 性質 (II)(iii) 以外の性質をみたす和 $+$ と積 $\cdot$ が与えられた集合 R を**可換環**という.

可換環や体は, 現代代数学において中心的な役割を果たす代数系である.

定義 6.5 ある複素数 α が適当な有理数 $a_0,\ a_1,\ \cdots,\ a_n;\ a_0 \neq 0$ を係数とする代数方程式

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n = 0$$

の解になるとき, α を**代数的数**という. そうではない数を**超越数**という.

代数的数, 超越数の興味ある例をいくつか挙げておこう.

例 6.6 ・有理数 a は代数的数である.
なぜならば, 有理係数の 1 次方程式 $x - a = 0$ の解になる.
・$\sqrt{a}\ \ (a \in \mathbf{Q})$ は代数的数である.
なぜならば, 有理係数の 2 次方程式 $x^2 - a = 0$ の解になる.
・円周率 π は超越数である（Lindemann, 1882）.
・自然対数の底 e は超越数である（Hermite, 1873）.
・$\alpha,\ \alpha \neq 0, 1$ を代数的数, β を代数的な無理数, とすれば, α^β は超越数である. この事実によって, たとえば $2^{\sqrt{2}}$ は超越数となる（ヒルベルト (D. Hilbert) の第 7 問題：A. O. Gel'fond（1934 年）, T. Schneider（1935 年））. 同様に, $\sqrt{2}^{\sqrt{2}}$ は超越数となる.
・$\alpha,\ \alpha \neq 0$ を代数的数とすれば, e^α は超越数である. たとえば, $e^{\sqrt{2}}$ は超越数であることがわかる.

7　ガウス整数

代数的数を用いた整数論の一例をあげてみよう. 整数の拡張として次のような数全体を考える:

$$\mathbf{Z}[i] = \{a + bi \ \mid \ a, b \in \mathbf{Z},\ i = \sqrt{-1}\}$$

この集合の元 $a + bi\ (a,\ b \in \mathbf{Z})$ を**ガウス** (C. F. Gauss) **整数**という. また, 有理整数に対する有理数に当たるものとして,

$$\mathbf{Q}(i) = \{a + bi \ \mid \ a, b \in \mathbf{Q}\}$$

を考える. $a + bi,\ c + di \in \mathbf{Q}(i)\ (c + di \neq 0)$ に対し,

$$(a + bi)/(c + di) = (ac + bd)/(c^2 + d^2) + (-ad + bc)i/(c^2 + d^2) \in \mathbf{Q}(i)$$

だから, $\mathbf{Q}(i)$ は体になる. $\mathbf{Q}(i)$ の任意の元 $z = a + bi$ $(a, b \in \mathbf{Q})$ は 2 次方程式

$$X^2 - 2aX + a^2 + b^2 = 0$$

をみたすから代数的数である. そのうち $\mathbf{Z}[i]$ に入る元が「整数」にあたり, これをガウス整数というのである.

次の命題は, 有理整数を用いた整数論の議論の代表的な例である.

命題 7.1 $\sqrt{2}$ は無理数である.

証明 背理法で証明するために, $\sqrt{2}$ が有理数であるとする. このとき, 互いに素な自然数 a, b で

$$\sqrt{2} = a/b$$

となるものが存在する. 分母を払って 2 乗して

$$2b^2 = a^2$$

を得る. したがって, a は 2 で割り切れる. よって, 自然数 c が存在して, $a = 2c$ となる. したがって,

$$b^2 = 2c^2$$

を得る. この式から b も 2 で割り切れる. これは, a, b が互いに素であるという仮定に反する. よって, $\sqrt{2}$ は無理数である. ■

このような整除の議論をガウス整数を用いても行うことができる. 例として次のような問題を取り上げてみよう.

問題 1. 素数 p に対し $p = x^2 + y^2$ となる整数 x, y が存在するか.

小さな素数について考えてみよう.

$$
\begin{array}{ll}
p & = x^2+y^2 \\
2 & = 1^2+1^2 \\
3 & \\
5 & = 1^2+2^2 \\
7 & \\
11 & \\
13 & = 2^2+3^2 \\
17 & = 1^2+4^2 \\
19 & \\
23 & \\
29 & = 2^2+5^2 \\
31 & \\
37 & = 1^2+6^2 \\
41 & = 4^2+5^2 \\
43 & \\
47 & \\
53 & = 2^2+7^2 \\
\vdots &
\end{array}
$$

これらから推測できるように, 次の定理が成立する.

定理 7.2 素数 p に対し $p = x^2 + y^2$ となる整数 x, y が存在するための必要十分条件は, $p = 2$ または $p \equiv 1 \pmod 4$ となることである.

整数 x, y を用いて素数 p が $p = x^2+y^2$ と書けるということは, $p = (x+yi)(x-yi)$ と 2 つのガウス整数 $x+yi$, $x-yi$ の積に因数分解できるということである. 素数 p が $p = 2$ または $p \equiv 1 \pmod 4$ の時に限りこのように因数分解できるのである.

8 有限体

Q, **R**, **C** が体になることはすでに述べた. これらの体は, それぞれ無限個の元を含んでいる. それでは, 有限個の元しか含まない体（有限体）は存在するのであろうか. 1830 年, フランスの数学者ガロア (E. Galois: 1811-1832) は論文「数の理論について (Sur la théorie des nombres)」を発表し, その中で有限個の元からなる集合に和と積を与えて体になるものが存在することを示した. この体を**有限体**という. 有限体は, 発見者にちなんで**ガロア体**ともよばれている.

まず, $m=2$ とし, 2 元からなる集合 $\mathbf{Z}/2\mathbf{Z}=\{\bar{0},\bar{1}\}$ をとり, 前節で定義した和, 積を考える. 具体的に書けば, 和は

$$\bar{0}+\bar{0}=\bar{0},\quad \bar{0}+\bar{1}=\bar{1},$$
$$\bar{1}+\bar{0}=\bar{1},\quad \bar{1}+\bar{1}=\bar{0}.$$

積は

$$\bar{0}\cdot\bar{0}=\bar{0},\quad \bar{0}\cdot\bar{1}=\bar{0},$$
$$\bar{1}\cdot\bar{0}=\bar{0},\quad \bar{1}\cdot\bar{1}=\bar{1}.$$

である. これによって $\mathbf{Z}/2\mathbf{Z}$ は体の公理をみたすから, 体になる. このようにして 2 元からなる体が構成できる. この体を $\mathbf{F}_2$ と書く.

さらに一般に, p をある素数とし,

$$\mathbf{Z}/p\mathbf{Z}=\{\bar{0},\bar{1},\cdots,\overline{p-1}\}$$

を考える. この合同類の集合に和と積は

$$\bar{a}+\bar{b}=\overline{a+b},\ \bar{a}\cdot\bar{b}=\overline{a\cdot b}$$

によって定義される.

定理 8.1 *p を素数とすれば, $\mathbf{Z}/p\mathbf{Z}$ は体になる.*

証明 $\bar{0}$ が零元, $\bar{1}$ が単位元となる. 体の条件のうち, 積に関する逆元の存在以外の条件は明らかに成立する. そこで, 任意の $\bar{a}\neq\bar{0}$ をとり, この元に逆元があることを証明しよう. p は素数だから, a は p と互いに素となる. ゆえに, 整数 x,y が存在して

$$xa+yp=1$$

となる. この式を法 p で考えれば, $\bar{x}\bar{a}=\bar{1}$ となり, $\bar{x}$ が $\bar{a}$ の逆元となる. ■

体 $\mathbf{Z}/p\mathbf{Z}$ を $\mathbf{F}_p$ と書く. これは, p 個の元を持つ有限体になる. $m\geq 2$ なる整数が素数でなければ, $\mathbf{Z}/m\mathbf{Z}$ は体にはならない. たとえば, $\mathbf{Z}/6\mathbf{Z}$ を考えれば, $\bar{2}\cdot\bar{3}=\bar{0}$ であるから, $\bar{2}\neq\bar{0}$ だがこの元は逆元をもたず, したがって $\mathbf{Z}/6\mathbf{Z}$ は体ではない.

さらに一般には, n を自然数として, $q=p^n$ とおけば, q 個の元をもつ有限体 $\mathbf{F}_q$ が存在することが知られている. また, 任意の有限体は, ある素数 p とある自然数 n に対して $\mathbf{F}_{p^n}$ の形になることも知られている.

9　整数論の定理

公開鍵暗号の 1 つである RSA 暗号の解説をするための数学的準備を行う. p, q を 2 つの素数とする. 可換環 $\mathbf{Z}/pq\mathbf{Z}$ を考え

$$(\mathbf{Z}/pq\mathbf{Z})^* = \{\bar{a} \mid a \in \mathbf{Z},\ ab \equiv 1 \pmod{pq} \text{ となる整数 } b \text{ が存在する.}\}$$

とおく. これは, 可換環 $\mathbf{Z}/pq\mathbf{Z}$ の元のうち, 乗法に関する逆元を有するもの全体の集合である. すなわち, $\bar{a} \in (\mathbf{Z}/pq\mathbf{Z})^*$ であるための必要十分条件は, $\bar{b} \in (\mathbf{Z}/pq\mathbf{Z})^*$ が存在して

$$\bar{a}\bar{b} = \bar{1}$$

となることである. また,

$$ab \equiv 1 \pmod{pq},\ a'b' \equiv 1 \pmod{pq}$$

ならば, 7 ページの補題 3.1 から

$$aa'bb' \equiv 1 \pmod{pq}$$

だから,

$$\bar{a},\ \bar{a'} \in (\mathbf{Z}/pq\mathbf{Z})^* \implies \bar{a}\bar{a'} \in (\mathbf{Z}/pq\mathbf{Z})^*$$

となる. すなわち, $(\mathbf{Z}/pq\mathbf{Z})^*$ は乗法に関して閉じている. $\mathbf{Z}/pq\mathbf{Z}$ は

$$\bar{0},\ \bar{1},\ \bar{2},\ \cdots,\ \overline{pq-2},\ \overline{pq-1}$$

からなり, その元数は pq 個である. そのうち, $(\mathbf{Z}/pq\mathbf{Z})^*$ に入る元数は $0 \leq a \leq pq-1$ なる整数 a で pq と互いに素なものの数に等しいから

$$(p-1)(q-1)$$

個である. このことから, フェルマーの小定理の一般化として次の結果を得る.

補題 9.1 *$a \in (\mathbf{Z}/pq\mathbf{Z})^*$ ならば,*

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$$

が成り立つ.

例 9.2 *$p = 71, q = 97$ とし, $n = pq = 6887$ を考える. このとき, $(p-1)(q-1) = 6720$. $a = 1687$ をとれば, 1687 は 71, 97 で割り切れないから $\overline{1687} \in (\mathbf{Z}/6887\mathbf{Z})^*$ である. このとき*

$$1687^{6720} \equiv 1 \pmod{6887}$$

を得る.

有限体についてもう一つ大事な定理を述べておこう. $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ の元 $\bar{a}$ で $\bar{a}^i$ $(i = 1, 2, 3, \cdots)$ が $\mathbf{F}_p$ の $\bar{0}$ 以外の元を尽くすとき, a を法 p に関する**原始根**という. 逆にいうと, a を p を法とする原始根とすれば,

$$\mathbf{F}_p = \{\bar{0}, \bar{a}, \bar{a}^2, \bar{a}^3, \cdots, \bar{a}^{p-2}, \bar{a}^{p-1} = \bar{1}\}$$

となる. 原始根について次の定理が知られている.

定理 9.3 素数 p に対して, p を法とする原始根が少なくとも 1 個存在する.

例 9.4

$$\mathbf{F}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

を考えれば, 各元の逆元は

$$\bar{1}^{-1} = \bar{1},\ \bar{2}^{-1} = \bar{3},\ \bar{3}^{-1} = \bar{2},\ \bar{4}^{-1} = \bar{4}$$

である. また, $\bar{2}$ を考えれば

$$\bar{2},\ \bar{2}^2 = \bar{4},\ \bar{2}^3 = \bar{3},\ \bar{2}^4 = \bar{1}$$

となって, $\mathbf{F}_5$ の $\bar{0}$ 以外の元をすべて得るから, 2 は 5 を法とする原始根である. 同様に, 3 も 5 を法とする原始根である.

p を素数とし, 法 p に関する原始根 g を 1 つ選ぶ. 原始根の定義から g のべき乗が $\mathbf{Z}/p\mathbf{Z}$ の $\bar{0}$ 以外の元をすべて尽くす. このとき, g^r を p で割った余り a を計算し $\bar{a} \in \mathbf{Z}/p\mathbf{Z}$ を求めることは, コンピュータにとってやさしい仕事である. しかし, p が巨大な素数の場合, 逆に $\bar{a}$ から r を計算することは, コンピュータにとっても途方もなく時間のかかる問題である. この問題を**離散対数問題**という.

$$a \equiv g^r \pmod{p},\ 1 \leq r \leq p-1$$

となるとき, r を a の**離散対数**と呼び

$$\mathrm{ind}_g a = r$$

と書く. $1 \leq a \leq p-1$ ならば, a の離散対数 r で $1 \leq r \leq p-1$ となるものがただ 1 つ存在する.

例 9.5 $p = 5$ の場合は, 2 は原始根だから, それを用いた離散対数は次のようになる.

	1	2	3	4
ind_2	4	1	3	2

10　RSA 暗号

暗号化の鍵と解読するための鍵を, 発信者と受信者が共有して用いる方式の暗号を**共通鍵暗号**という. これに対し, ディフィー (W. Diffie) とヘルマン (M. Hellman) は, 1976 年, 暗号化の鍵を公開しても, 多数の人の中で不特定の 2 人が暗号通信を行うことができるという理論を発表した. これが**公開鍵暗号**と呼ばれる暗号方式である. ここでは, たとえ強力なコンピューターを用いても, 計算を完了するためには途方もない時間がかかり, したがって解読できないという原理を用いる. その暗号方式の構成には, 次のいずれかに基づくものが代表的である.

(i) 素因数分解問題の困難に基づくもの.

(ii) 離散対数問題の困難に基づくもの.

公開鍵暗号の代表的な例である **RSA 暗号**の紹介をしよう. この暗号は 1978 年にリヴェスト (R. Rivest), シャミア (A. Shamir), アドルマン (L. N. Adleman) によって発表された. RSA 暗号は, 2 つの大きな素数の積を素因数分解することが難しいことに基づく公開鍵暗号である. ユーザー B が暗号を送信し, ユーザー A が受信し秘密情報を得るという設定である.

まず, ユーザー A は大きな素数 p, q を選び, $n = pq$ とおく. $\mathbf{Z}/(p-1)(q-1)\mathbf{Z}$ の元 e で

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

となる元 d が存在するものをランダムに選ぶ. そこで, n, e を公開する. ユーザー A は p, q, d を秘密鍵として, 秘匿しておく.

ユーザー B がユーザー A に平文 $M \in (\mathbf{Z}/n\mathbf{Z})^*$ を送信するために,

$$M^e \pmod{n}$$

を計算し暗号化する. n の因数分解が困難であるため, 第三者は d を計算できず, $M^e \pmod{n}$ から M を復元できないが, ユーザー A は n の因数分解を知っているため d を計算でき, $(M^e)^d \equiv M \pmod{n}$ によって, 平文 M を復元できるのである.

実際に復元できていることを示しておこう.

18 ページの補題 9.1 から,

$$M^{(p-1)(q-1)} \equiv 1 \pmod{n}.$$

$ed \equiv 1 \pmod{(p-1)(q-1)}$ だから, ある整数 s があって

$$ed = (p-1)(q-1)s + 1$$

となる. したがって,

$$\begin{aligned} M^{ed} \pmod n &\equiv M^{(p-1)(q-1)s+1} \pmod n \\ &\equiv (M^{(p-1)(q-1)})^s M \pmod n \\ &\equiv M \pmod n \end{aligned}$$

となる.

例 10.1 $p = 71, q = 97$ の場合を考える. $n = pq = 6887$ である. このとき, $(\mathbf{Z}/6887\mathbf{Z})^*$ の元数は $(p-1)(q-1) = 6720$. $e = 13$ とすれば, ユークリッドの互除法を用いて,

$$6720 = 516 \times 13 + 12,\ 13 = 1 \times 12 + 1$$

から,

$$13 \times 517 = 6720 + 1$$

を得る. よって, $d = 517$ とすれば,

$$13 \times 517 \ \equiv \ 1 \pmod{6720}$$

となる. 平文 $M = 1687$ をこのシステムで暗号化すれば,

$$M^e = 1687^{13} \ \equiv \ 57 \pmod{6887}$$

ユーザー B は暗号文 57 をユーザー A に送る. ユーザー A は

$$57^d = 57^{517} \equiv \ 1687 \pmod{6887}$$

によって平文 $M = 1687$ を復元することができる.

11 素数分布とリーマンのゼータ関数

11.1 与えられた素数の有限集合と互いに素になる確率

1. 連続する自然数の集合 $S = \{a+1, a+2, \cdots, b-1, b\}$ からひとつ数 x を選んだときにそれが偶数である確率は $b-a$ が十分大きいと $\frac{1}{2}$ といえる.

2. 同じく 3 で割れる確率は $\frac{1}{3}$ といえる.

3. ベン図を描いてみればわかるように, 2 でも 3 でも割り切れない確率は

$$1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{6}$$

となる. 重なる部分が 6 の倍数となっていることに注意.

4. 2 でも 3 でも, そして 5 でも割り切れない確率は同様に

$$1-\frac{1}{2}-\frac{1}{3}-\frac{1}{5}+\frac{1}{2\cdot 3}+\frac{1}{2\cdot 5}+\frac{1}{3\cdot 5}-\frac{1}{2\cdot 3\cdot 5}$$

と計算されるが, これは幸運にも因数分解できてしまう.

$$=(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5})$$

5. （作業仮定）ある数 $n+1$ が素数になるためには n 以下の素数と互いに素となることが必要十分なので（もう少し節約して $\sqrt{n}$ 以下の素数で確かめればよいが ... ）n 以下の素数を $p_1, \ldots, p_m$ とおくと, $n+1$ が素数になる確率は

$$(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_m}) \tag{1}$$

と考えてよいのではないか.

11.2 無限等比級数, 素因数分解の一意性

1. 等比級数の和の公式

$$1+x+x^2+\cdots+x^n=\frac{1-x^{n+1}}{1-x}$$

$0<x<1$ の時は無限和を考えることができる. つまり上の極限をとる.

$$\sum_{i=0}^{\infty}x^i=1+x+x^2+\cdots=\frac{1}{1-x}$$

2. 上の x として $0<\frac{1}{p_1}<1$ をとれば

$$\frac{1}{1-\frac{1}{p_1}}=1+\frac{1}{p_1}+\frac{1}{p_1^2}+\frac{1}{p_1^3}+\cdots=\sum_{i=0}^{\infty}\frac{1}{p_1^n}$$

3. 1 から n までの数はただ一通りに素因数分解され, かつその因数は $\{p_1, \ldots, p_m\}$ の元なので,

$$(\frac{1}{1-\frac{1}{p_1}})(\frac{1}{1-\frac{1}{p_2}})\cdots(\frac{1}{1-\frac{1}{p_m}})$$

の展開には $\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}$ が一度づつでてきて, さらに出てくる項はすべて正の数.

4. 従って下の不等式をえる.

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}\leq(\frac{1}{1-\frac{1}{p_1}})(\frac{1}{1-\frac{1}{p_2}})\cdots(\frac{1}{1-\frac{1}{p_m}}) \tag{2}$$

この式の右辺と式 (1) は逆数になっている.

11.3 調和級数と対数

1.

$$\begin{aligned}&1+\tfrac{1}{2}+(\tfrac{1}{3}+\tfrac{1}{4})+(\tfrac{1}{5}+\tfrac{1}{6}+\tfrac{1}{7}+\tfrac{1}{8})+\cdots+(\tfrac{1}{2^k}+\tfrac{1}{2^k+1}+\cdots+\tfrac{1}{2^{k+1}})\\ &\geq 1+\tfrac{1}{2}+2\times\tfrac{1}{4}+4\times\tfrac{1}{8}+\cdots+2^k\times\tfrac{1}{2^{k+1}}\\ &\geq 1+\tfrac{k+1}{2}\end{aligned}$$

2. 従って

$$\sum_{i=1}^{2^k}\frac{1}{i}\geq 1+\frac{k}{2}$$

3. 一般に正の実数 x に対して $x=2^y$ となる y が定まる. この y のことを x の 2 を底とする対数という. そして $y=\log_2 x$ とあらわす. このとき任意の自然数 n に対して

$$\sum_{i=1}^{n}\frac{1}{i}\geq 1+\frac{\log_2 n}{2} \tag{3}$$

が成立する.

4. 結論. 不等式 (2) と不等式 (3) より $n+1$ が素数である確率 (1) は

$$(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_m})\leq\frac{2}{2+\log_2 n}$$

という不等式を満たす. この不等式の右辺は大変ゆっくりではあるが 0 に近づいていくことがわかる.

5. 実は

$$\lim_{X\to\infty}\frac{(\{p:\text{素数}\mid p<X\}\text{の個数})\cdot\log X}{X}=1$$

がルジャンドル（とガウス）により予想され, アダマール-ドゥラバレ-プサンにより証明された. ここで log の底としては自然対数の底

$$e = \lim_{n\to\infty}(1+\frac{1}{n})^n$$

をとる. これは素数の分布がランダムであることを表している定理である. 証明には複素関数論（複素数を使った微積分学）が不可欠.

6. さらに良い評価

$$\frac{\sharp\{p : \text{素数} \mid p < X\} - \int_2^X \frac{dt}{\log(t)}}{\sqrt{X}\log X}$$

が X について有界関数となるという予想があり, ゼータ関数という複素数関数がどこで値が 0 になるかという, 有名なリーマン予想と同値である.

7. リーマンのゼータ関数

$$\zeta(s) = 1 + 1/2^s + 1/3^s + \cdots + 1/n^s + \cdots$$

オイラー積表示

$$\zeta(s) = \prod_{p:\text{素数}} (1-p^{-s})^{-1}$$

$s =$ 正の偶数, での値

$$\zeta(2) = \pi^2/6, \quad \zeta(4) = \pi^4/90, \quad \zeta(6) = \pi^6/945, \cdots$$

$s =$ 負の偶数, での値

$$\zeta(-2n) = 0$$

リーマン予想

$\zeta(s)$ の負の偶数以外の零点はすべて s の実部が $1/2$ の直線上に存在する.