

B2 代数計算

【整式】

整式 $P = 6x^3 - 7x^2 + 5x + 2$ と $Q = 2x^2 - 3x + 2$ について

P を Q で割った商と余りを求めよ。

整式 $P = x^3 - 2x^2 - x + 2$ と $Q = x^3 - 2x^2 + x - 2$ について

P と Q の GCD と LCM を求めよ。

【有理式】

次の分数式から分子・分母を取り出すこと。

$$\frac{x^2 + x + 1}{x^3 + x^2 + x + 1}$$

次を通分せよ。

$$\frac{1}{a+1} + \frac{1}{a+2} + \frac{1}{a+3}$$

分母は ExpandDenominator で展開せよ。

次を部分分数へ分解せよ。

$$\frac{1}{x^2 - 9}$$

$$\frac{x^2 + x + 1}{(x+1)(x^2+1)^2}$$

【展開】

次を展開せよ。

$$(x+y)(x-y)$$

$$(x+y+z)^2$$

$$(x-2y+3z)^3$$

次を展開し、() 内に指定した文字で整理すること。

$$(x-2y+3z)^8 \quad (x)$$

$$(x-2y+3z)^8 \quad (y)$$

$$(x-2y+3z)^8 \quad (z)$$

項を並べかえて、降幂の順にせよ。

$$x + x^2 - x^3 + 1 - x^4$$

$$1 + x + y + xy + x^2y + x^2y^3 - 3xy^4 + 2x^2y^2 - 4xy^3$$

【因数分解】

次を因数分解せよ。(整数の範囲で)

$$x^6 - x^5 - 9x^4 + x^3 + 20x^2 + 12x$$

$$x^3 + y^3 + z^3 - 3xyz$$

$$u^{10} - v^{10}$$

実数の範囲で因数分解せよ。

$$x^2 - 2 \quad x^2 - 2y^2 \quad x^4 + 1$$

複素数の範囲で因数分解せよ。

$$x^2 + 2 \quad x^3 + 1 \quad x^4 - 1$$

【 $t^n - 1$ の因数分解】 起源は R, Cotes ャツ 1682-1716

$t^n - 1$ を因数分解して、既約因子の係数を調べよ。

$t^{105} - 1, t^{165} - 1$ では係数に $-2, 2$ が現れる

$t^{385} - 1, t^{595} - 1$ では係数に $-3, 3$ が現れる

$t^{7917} - 1, t^{8645} - 1$ では $\{-9, -8, \dots, -2, -1, 1, 2, \dots, 8, 9\}$ が現れる。

プログラム例

```
ff=FactorList[x^105 - 1]
ll = Length[ff]
aa = {};
For[i = 1, i <= ll, i = i + 1,
aa = Append[aa, CoefficientList[ff[[i]], [[1]], x]]];
aa
bb = Flatten[aa]
cc = Union[bb]
```

【円周等分多項式】

単位円を等分した多項式 $C_n(x) = \prod_k (x - e^{\frac{2\pi i k}{n}})$

ただし、 k は n より小さく n と互いに素な正整数をわたる
は、Cyclotomic[n,x] で得られる。

Cyclotomic[6,x] = $x^2 - x + 1$ である。これは

Factor[x^6-1] = $(x-1)(x+1)(x^2-x+1)(x^2+x+1)$ の因数である。

【ルジャンドル多項式】

ルジャンドル多項式 $P_n(x)$ は n 次の多項式であり、LegendreP[n,x] で得られる。

例えば、 $P_0(x) = 1$, $P_1(x) = x$, $P_2(x) = \frac{3}{2}x^2 - \frac{1}{2}$, $P_3(x) = \frac{5}{2}x^3 - \frac{3}{2}x$ である。

与えられた n に対して、 x^n を $P_0(x), P_1(x), \dots, P_n(x)$ の一次結合で表すこと。

【ベルヌーイ数とベルヌーイ多項式】

ベルヌーイ数 B_n は関数 $f(t) = \frac{t}{e^t - 1}$ のマクローリン展開式の係数として

$$\frac{t}{e^t - 1} = B_0 + B_1 \frac{t}{1!} + B_2 \frac{t^2}{2!} + \cdots + B_n \frac{t^n}{n!} + \cdots$$

で定義される。

ベルヌーイ多項式 $B_n(x)$ は関数 $f(t) = t \frac{e^{tx}}{e^t - 1}$ のマクローリン展開式の係数として

$$t \frac{e^{tx}}{e^t - 1} = B_0(x) + B_1(x) \frac{t}{1!} + B_2(x) \frac{t^2}{2!} + \cdots + B_n(x) \frac{t^n}{n!} + \cdots$$

で定義される。

これらは `BernoulliB[n]` や `BernoulliB[n,x]` で求まる。

ベルヌーイ数・多項式が現れる例

$$1^n + 2^n + \cdots + k^n = \frac{B_{n+1}(k+1) - B_{n+1}(1)}{n+1}$$

$$\tan x = \sum_{n=1}^{\infty} \frac{2^{2n} (2^{2n} - 1) |B_{2n}|}{2n} \frac{x^{2n-1}}{(2n-1)!} \quad (\text{マクローリン展開の係数として})$$

$$B_n(x+1) - B_n(x) = nx^{n-1}$$

【ゼータ関数】

リーマンのゼータ（ツェータ）関数は複素数 $s = a + bI$ に対してゼータ級数

$$\zeta(s) = 1 + \frac{1}{1^s} + \frac{1}{2^s} + \cdots + \frac{1}{n^s} + \cdots$$

として定義される。 $\operatorname{Re}(s) = a > 1$ のときのみ収束する。しかしこの

関数は（特異点 $s = 1$ を除いて）全複素平面に解析接続できる。

これは `Zeta[s]` で求められる。特に s が偶数 $2n$ のときは

$$\zeta(2n) = \frac{(2\pi)^{2n}}{2(2n)!} |B_{2n}| \quad (\text{オイラー})$$

である。例えば $\zeta(2) = \frac{\pi^2}{6}$, $\zeta(4) = \frac{\pi^4}{90}$, $\zeta(6) = \frac{\pi^6}{945}$ である。

`Zeta[I]/N` により $0.00330022 - 0.418155I$ と表示される。

関数 `Zeta[n]` のグラフを n の範囲 $[-10, 10]$ あるいは $[-20, 0]$ で描いてみると、 $\zeta(-2n) = 0$ ($n = 1, 2, 3, \dots$) が分かる。これらは、ゼータ関数の自明な零点と呼ばれている。

他にも零点があって、その正確な位置が、未解決問題のリーマン予想

「すべての自明でないゼータ関数の零点の実部は $1/2$ 」

である。

この予想を理解するには、実数値関数 $f(x, y) = |\zeta(x + yi)|$ あるいは

$f(x, y) = \frac{1}{|\zeta(x + yi)|}$ のグラフを $-4 \leq x \leq 4$, $-10 \leq y \leq 40$ の範囲で描いてみ

るとよい。 $\zeta(x+yi)$ が0に近いとき、 $f(x,y) = \frac{1}{|\zeta(x+yi)|}$ は大きい。

【グレブナ基底】

K は $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ のいずれかの体とする。 K 上の n 変数の多項式全体のなす環 $K[X_1, X_2, \dots, X_n]$ における割算を考える。

$K[X_1, X_2, \dots, X_n]$ の集合 G で生成したイデアルを $\langle G \rangle$ で表わす。

非負の n 個の整数の集合 $Z_{\geq 0}^n = \{(\alpha_1, \alpha_2, \dots, \alpha_n) \mid \alpha_1, \alpha_2, \dots, \alpha_n \in Z_{\geq 0}\}$ に辞書式順序を付ける。例えば $n=3$ では

$$(2, 3, 1) > (2, 3, 0) > (2, 2, 5) > (1, 2, 6) > (0, 0, 0) \text{ 等}$$

$\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ に対して単項式 $X^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \dots X_n^{\alpha_n}$ を対応させる。

$K[X_1, X_2, \dots, X_n]$ の元は $f = \sum_{\alpha} a_{\alpha} X^{\alpha}$ の形をしている。 $a_{\alpha} \neq 0$ であるような

α のうち、辞書式順序で最大なものを f の multidegree と呼び、

$\alpha = \text{multideg}(f)$ で表わす。 $a_{\text{multideg}(f)}$ を leading coefficient と呼び、

$LC(f)$ で表わす。 $X^{\text{multideg}(f)}$ を leading monomial といい、 $LM(f)$ で表わす。

最後に $LC(f)LM(f)$ を leading term といい、 $LT(f)$ で表わす。

多項式 f を多項式の集合 $\{f_1, f_2, \dots, f_s\}$ で割るとは、

$$f = a_1 f_1 + a_2 f_2 + \dots + a_s f_s + r \quad (a_1, a_2, \dots, a_s, r \text{ は多項式})$$

で、 $LM(f_1), LM(f_2), \dots, LM(f_s)$ のどれも r に現れるどの単項式も割り

切らないものを見つける」ことである。

ここで、常に $a_1, a_2, \dots, a_s, r$ を見つけることができるが、一意的とは限らない。

例 $f = X^2 Y + X Y^2 + Y^2$, $f_1 = X Y - 1$, $f_2 = Y^2 - 1$ のとき

$$f = (X+Y) \cdot f_1 + 1 \cdot f_2 + (X+Y+1) = (X+1) \cdot f_2 + X \cdot f_1 + (2X+1)$$

このような商と余りは PolynomialReduce によりリストで得られる。

```
PolynomialReduce[x^2 y+x y^2+y^2, {x y-1,y^2-1},{x,y}]
```

```
PolynomialReduce[x^2 y+x y^2+y^2, {y^2-1,x y-1},{x,y}]
```

ヒルベルトの基底定理より、 $K[X_1, X_2, \dots, X_n]$ のイデアル $I \neq 0$ について、

$$\langle LM(I) \rangle = \langle LM(f) \mid f \in I \rangle = \langle LM(f_1), LM(f_2), \dots, LM(f_s) \rangle$$

となる I の元の集合 $\{f_1, f_2, \dots, f_s\}$ がある。これを I のグレブナ基底という。

イデアル $I \neq 0$ のグレブナ基底は I の生成元である。

任意の $g \in K[X_1, X_2, \dots, X_n]$ をグレブナ基底 $\{f_1, f_2, \dots, f_s\}$ で割って

$$g = a_1 f_1 + a_2 f_2 + \dots + a_s f_s + r$$

と表わすとき、余り r は一意的である。

イデアル I のグレブナ基底 $\{f_1, f_2, \dots, f_s\}$ が被約(reduced) であるとは、

$LC(f_1) = LC(f_2) = \dots = LC(f_s) = 1$ かつ、異なる i, j について $LM(f_i)$ は f_j に現れるどの単項式も割り切らぬこととする。

イデアル $I \neq 0$ の被約グレブナ基底は常に存在して、一意的である。

GroebnerBasis[{poly1,poly2,...},{x1,x2,...}]

$x_1, x_2, \dots$ の多項式 $\text{poly1}, \text{poly2}, \dots$ のグレブナ基底を探す。

GroebnerBasis[{poly1,poly2,...},{x1,x2,...}, {y1,y2,...}]

$y_1, y_2, \dots$ を消去して、グレブナ基底を探す。

次のイデアルのグレブナ基底を求めよ。

$\langle \{3x - 6y - 2z, 2x - 4y + 4z, x - 2y - z - w\} \rangle$ $\mathbb{Q}[x, y, z, w]$ のイデアル

$\langle \{x - t^2 - t^4, y - t^3 - t^5\} \rangle$ $\mathbb{Q}[x, y, t]$ のイデアル

$\langle \{x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1\} \rangle$

$\langle \{x^2 + y + z - 1, x + y^2 + z - 2, x + y + z^2 - 3\} \rangle$

【素数を法とする多項式】

素数 p を法とする整数のなす有限体 $Z_p = \mathbb{Z}/(p)$ の要素を係数とする多項式を扱う。

PolynomialMod[poly,p] poly の係数を mod p で簡略化する。

Expand[poly,Modulus->p] mod p で poly を展開する。

Factor[poly,Modulus->p] mod p で poly を因数分解する。

PolynomialGCD[poly1,poly2,Modulus->p]

mod p で $\text{poly1}, \text{poly2}$ の最大公約式を探す。

GroebnerBasis[polys,vars,Modulus->p]

mod p で polys のグレブナ基底を探す。

$Z_2[x]$ の多項式 $f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ を $g(x) = x^2 + 1$ で割った商と余りを求めよ。

$Z_{13}[x]$ の多項式 $f(x) = 9x^6 + 4x^5 - 5x^3 - 3x^2 + x + 6$ を $g(x) = x + 4$ で割った商と余りを求めよ。

$Z_2[x]$ の多項式 $f(x) = x^4 + x^3 + 1$ と $g(x) = x^2 + x + 1$ の最大公約多項式を求めよ。

$Z_3[x]$ の多項式 $f(x) = 2x^4 + 2x^3 + x^2 + x$ と $g(x) = 2x^3 + x^2 + 2x + 1$ の最大公約多項式を求めよ。

$Z_7[x]$ において $f(x) = x^4 - 3x^2 + 2x + 1$ が既約であるか否か判定し、可約なときは、既約な多項式の積で表せ。

Z_2 上の 4 次以下の既約多項式をすべて求めよ。

Z_{31} 上の多項式 $x^5 - 1$ を既約分解せよ。

参考書

- | | | | | |
|----------------------|--------|--------|------------|------|
| 情報の数理 | 応用代数学 | 平松豊一 | 裳華房 | 1997 |
| 21 世紀の数学 | 環と体の理論 | 酒井文雄 | 共立出版 | 1997 |
| Mathematica で見える現代数学 | ワゴン・長岡 | ブレイン図書 | | 1992 |
| グレブナ基底 | 丸山正樹 | 数学通信 | 第 3 巻第 3 号 | 1998 |
| パワーアップ離散数学 | 大山達雄 | 共立出版 | | 1997 |