定義 (約数，倍数，$b \mid a$)． 整数 $a, b \in \mathbb{Z}$, $b \neq 0$ に対して，$a = bc$ となる整数 $c \in \mathbb{Z}$ が存在するとき，b **は** a **を割り切る**，b **は** a **の約数** (divisor)，a **は** b **の倍数** (multiple) などと言い，$b \mid a$ **と表す**．

例 (割り切る)． -2 は 4 を割り切り，また 5 は 0 を割り切る．つまり，$-2 \mid 4$ であり，$5 \mid 0$ である．

命題 [1]． $a, b, c \in \mathbb{Z}$ に対して，以下が成り立つ：
(1) $a \mid b$ かつ $a \mid c \Longrightarrow a \mid (b \pm c)$,　(2) $a \mid b \Rightarrow a \mid bc$,　(3) $a \mid b$ かつ $b \mid c \Longrightarrow a \mid c$,
(4) $a \mid b \iff -a \mid b$,　(5) $a \mid b$ かつ $b \mid a \iff a = \pm b$.

注意． 命題 [1](4) より，$b \in \mathbb{Z}$ の約数は正負がペアになって出てくる．そこで，b の約数 d といって (負の約数は考えず) **正の約数** $d > 0$ **のみを指す**ことが多い (← どちらなのか注意が必要)

定義 (最大公約数)． $a, b \in \mathbb{Z}$ に対して，$d \mid a$ かつ $d \mid b$ を満たす $d \in \mathbb{N}$ を a と b の**公約数** (common divisor)，a と b の公約数のうち最大のものを a と b の**最大公約数** (greatest common divisor) という．a と b の最大公約数を $\gcd(a, b)$ または単に (a, b) と表す．(← $d \in \mathbb{N}$ より $d > 0$ に注意する)

例 (最大公約数)． (i) $\gcd(-3, 6) = 3$, (ii) $\gcd(a, 0) = |a|$, $(\forall a \in \mathbb{Z})$, (iii) $\gcd(0, 0)$ は存在しない．

命題 [2](除法の原理)． $a, b \in \mathbb{Z}$, $b > 0$ に対して，

$$a = qb + r,\ 0 \leq r < b$$

を満たす整数の組 $(q, r) \in \mathbb{Z}^2$ がただ 1 組存在する．

∵ **(存在)** $a \in \mathbb{Z}$ に対して，$qb \leq a < (q+1)b$ なる $q \in \mathbb{Z}$ が存在する．そこで，$r := a - qb$ とすれば，$a = qb + r$ かつ $0 \leq r < b$ となる (← 各自確認する!).
(一意性) $a = q'b + r'$, $0 \leq r' < b$ とすれば，$a = qb + r = q'b + r'$ より，$(q - q')b = r' - r$ を得る．条件より，$-b < r - r' < b$ であるから，$-b < (q - q')b < b$ すなわち $-1 < q - q' < 1$ となり，$q = q'$ を得る．よって，$r = r'$ でもある．(← 各自確認する!)

命題 [3]． $a, b, q, r \in \mathbb{Z}$, $b > 0$ に対して，$a = qb + r \Longrightarrow \gcd(a, b) = \gcd(b, r)$.

∵ $g_1 := \gcd(a, b)$, $g_2 := \gcd(b, r)$ に対して，$g_1 \mid g_2$ かつ $g_2 \mid g_1$ を示せばよい (← $g_1, g_2 > 0$ と命題 [1] の (5) より)．いま，$a = g_1 a_1$, $b = g_1 b_1$, $b = g_2 b_2$, $r = g_2 r_2$ と書けるので，$a = qb + r = qg_2 b_2 + g_2 r_2 = (qb_2 + r_2)g_2$ から $g_2 \mid a$ であり，$g_2 \mid \gcd(a, b) = g_1$．また，$r = a - qb = g_1 a_1 - qg_1 b_1 = (a_1 - qb_1)g_1$ より $g_1 \mid r$ となり，$g_1 \mid \gcd(b, r) = g_2$．よって $g_1 \mid g_2$ かつ $g_2 \mid g_1$ より $g_1 = g_2$ である (← $g_1, g_2 > 0$)．

定義 (最小公倍数)． $a, b \in \mathbb{Z}$ に対して，$a \mid m$ かつ $b \mid m$ を満たす $m \in \mathbb{Z}$ を a と b の**公倍数** (common multiple)，a と b の公倍数のうち正であって最小のものを a と b の**最小公倍数** (least common multiple) という．a と b の最小公倍数を $\mathrm{lcm}(a, b)$ と書く．

例 (最小公倍数)． $a = 12 = 2^2 \cdot 3$, $b = 30 = 2 \cdot 3 \cdot 5$ に対して，
- $\mathrm{lcm}(a, b) = 2^2 \cdot 3 \cdot 5 = 60$,
- $\gcd(a, b) = 2 \cdot 3 = 6$,
- $ab = 360 = \mathrm{lcm}(a, b)\gcd(a, b)$.

命題 [4]． $a, b \in \mathbb{N}$ とする．(1) $a \mid m$ かつ $b \mid m \iff \mathrm{lcm}(a, b) \mid m$,　(2) $\mathrm{lcm}(a, b) = \dfrac{ab}{\gcd(a, b)}$.

[**証明**] $l := \mathrm{lcm}(a, b)$, $g := \gcd(a, b)$ と書く．(1)($\Longleftarrow$) は定義から従う．(1)($\Longrightarrow$) $a \mid m$ かつ $b \mid m$ を仮定し，m を l で割って $m = ql + r$, $0 \leq r < l$ とすれば，m と l が a, b の公倍数であることから，r も a, b の公倍数となる．しかし，l の最小性から $r = 0$ でなくてはならない．よって $l \mid m$.
(2) (1) で $m = ab$ とすれば，$l \mid ab$ であり，$ab = ld$, $d \in \mathbb{N}$ と表せる．よって，$ab = lg$ を示すには，$d \mid g$ かつ $g \mid d$ を示せばよい．$a = d(l/b)$, $b = d(l/a)$ から d は a, b の公約数であり，$d \mid g$ が成り立つ．また，$ab/g = a(b/g) = b(a/g)$ であるから，ab/g は a, b の公倍数であり，(1) より $l \mid (ab/g)$. いま，$l = ab/d$ であったから，$(ab/d) \mid (ab/g)$ となり，$g \mid d$ が得られる．よって，$d = g$ が成り立つ．　□

• 命題 [2] と命題 [3] を繰り返し用いれば，次の様に $\gcd(a,b)$ を非常に効率よく計算できる．

定理 5 (ユークリッドの互除法)． $a,b\in\mathbb{Z}$, $b>0$ に対して，

$$\begin{aligned} a &= q\cdot b + r_0, && 0\le r_0 < b,\\ b &= q_1\cdot r_0 + r_1, && 0\le r_1 < r,\\ r_0 &= q_2\cdot r_1 + r_2, && 0\le r_2 < r_1,\\ r_1 &= q_3\cdot r_2 + r_3, && 0\le r_3 < r_2,\\ &\vdots \end{aligned}$$

と繰り返していけば，$b>r_0>r_1>r_2>\cdots>r_n\ge 0$ より，ある $n\in\mathbb{N}$ で $r_n=0$ となる．

$$\begin{aligned} r_{n-4} &= q_{n-2}\cdot r_{n-3} + r_{n-2}, 0\le r_{n-2} < r_{n-3},\\ r_{n-3} &= q_{n-1}\cdot r_{n-2} + \mathbf{r}_{n-1}, 0\le \mathbf{r}_{n-1} < r_{n-2},\\ r_{n-2} &= q_n\cdot r_{n-1} + \mathbf{0}, \qquad r_n = \mathbf{0}. \end{aligned}$$

よって，$\gcd(a,b)=\gcd(b,r_0)=\gcd(r_0,r_1)=\cdots=\gcd(r_{n-2},r_{n-1})=\gcd(r_{n-1},0)=\mathbf{r}_{n-1}$ となる．

> $a,b\in\mathbb{Z}$ の素因数分解が分からないのに，$\gcd(a,b)$ が求まってしまった！

定理 6． 整数 $a,b\in\mathbb{Z}$ に対して，$d:=\gcd(a,b)\in\mathbb{N}$ とする．このとき，

$$sa+tb=d$$

を満たす整数 $s,t\in\mathbb{Z}$ が存在する．

∵ 上述のユークリッドの互除法を $a,b\in\mathbb{Z}$ に適用して，$d=r_{n-1}$ を得たとする．このとき，ユークリッドの互除法を逆にたどっていけば，$d=r_{n-1}$ は $r_{n-1}=r_{n-3}-q_{n-1}\cdot r_{n-2}$ として，r_{n-3} と r_{n-2} の一次結合で書け，$2\le i\le n$ に対しても r_{n-i} は $r_{n-(i+1)}$ と $r_{n-(i+2)}$ の一次結合で書ける．このように繰り返していけば，最終的には $d=r_{n-1}$ は a と b の一次結合で書ける：$d=sa+tb$ $(s,t\in\mathbb{Z})$.

定義 (互いに素)． 整数 $a,b\in\mathbb{Z}$ は $\gcd(a,b)=1$ のとき，**互いに素**である (relatively prime) という．

定理 [7] (互いに素な整数 a,b の特徴付け)． $a,b\in\mathbb{Z}$ に対して，

$$\gcd(a,b)=1\ (a\text{ と }b\text{ が互いに素}) \iff sa+tb=1 \text{ を満たす } s,t\in\mathbb{Z} \text{ が存在する.}$$

∵ ($\Longrightarrow$) 定理 6 ですでに示した．
($\Longleftarrow$) $d:=\gcd(a,b)$ は $sa+tb=1$ より，$d\,|\,1$ で $d=\pm1$ となるが，定義から $d>0$ であり，$d=1$.

系 [8]． $a,b,c\in\mathbb{Z}$, $a\neq 0$ に対して，$a\,|\,bc$ かつ $(a,b)=1\Longrightarrow a\,|\,c$.

∵ 仮定 $(a,b)=1$ と定理 [7] より，$sa+tb=1$ なる $s,t\in\mathbb{Z}$ が存在する．両辺を c 倍すれば，$acs+(bc)t=c$ であり，仮定 $a\,|\,bc$ より $a\,|\,c$ を得る．

定義 (素数)． 1 以外の自然数 $p\in\mathbb{N}$ の (正の) 約数が 1 と p 自身のみであるとき，p を**素数** (prime number) という．1 以外の素数でない自然数を**合成数** (composite number) という．

例 (素数，合成数)． $2,3,5,7,11,13,17,\ldots$ は素数．$4,6,8,9,10,12,14,15,16,18,20,\ldots$ は合成数．

系 [9](素数の基本性質)． p を素数とする．
(1) $p\,|\,ab\Longrightarrow p\,|\,a$ または $p\,|\,b$.
(2) $p\,|\,a_1\cdots a_r\Longrightarrow p$ はいずれかの a_i, $1\le i\le r$ を割り切る．

∵ (1) p は素数であるから，$p\not|\,a$ の場合には $(p,a)=1$ となる．よって，系 [8] より $p\,|\,b$ を得る．
(2) (1) を $a_1(a_2\cdots a_r)$ に用いて，これを繰り返していけばよい ($\leftarrow$ 厳密には数学的帰納法を用いる)．

定理 [10](素因数分解の一意性). (1 以外の) 任意の自然数 $n \in \mathbb{N} \setminus \{1\}$ は素数の積に分解し，その表示は積の順序を除いて一意的である．(← 「順序を除いて一意的」は教科書 p.38 を参照)

☹ **(分解可能)** n が素数でなければ，n には $n = ab,\ 1 < a, b < n$ なる約数 a, b が存在する．これを繰り返せば，素数でない約数は (単調減少に) それより小さな約数の積に分解する．この分解は止まらなくてはならないので，最後には素数の積となる．
(一意性) $n = p_1 \cdots p_s = q_1 \cdots q_t,\ s \leq t$ と 2 通りの素数の積に書けたとする (各 p_i, q_j には重複があってよい)．このとき，p_1 は系 [9] より $q_1, \ldots, q_t$ のうちの 1 つ q_k を割り切る．しかし，各 q_j は素数であるから $p_1 = q_k$ となる．ここで，番号を付け替えて，$q_1 := q_k$ とする．いま，$p_2 \cdots p_s = q_2 \cdots q_t$ であるから，この議論を繰り返して，q_j の番号を付け替えれば $p_2 = q_2$ とできる．これを残りの $p_3, \ldots, p_s$ に対しても繰り返せば，$s = t$ かつ $p_i = p_j,\ 1 \leq i, j \leq s$ を得る．

素因数分解の一意性はいかにも当たり前のように見える．しかし，実は**整数論** (代数) では，その名前とは反して，整数の世界 (集合) $\mathbb{Z}$ をより大きな世界 (集合)，例えば，

$$\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \,|\, a, b \in \mathbb{Z}\}$$

に広げて考える必要がでてくる．さらに，集合 $\mathbb{Z}[\sqrt{-5}]$ は**代数体**

$$\mathbb{Q}(\sqrt{-5}) := \{a + b\sqrt{-5} \,|\, a, b \in \mathbb{Q}\} \quad (\leftarrow \text{実際に体の定義を満たしている!})$$

の部分集合であって，整数論では $\mathbb{Z}[\sqrt{-5}]$ は**代数体** $\mathbb{Q}(\sqrt{-5})$ の**整数環** (← 実際に環の定義を満たしている!)，$\mathbb{Z}[\sqrt{-5}]$ の元 (要素) は単に**整数**と呼ばれる．つまり (整数論では) $1 + 2\sqrt{-5}$ は**整数**と呼ばれる (!)．この世界 (環) $\mathbb{Z}[\sqrt{-5}]$ の元 (整数) に対して，素数にあたるものを定義して同様のことを考えると，素因数分解の一意性は成り立たなくなる．例えば，

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}) = (4 + \sqrt{-5})(4 - \sqrt{-5})$$

であり，それぞれの因子 (約数) は $\mathbb{Z}[\sqrt{-5}]$ の元の積には分解できない．(← この世界の素数)

フェルマー (Fermat, 1601–1665) の平方和定理. 奇数の素数 p に対して，

$$p \text{ は } 4m + 1 \text{ の形} \iff p = s^2 + t^2 \text{ と 2 つの整数の平方和で表される.}$$

(証明を最初に公表したのは**オイラー (Euler, 1707–1783)**, 参考文献 [7] (第 II 章, §VIII))
例えば，$5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$, $29 = 2^2 + 5^2$, $37 = 1^2 + 6^2$, $41 = 4^2 + 5^2$.
これは，$p = 4m + 1$ の形の素数は，整数の世界 (集合)$\mathbb{Z}$ を $\mathbb{Z}[\sqrt{-1}] := \{a + b\sqrt{-1} \,|\, a, b \in \mathbb{Z}\}$ に拡張すると，$p = (s + t\sqrt{-1})(s - t\sqrt{-1})$ と分解して，(この世界の) **素数ではなくなってしまう**ことを表している．一方，$p = 4m + 3$ は $\mathbb{Z}[\sqrt{-1}]$ でも素数である．

クンマー (Kummer, 1810–1893) が正則素数と呼ばれる素数 (例えば，100 以下の素数では 37, 59, 67 の 3 つ以外の全ての素数) について，フェルマーの最終定理を解決したことは授業中に紹介した．クンマーは上述の「素因数分解の一意性」が成り立たないことを解消するために，**(素) イデアル**「理想数」の概念を導入して，成果を得た．

高木貞治 (1875–1960) による**類体論** (Class Field Theory) は，(上述のフェルマーの平方和定理の拡張ともみなせる) 非常に美しい理論で，アーベル体 (代数体) という世界 (集合) では素数 p がどのように分解するかを記述している．また，ワイルスによるフェルマーの最終定理の証明では，**岩澤健吉 (1917–1998)** による**岩澤理論** (Iwasawa Theory) が活躍している．

• ベルヌーイ数 $B_0, B_1, \ldots, B_{15}$ の表は p.17 (第 6 回) にある．実は，次のような事が知られている (← もちろんこの授業では解説できない)：

(known) Fact 1. s 乗和の公式は，一般にベルヌーイ数 B_j を用いて次のように書ける：

$$F_s(n) = \sum_{k=1}^{n} k^s = \sum_{j=0}^{s} \binom{s}{j} B_j \frac{n^{s+1-j}}{s+1-j}.$$

(known) Fact 2. ベルヌーイ数 B_n は次のべき級数展開の係数に現れる有理数である：

$$\frac{te^t}{e^t-1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

定義 (正則素数). 素数 p は，ベルヌーイ数 B_k, $(k = 2, 4, 6, \ldots, p-3)$ の分子を割り切らないとき，**正則素数** (regular prime) と呼ばれる．正則素数でない素数を**非正則素数** (irregular prime) という．(← ある k, $(2 \leq k \leq p-3)$ に対して，p が B_k の分子の約数になるとき)

定理 (Kummer, 1847). p が正則素数 $\Longrightarrow x^p + y^p = z^p$ を満たす $x, y, z \in \mathbb{N}$ は存在しない．

例 (非正則素数).
• (p. 17 の表を求めてみると) $B_{12} = -\frac{691}{2730}$ である．よって，素数 691 は**非正則素数**である．
• 100 以下の素数では，37, 59, 67 の 3 つだけが非正則であることが知られている．
• 100 以下の素数だけをみると，**ほとんど全ての素数は正則素数なのではないか**と思ってしまうが，正則素数が無限にあるかは知られていない．(← それどころか $\cdots$)
• 岩澤理論の入門書である参考文献 [8](p.410) には 4001 以下の非正則素数の Table がある．例えば，691 以下の非正則素数は：$p = 37, 59, 67, 101, 103, 131, 149, 157, 233, 257, 263, 271, 283, 293, 307, 311, 347, 353, 379, 389, 401, 409, 421, 433, 461, 463, 467, 491, 523, 541, 547, 557, 577, 587, 593, 607, 613, 617, 619, 631, 647, 653, 659, 673, 677, 683, 691,$ によって与えられる．

(known) Fact 3. 非正則素数は無限に存在する．(← クンマーの定理が適用できない!)
(← ある代数体で素因数分解が一意的に出来ないことが深く関わっている (参考文献 [8]))

演習問題 (期末テストの予想問題)

• 命題 [1], [2], [3], [4], 定理 [7], 系 [8], [9], 定理 [10] を示せ．

• 次の $(a, b) \in \mathbb{N}^2$ に対して，$\gcd(a, b)$ の値と $sa + tb = \gcd(a, b)$ を満たす整数 $s, t \in \mathbb{Z}$ を求めよ．
(i) $(102, 114)$, (ii) $(330, 858)$, (iii) $(434, 465)$, (iv) $(1785, 1859)$, (v) $(510510, 519593)$.

参考文献

[1] 初等的数論の代数—ホモモーフィズムに学ぶ, 近藤庄一 (著), 293 ページ, サイエンティスト社 (1996), 3262 円.

[2] 初等整数論, 講座 数学の考え方 ⟨16⟩, 木田祐司 (著), 218 ページ, 朝倉書店 (2001), 3990 円.

[3] 代数と数論の基礎 (共立講座 21 世紀の数学), 中島匠一 (著), 296 ページ, 共立出版 (2000), 3990 円.

[4] 群・環・体入門, 新妻弘, 木村哲三 (著), 291 ページ, 共立出版 (1999), 3465 円.

[5] 演習 群・環・体入門, 新妻弘 (著), 243 ページ, 共立出版 (2000), 3045 円.

[6] 暗号の整数論—素数研究が生きるセキュリティ技術 (現代技術への数学入門シリーズ), 境隆一, 金子昌信 (著), 若山正人 (編集), 56 ページ, 講談社 (2009), 1680 円.

[7] 数論—歴史からのアプローチ, アンドレ ヴェイユ (著), 足立恒雄, 三宅克哉 (翻訳), 386 ページ, 日本評論社 (1987), 7875 円.

[8] Introduction to Cyclotomic Fields (GTM83) (洋書), L.C.Washington(著), 487 ページ, Springer-Verlag.

これまでの授業の補足

完全数, 友愛数 (p.17)

$(220, 284)$ が**友愛数**であることは，次のように確かめられる：

220 の約数の和：$1+2+4+5+10+11+20+22+44+55+110=284$
$220=1+2+4+71+142$：284 の約数の和

$6, 28, 496$ が**完全数**であることは，次のように確かめられる：

$6=1+2+3$,
$28=1+2+4+7+14$,
$496=1+2+4+8+16+31+62+124+248$

定理 (ユークリッド)
2^n-1 が素数 $\Longrightarrow 2^{n-1}(2^n-1)$ は完全数 (偶数).

定理 (オイラー)
偶数の完全数は $2^{n-1}(2^n-1)$ の形の数に限られる.

2^n-1 の形の素数を**メルセンヌ素数**という.

上の定理から，偶数の完全数を見つけるにはメルセンヌ素数を見つければよい．例えば,

$2^7-1=127$ はメルセンヌ素数 $\Longrightarrow 2^6(2^7-1)=64\times 127=8128$ は完全数.

この調子でいくらでも完全数を見つけられる気がするが，なかなかそうはいかない．実際，この次に小さい完全数は，33550336, 8589869056 であることが知られている．それどころか，メルセンヌ素数や完全数が無限に存在するかは現在でも分かっていない，**未解決問題**である．現在知られているメルセンヌ素数，完全数 (偶数) は 47 個だけであり，奇数の完全数は 1 つも発見されていない．(47 個目のメルセンヌ素数 $2^{42643801}-1$ は 2009 年 4 月に発見された．ちなみに，2008 年 8 月の UCLA のコンピュータによる 45 個目の $2^{43112609}-1$ の発見は，**1000 万桁**を超す人類初めての素数の発見であったので，**10 万ドル**の賞金が与えられた．)

奇数の完全数については，**もし存在すれば** 10^{300} より大きいこと，また 2008 年には Goto-Ohno (2 人の日本人数学者) によって，10^8 より大きい素因数をもつことが示されている.

ちなみに，$2^{2^n}+1$ の形の素数を**フェルマー素数**という.

$2^1+1=3,\ 2^2+1=5,\ 2^4+1=17,\ 2^8+1=257,\ 2^{16}+1=65537$

は全て素数であり，このまま素数が生み出されるように思ってしまうが，**オイラー** (1707–1783) は 1732 年に $2^{32}+1=4294967297=641\times 6700417$ であることを証明した．それどころか，今日現在まで，上記の 4 つ以外のフェルマー素数が存在するかは**未解決問題**である.

フェルマー予想とオイラー予想

フェルマーの最終定理 (フェルマー予想) $x^n+y^n=z^n$ を拡張した次のような予想があった：

予想 (オイラー, 1769)
$x^4+y^4+z^4=w^4$ を満たす $x, y, z, w\in\mathbb{N}$ は存在しない.

確かに，どこまでやっても $x, y, z, w\in\mathbb{N}$ を見つけることが出来ない．しかし，見つからないからと言って，証明にはならないので，その難しさはフェルマーの最終定理と同じような気がする．しかし，Elkies は 1988 年に**楕円曲線**の理論を使って，次の様な反例を与え，更にはその解が無限に存在することを示してしまった：

$2682440^4+15365639^4+18796760^4=20615673^4$,

$95800^4+217519^4+414560^4=422481^4$.

一度見つかってしまえば，**確かめる事は出来る**．(が，やってみると大変なことも分かる．)

リーマンゼータ関数とリーマン予想

実数列 $\{a_k\}_{k\in\mathbb{N}}$, $a_k=\sum_{n=1}^{k}\frac{1}{n^s}$ は，$s=2,3,4,\ldots$ に対して，**単調増加かつ上に有界**であり

($\leftarrow$ 各自示す!)，**収束する**．その収束先 $\zeta(s)=\lim_{k\to\infty}\sum_{n=1}^{k}\frac{1}{n^s}$ は以下のように求められる：

$\zeta(2)=1.64493406684822643647241516664602518921894990120679843773555822937000 7\cdots$
$\zeta(3)=1.20205690315959428539973816151144999076498629234049888179227155534183 8\cdots$
$\zeta(4)=1.08232323371113819151600369654116790277475095191872690768297621544412 0\cdots$
$\zeta(5)=1.03692775514336992633136548645703416805708091950191281197419267790380 3\cdots$
$\zeta(6)=1.01734306198444913971451792979092052790181749003285356184240866400433 2\cdots$
$\zeta(7)=1.00834927738192282683979754984979675959986356056523870641728313657160 1\cdots$
$\zeta(8)=1.00407735619794433937868523850865246525896079064985002032911020265258 3\cdots$
$\zeta(9)=1.00200839282608221441785276923241206048560585139488875654859661590978 5\cdots$
$\zeta(10)=1.00099457512781808533714595890031901700601953156447751725778899463629 1\cdots$
$\zeta(11)=1.00049418860411946455870228252646993646860643575820861711914143610005 4\cdots$
$\zeta(12)=1.00024608655330804829863799804773967096041608845800340453304095213325 2\cdots$

特に，$\zeta(2)$ がどのような数かは**バーゼル問題** (1644) と呼ばれて長年未解決であった．

定理 (オイラー)

B_n をベルヌーイ数として，$\zeta(2n)=\frac{(-1)^{n-1}}{2}\frac{(2\pi)^{2n}}{(2n)!}B_{2n}$.

例えば,
$\zeta(2)=\frac{\pi^2}{6}$, $\zeta(4)=\frac{\pi^4}{90}$, $\zeta(6)=\frac{\pi^6}{945}$, $\zeta(8)=\frac{\pi^8}{9450}$, $\zeta(10)=\frac{\pi^{10}}{93555}$, $\zeta(12)=\frac{691\pi^{12}}{638512875},\ldots$
しかし，奇数に対しては $\zeta(2n+1)$ の値はほとんどよく分かっていない．

定理 (Apéry, 1979)

$\zeta(3)\notin\mathbb{Q}$. ($\leftarrow$ すなわち，$\zeta(3)$ は無理数 (有理数ではない)).

定理 (Zudilin, 2001)

$\zeta(5),\zeta(7),\zeta(9),\zeta(11)$ のうち，少なくとも 1 つは無理数．($\leftarrow$ しかし，どれかは分からない．)

$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}$ は**リーマンゼータ関数**と呼ばれており，**有名なリーマン予想**は $\zeta(s)$ の零点 (0 になる s の値) に関する予想である．しかし，ここで言う関数とは**複素関数**のことであり，$s\in\mathbb{C}$ である．これを理解するには，大学で**複素関数論**の授業を受け，**解析接続**を学ばないと，その意味すらよく分からない．

解析接続によって，$s\in\mathbb{C}$ $(s\neq 1)$ に対して定義された $\zeta(s)$ の値として，例えば，負の整数点，すなわち $\zeta(-1),\zeta(-2),\ldots$ には再びベルヌーイ数が現れる：

定理

B_n をベルヌーイ数として，$\zeta(-n)=-\frac{B_{n+1}}{n+1}$.

また p.15 で出てきた **Dirichlet の算術級数中の素数定理**を示すには，リーマンゼータ関数の拡張である**ディリクレの L 関数** $L(s,\chi):=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$ が用いられ，但し，χ は Dirichlet 指標，その証明は $s=1$ の値が 0 にならないこと，$L(1,\chi)\neq 0$, $(\chi\neq\mathbf{1})$，に基づいている．