やり直しのための 伝送数学

三谷 政昭

連載第23回の今回は，エラー訂正技術の例としてOFDMシステムで多用されるブロック符号としてRS（リード・ソロモン）符号を取り上げる．この符号は，連続したビット・エラー（バースト・エラー）の訂正が可能で，モジュロ（剰余）演算に基礎をなしており，数学分野での整数論，体，環などの群論と呼ぶ知識が必要となる．（編集部）

第23回　OFDMシステムの受信性能向上技術（その3）　複数バースト・エラー訂正可能なRS符号

前回（2011年10月号，pp.152-159）は，エラー検出・訂正技術の基本的な考え方を中心に，ハミング符号による符号化/復号化のしくみや計算方法を具体的に紹介した．

今回は，地上デジタル放送のような雑音とマルチパスの影響を受けやすい通信路やケーブル・テレビなどで利用される“RS（リード・ソロモン）符号”を解説する．モジュロ演算や，素数に基づく符号表現などの基礎理論から始めて，複数個のバースト・エラーを訂正するしくみを味わってもらおうという趣向である．特に，数学的な表現が難解なので，具体的な数値例を示すことにより，理解しやすくなるように工夫した説明を心がけたつもりではあるが，果たしてどうなることやら……（かなり心配，ドキドキ感が抜けきれないなぁ）．

1．RS符号，BCH符号の基礎数学

まずは，符号理論を系統的に理解するのに必要となる剰余計算（余りを求める）についての理解を深める．

例えば，7で割ったときの余り（モジュロ7の演算といい，mod 7と表記）は集合｛0，1，2，3，4，5，6｝であり，7種類の元（げん）をもっている．ここで，通常の算法としての加算（+），乗算（・あるいは×）の計算結果（和，積）をそれぞれ**表1**，**表2**に示す．つまり，通常の加算では5＋6＝11であるが，11を7で割った余りが4となるので，mod 7では5＋6＝4となる．また，通常の乗算では5・6=30となるが，30を7で割ったときの余りが2であることから，mod 7では5・6=2となるわけである．

ところで，加算の表では全ての各行，各列に0が1回だけ現れるので，加算に関する逆元（$-a$）が，

$$a+(-a)=0 \quad \cdots\cdots(1)$$

となるように定義される（**表3**）．つまり，（－3）は，

$$3+y=7 \quad \cdots\cdots(2)$$

を満たす正整数値y（$0 \leqq y \leqq 6$）を考えればよい．なぜなら，mod 7の演算では，右辺の数値7は7で割ると余りは0であり，

$$3+y=0 \quad \cdots\cdots(3)$$

と表される．よって，式(2)と式(3)からy=4とy=－3が得られるので，

$$(-3)=4 \bmod 7 \quad \cdots\cdots(4)$$

であり，同様の計算によって加算に関する逆元が**表3**のように求められるわけだ．

また，乗算の表では第1行と第1列を除いて，残りの全ての各行，各列に1が1回だけ現れるので，乗算に関する逆元$a^{-1}=\frac{1}{a}$として，

$$a \cdot a^{-1}=1 \quad \cdots\cdots(5)$$

となるように定義される（**表4**）．例えば，$3^{-1}=\frac{1}{3}$は，

◀**表1**
加算（mod 7）

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

▶**表2**
乗算（mod 7）

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

KEYWORD——RS符号，BCH符号，エラー訂正，生成多項式，ガロア体