入学年度	学部	学 科	組	番 号	検	フリガナ
						氏 名

0 と 1 のみからなる集合 $\{0,1\}$ において $1+1=0$ と定義し，それ以外は通常の演算を定義すると，四則演算が可能な閉じた数の体系ができる．これを $\mathbf{F}_2$ とか $GF(2)$ と書き，位数 2 の「有限体」とか「ガロワ体」と呼ぶ．

前回，$\mathbf{F}_2=\{0,1\}$ からはじめて 8 個の元からなる新たな数の体系 $\mathbf{F}_8$ を構成した．基本的な考え方は，実数から複素数に数の概念を拡張する仕方と同様である．複素数は実数に $i^2=-1$ をみたす「虚数」i を付け加えて出来るのであった．$\mathbf{F}_8$ は $\mathbf{F}_2$ に $a^3+a+1=0$ という 3 次式をみたす新たな「虚数」a を付け加えて得られる．要素の個数がさらに 2 倍の $\mathbf{F}_{16}$ も同様に構成される．$\mathbf{F}_{16}$ は $\mathbf{F}_2$ に 4 次式

$$b^4+b+1=0$$

をみたす，a とは別の「虚数」b を付け加えて得られる．b の 4 次以上の式は b^4 が現れるごとに $b+1$ に置き換えることによってすべて 3 次以下の式に変形することができるので，$\mathbf{F}_{16}$ に属する数はすべて b の 3 次以下の式で表すことが出来る．$\mathbf{F}_8$ と同様に $b^1,b^2,\ldots,b^n,\ldots$ を計算し，b の 3 次以下の式の形に直して見てみよう．

$b^0=$

$b^1=$

$b^2=$

$b^3=$

$b^4=$

$b^5=$

$b^6=$

$b^7=$

$b^8=$

$b^9=$

$b^{10}=$

$b^{11}=$

$b^{12}=$

$b^{13}=$

$b^{14}=$

$b^{15}=$

$\mathbf{F}_{16}$ の数は

$$kb^3+lb^2+mb+n \quad (k,l,m,n \text{ は } 0 \text{ または } 1)$$

の形に表される．いま，この多項式 kb^3+lb^2+mb+n を “$klmn$” と書きこれを 2 進数で表された整数と考える．例えば，b^3+b+1 を 1011 と表し，これを 2 進数 $1011_{(2)}$ とみて，それを 10 進法で表し 11 を対応させる．すなわち，

$$b^3+b+1 \quad\longmapsto\quad 1\cdot b^3+0\cdot b^2+1\cdot b+1 \quad\longmapsto\quad 1011 \quad\longmapsto\quad 1011_{(2)}=11$$

1 以下の表を完成させよ．

指数 k	b^k	3 次以下の式	2 進法	10 進法
0	b^0	1	1	1
1	b^1			
2	b^2			
3	b^3			
4	b^4			
5	b^5			
6	b^6			
7	b^7	b^3+b+1	1011	11
8	b^8			
9	b^9			
10	b^{10}			
11	b^{11}			
12	b^{12}			
13	b^{13}			
14	b^{14}			

【裏に続く】

2 前ページの表を並べ替え，以下の表を完成させよ．

10 進法	2 進法	3 次以下の式	b^k	指数 k
1	1	1	b^0	0
2				
3				
4				
5				
6				
7				
8				
9				
10				
11	1011	b^3+b+1	b^7	7
12				
13				
14				
15				

この表を用いると，3 次以下の式で表された F_{16} の 2 つの数のかけ算を，それぞれの数を b^k の形に表した上で，指数の足し算として計算できる．

3 a) $(b^3+b+1)(b+1)=$

b) $(b^3+b^2+1)(b^2+b+1)=$

c) $(b^2+b+1)(b^2+1)=$

d) $(b^3+b+1)(b^3+1)=$

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)

Mathematica で問題 1 の表を作るには次のようにすればよい．

```
<< FiniteFields‘

F16 = GF[2, {1, 1, 0, 0, 1}];

Table[{i, b^i,
   ElementToPolynomial[Power[F16[{0, 1, 0, 0}], i], b]
    // TraditionalForm,
   BaseForm[
    ElementToPolynomial[Power[F16[{0, 1, 0, 0}], i], b] /. b -> 2,
    2],
   ElementToPolynomial[Power[F16[{0, 1, 0, 0}], i], b] /. b -> 2},
  {i, 1, 15}] // TableForm
```

QR-コードなどに実際に使われるのは $2^8=256$ 個の数からなる体 $\mathbf{F}_{256}$ である．この体は F_2 に $g^8+g^4+g^3+g^2+1=0$ をみたす虚数 g を付け加えて得られる体である． $\mathbf{F}_{256}$ について上の表と同じ表を作るには上の式を少し変更して次のようにすればよい．

```
F256 = GF[2, {1, 0, 1, 1, 1, 0, 0, 0, 1}];

Table[{i, g^i,
   ElementToPolynomial[Power[F256[{0, 1, 0, 0}], i], g] //
    TraditionalForm,
   BaseForm[
    ElementToPolynomial[Power[F256[{0, 1, 0, 0}], i], g] /. g -> 2,
    2],
    ElementToPolynomial[Power[F256[{0, 1, 0, 0}], i], g] /. g -> 2},
   {i, 1, 255}] // TableForm
```