入学年度		学部	学科		組		番号			検	フリガナ	
		D		1							氏名	

有限体 $\mathbb{F}_8$ は $\mathbb{F}_2$ に $\alpha^3+\alpha+1=0$ をみたす数 α を加えて得られる数の体系であった．$\mathbb{F}_8$ の元はすべて α の2次以下の多項式として表され（**加法表示**），0を除く7個の元は α^k（$0 \leqq k \leqq 6$）と表せる（**乗法表示**）．α の多項式 $P(\alpha)$ を3次以下の式に直すことは，$P(\alpha)$ を $\alpha^3+\alpha+1$ で割った余りを求めることに他ならない．これをMathematica™を用いて計算してみよう．基本は多項式の割り算である**PolynomialMod**を用いればよいが，ここでは $1+1=0$ という計算ルールのもとで計算することも勘定に入れなければならない．例えば α^7 を α の3次以下の式に直すには，次のようにする．（α をMathematica™で入力するのが面倒であれば a を用いてもよい．）

```
PolynomialMod[α^7,α^4 + α + 1,Modulus -> 2] ⇧+↵
```

（⇧+↵ はShiftキーとEnterキーを同時に押し，コマンドを実行することを意味する．）

k をいろいろ変えて，α^k を一度に計算するには **Table** コマンドを使うとよい．このコマンドについての詳しい説明は，Mathematica のヘルプと次のサイトを参照のこと．

https://www1.econ.hit-u.ac.jp/kawahira/courses/mathematica/03.pdf

まず，次のようにすると結果が1行になって出てくる．

```
Table[PolynomialMod[α^k, α^3 + α + 1, Modulus -> 2], {k, 0, 7}] ⇧+↵
```

ここで，**TableForm** というコマンドを使うと，結果が縦書きになり、見やすくなる．

```
Table[
  PolynomialMod[α^k, α^3 + α + 1, Modulus -> 2], {k, 0, 7}] //TableForm ⇧+↵
```

さらに，次のようにすると，α^k とその計算結果を並べて表示できる．

```
Table[
  {α^k,PolynomialMod[α^k, α^3 + α + 1, Modulus -> 2]},
  {k, 0, 7}] //TableForm  ⇧+↵
```

1 有限体 $\mathbb{F}_{16}$ は $\mathbb{F}_2$ に $\beta^4+\beta+1=0$ をみたす数 β を加えて得られる．$\mathbb{F}_{16}$ の元はすべて β の3次以下の多項式として表される．上の計算を真似して，$k=0,1,2,\ldots,15$ について β^k を β の3次以下の多項式として表示する表を作れ．

Mathematica™ には有限体の計算を実行できる “Finite Fields” というパッケージが含まれている．これを用いると問題1の表が簡単に作れる．

```
<< FiniteFields` ⇧+↵

F16 = GF[2, {1, 1, 0, 0, 1}]; ⇧+↵

Table[{k, β^k,
   ElementToPolynomial[Power[F16[{0, 1, 0, 0}], k], β] // TraditionalForm,
   BaseForm[
    ElementToPolynomial[Power[F16[{0, 1, 0, 0}], k], β]
    /. β -> 2, 2],
   ElementToPolynomial[Power[F16[{0, 1, 0, 0}], k], β]
   /. β -> 2},
  {k, 1, 15}] // TableForm ⇧+↵
```

ここで，Mathematica™ では多項式を昇べきの順に表示するのが標準となっていることに注意しておく．すなわち，$\beta^4+\beta+1$ はMathematica™では $1+\beta+\beta^4$ と表示される．上の `GF[2, {1, 1, 0, 0, 1}]` の中の{1, 1, 0, 0, 1}はこのMathematica™の慣習を反映して $1+\beta+\beta^4$ を表している．また，`TraditionalForm` と指定することにより，多項式を見慣れた降べきの順に表すこともできる．

上の式で得られた結果の第3列目は β の3次以下の式の係数を並べて得た数を2進法表示した整数とみなしたものである．例えば，β^2+1 は $\beta^2+0\cdot b+1$ とみて101とし，それを2進法表示した整数 101_2 とみたものである．そして，第4列目はその整数を10進表示に直したものである．

2 QRコードなどの実用上は $2^8=256$ 個の元を持つ有限体 $\mathbb{F}_{256}$ が使われることが多い．$\mathbb{F}_{256}$ は $\mathbb{F}_2$ に $\gamma^8+\gamma^4+\gamma^3+\gamma^2+1=0$ をみたす数 γ を加えて得られる．$\mathbb{F}_{256}$ の元はすべて γ の7次以下の多項式として表される．上の計算を真似して，$k=1,2,\ldots,255$ について γ^k を β の7次以下の多項式として表示する表を作れ．

• BCH符号

次に，前回に扱った，ハミング符号を $\mathbb{F}_2$ 上の多項式を用いて再構成してできた符号は一般にBCH符号と呼ばれるものである．これについては次回以降詳しく説明するが，まず前回現れたの符号多項式をMathematica™で計算してみる．

まず，$(7,4)$ 型のハミング符号では，情報語は4bitであり，0から15までの数を2進法表示した0000から1111までの16語である．まず，これらをベクトルとみる．たとえば，5は2進法表示すると0101となるので，これをベクトル $(0,1,0,1)$ と同一視する．さらに，これとベクトル $(x^3,x^2,x,1)$ の内積をとると，

$$(0,1,0,1)\cdot(x^3,x^2,x,1)=0\cdot x^3+1\cdot x^2+0\cdot x+1\cdot 1=x^2+1$$

となる．

【裏に続く】

まず，0 から 15 までの数 n を 4 桁の 2 進法表示し，それを 4 次元ベクトルにする関数 f を定義する．

```
f[n_] := (
  n1 = n;
  vect = {};
  While[n1 > 0,
   vect = Prepend[vect, Mod[n1, 2]];
   n1 = Quotient[n1, 2]];
  Return[PadLeft[vect, 4]];
  )  ⇧+↵
```

ここで例えば，

```
f[5].Table[x^(3 - k), {k, 0, 3}] ⇧+↵
```

とすると，$1 + x^2$ という答えが出るはずである．（表示の順序は昇べきの順になってしまう．）

情報語から符号語を作る方法を思い出したみと，多項式 $q(x)$ に対して $u(x)$ を

$$u(x) = (q(x))x^3 + \left(q(x)x^3 \text{ を } x^3 + x + 1 \text{ で割った余り} \right)$$

と定義するのであった．Mathemtica™ を用いて上で得た $1 + x^2$ から符号語を作るには，

```
Expand[(1 + x^2)*x^3] + PolynomialMod[(1 + x^2)*x^3, x^3 + x + 1,
  Modulus -> 2]
```

とすればよい．$x^2 + x^3 + x^5$ という答えが得られるはずである．ここまでの計算を自動化して表にするには次のようにする．

```
Table[{k, BaseForm[k, 2],
   Expand[f[k].{x^3, x^2, x, 1}]  // TraditionalForm,
   Expand[f[k].{x^3, x^2, x, 1}*x^3] +
     PolynomialMod[f[k].{x^3, x^2, x, 1}*x^3, x^3 + x + 1,
      Modulus -> 2] // TraditionalForm},
  {k, 0, 15}] // TableForm
```

さらに，最後の列の x の 6 次以下の多項式を 7 次元ベクトルに変えて表示するには次のようにすればよい．

```
Table[{k, BaseForm[k, 2],
   Expand[f[k].{x^3, x^2, x, 1}]  // TraditionalForm,
   Expand[f[k].{x^3, x^2, x, 1}*x^3] +
     PolynomialMod[f[k].{x^3, x^2, x, 1}*x^3, x^3 + x + 1,
      Modulus -> 2] // TraditionalForm,
   PadLeft[Reverse[CoefficientList[
       Expand[f[k].{x^3, x^2, x, 1}*x^3] +
        PolynomialMod[f[k].{x^3, x^2, x, 1}*x^3, x^3 + x + 1,
         Modulus -> 2], x]
      ], 7] // StandardForm},
  {k, 0, 15}] // TableForm
```

3 前々回に作った符号多項式の表と，上で得られた結果と比較せよ．

ここで，最後の列の 7 次元ベクトルだけを取りだし，それらの間の Hamming 距離を計算し，表にしてみる．

```
words = Table[
   PadLeft[Reverse[CoefficientList[
      Expand[f[k].{x^3, x^2, x, 1}*x^3]
       + PolynomialMod[f[k] . {x^3, x^2, x, 1}*x^3, x^3 + x + 1,
        Modulus -> 2], x]], 7],
   {k, 0, 15}];
Table[Table[HammingDistance[words[[i]], words[[j]]], {j, 1, 16}], {i, 1, 16}]
```

4 上の結果から 16 個の符号語間の Hamming 距離の最小値を求めよ．

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)