第４週

公開暗号理論を理解するにはある程度の整数論の理解が必要である。ここではユークリッドの互除法とフェルマーの小定理を説明します。

１．整数について

定理４．１　$a,b\in\mathbb{Z}$，$b\neq 0$ とする。このとき，$a=bq+r \quad 0\le r<|b|$ となる整数 q と r が一意的に存在する。

証明　存在することは明らかなので，一意性についてのみ証明する。
$a=bq'+r'$，$q'\neq q, r'\neq r$ であったとする。$bq+r=bq'+r'$ より，$b(q'-q)=r-r'$ である。$r'<r$ としてもよしのでそう仮定する。すると，$0<r-r'<|b|$ であるが，$b|(r-r')$ なってしまって矛盾する。□

＊$x|y$ は x は y を割り切るという意味の記号です。

定義　$a,b\in\mathbb{Z}, a\neq 0, b\neq 0$ とする。

① $d|a$ かつ $d|b$ となる d を a と b の**公約数**という。
② d は a と b の公約数で，$c|a$ かつ $c|b$ となるどんな整数 c も $c|d$ となるとき，d を a と b の**最大公約数**という。
③ a と b の最大公約数を $\gcd(a,b)$ と書き，さらに $\gcd(a,b)=1$ のとき，a と b は**互いに素**であるという。

定理４．２　$\gcd(a,b)=d$ とする。このとき，$d=ax+by$ となる整数 x, y が存在する。

証明　$ax+by$ の最小の正の整数を d とする。$a=dq+r \ 0\le r<d$ とおくと，
$r=a-dq=a-(ax+by)q=a(1-qx)+b(1-qy)$ となる。d の最小性より $r=0$ でなくてはならない。よって，$d|a$ である。同様に $d|b$ もいえる。次にもし $a=ca', b=cb'$ であったとすると，$d=c(a'x+b'y)$ なので，$c|d$ である。よって $d=\gcd(a,b)$ である。

１．ユークリッド互除法について
ユークリッド互除法とは定理４．２を使って最大公約数を求める方法です。

定理４．３（ユークリッド互除法）　$a=b+c$ で $d|a$ かつ $d|b$ ならば，$d|c$ である。

証明　$d|a$ かつ $d|b$ より $d|(a-b)$ である。$c=a-b$ より $d|c$ である。□

$d=\gcd(72,56)$ をユークリッド互除法で求めてみます。
$72=56\times 1+16$ よって，$d=\gcd(56,16)$,
$56=16\times 3+8$ よって，$d=\gcd(16,8)$,
$16=8\times 2+0$ よって，$d=\gcd(8,0)=8$,
したがって，$d=\gcd(72,56)=8$ です。

【練習４】$d=\gcd(5112,1775)$ を求めよ。

２．剰余の計算

$a=qm+r\ (0\le r<m)$ のとき，r を m で割ったときの余りといい，

$$a\equiv r \bmod m \quad \text{または，} \quad a\equiv r\ (m)$$

と書き，a と r は**法 m で合同**であるといいます。

命題４．４　$a\equiv c\ (m),\ \ b\equiv d\ (m)$ のとき，次が成り立つ。

①　$a+b=c+d\ (m)$，　②　$a-b=c-d\ (m)$，　③　$ab=cd\ (m)$

証明　略　□

例１）　12345^3 を51で割ったときの余りを求めてみます。
$12345\equiv 3\ (51)$ です。よって，命題４の③により，余りは27となります。

例２）　180^{180} を51で割ったときの余りを求めてみます。普通の電卓ではエラーになるので，分割して考えます。$180\equiv 27\ (51)$ です。また，$27^{180}=(27^2)^{90}$ と考えます。$(27)^2\equiv 15\ (51)$ であり，$15^{90}=(15^2)^{45}\equiv 21^{45}\ (51)$ です。さらに $21^{45}=(21^3)^{15}\equiv 30^{15}\ (51)$，さらに，$30^{15}=(30^3)^5\equiv 21^5\equiv 21\ (51)$ となります。したがって，21が余りです。

【練習５】263^{510} を35で割ったときの余りを求めてみよう。

定理４．５　p を素数，$a\in\mathbb{Z}_p, a\neq 0$ とする。このとき，$a\cdot x=1$ となる $x\in\mathbb{Z}_p$ が存在する。

証明　$\gcd(p,a)=1$ なので，定理２より，$ax+py=1$ となる整数 x,y が存在する。従って $ax\equiv 1\ (p)$ となり証明された。□

上の x を a の逆元といい，普通 a^{-1} と書きます。

補題４．６　p を素数，$a,b,x\in\mathbb{Z}_p$ とする。$x\neq 0, a\neq b$ ならば，$ax\neq bx$ である。

証明　$ax=bx$ としよう。$(a-b)x=0$ で $x\neq 0$ とし，x^{-1} を両辺に掛けると，$a-b=0$ となる。□

補代４．６は，$a,2a,3a,\cdots(p-1)a$ は $\mathbb{Z}_p$ において全て異なる元であるということを意味する。

定理４．７　p を素数のとき，$\mathbb{Z}_p$ は体である。

証明　定理４．５と補題４．６よりいえる。□

定理４．８（フェルマーの小定理）　p を素数とする。a を p と互いに素な整数とすと，$a^{p-1}\equiv 1\ \ (p)$ が成り立つ。

証明　$\mathbb{Z}_p$ で考えると，$1\cdot 2\cdots(p-1)\equiv a\cdot 2a\cdots(p-1)a\equiv a^{p-1}(1\cdot 2\cdots(p-1))\ \ (p)$
であるので，$a^{p-1}\equiv 1\ \ (p)$ が成立する。□

第５週，第６週

１．はじめに

アナログ暗号は文字を数字に置き換えたものです。例えば次の頁の[表１]を使い He likes ciphers を暗号化（デジタル化）したとすると、1815 2219211529 13192618152829 となります。しかし、コンピュータが目覚しい勢いで発達している現在、このような暗号はすでに使い物にならなくなっています。

２．因数分解について

暗号で剰余を扱うとき、問題となるのが、どの数を法とするかです。余りめちゃくちゃな数だと、暗号を解読するときが問題となるし、簡単な数だとすぐに暗号がばれてしまう危険があります。１つの案として法を大きな素数にするという考え方があります。法を素数 p にすると、前回示したようにフェルマーの小定理が成立します。

この定理を使うと与えられた数 n が素数であるかどうかを、ある程度判定できます。つまり x をランダムに選んでそれを $n-1$ 乗して余りが 1 に成るかどうかを検査してみるのです。現在ではこれを修正して n が確かに素数であると断定できる検査法が確立しています。現在 50～７０桁の数 n が素数であるかどうかを判定するのは、高速計算機で、1 時間もあれば十分に可能であるそうです。

そこで、n を 2 つの素数 p と q の積として考えます。n が素数ではないということが解かったとき、それを完全に素因数分解しようとすると現在のコンピュータでは何百年もかかってしまいます。つまり素数に関する検査法があるのに対して、n を高速に因数分解する方法はまだ完全に確立していないのです。

３．RSA による暗号化と解読法

公開暗号を実際に作りながら、説明していきます。まず公開暗号として、法 n を決めます。例えば n として 92051747 とします。これは、２つの素数 p =5647 と q =16301 の積である。次に適当な大きな数字 r を 1 つ公開します。例えば r として 101 を選ぶとします。この r は $p-1$ と $q-1$ の積 92029800 と互いに素(最大公約数が１)になるように選んでいます。この 2 つの数字 92051747 と 101 が、公開暗号です。 注意すべきことは、p =5647 と q =16301 は秘密であって、本当は私以外誰も知らないのです。

公開暗号鍵 $n = 92051747$ $r = 101$

公開暗号の特徴は、あなたが他人に暗号メッセージを送るときに、他人の公開暗号鍵を使って自分のメールを**暗号化**していくことです。 つまりあなたのメールを私に送るとき、私の公開暗号鍵を使うのです。

（１） 暗号化 (encipherment)

あなたは私に対して次の文章 (plain text) を暗号化して送ることにします。ここで公開暗号鍵の n が 92051747 なので，メッセージは 90000000 までとします。

help

まずこれを、表１に従ってアナログ化すると、

18152226

となります。次に法 92051747 で r=101 を使って剰余の計算♣を行うと、

$$18152226^{101} \equiv 82813927 \bmod 92051747$$

となります。これで、暗号文 (cipher)

82813927

の完成です。あなたはこの数字を私に送ればよいのです。

♣ 計算は WINDOWS の PC であれば，スタートのプログラムのアクセサリーにある電卓を使うとよいです。但し電卓の種類は関数電卓を選択します。

（2） 解読 (decipherment)

あなたから送られてきた暗号を**解読**しましょう。しかし実際は私だけの秘密の作業です。解読に必要な解読用鍵ｓを作らなければなりません。そのために準備として、$p-1$　$q-1$　の 2 つの数字、$5647-1=5646$ と$16301\text{-}1=16300$を用意します。そして次の方程式からｓ を求めます。

$$rs \equiv 1 \mod (p-1)(q-1)$$

即ち、

$$101s \equiv 1 \mod 92029800$$

です。これを解いて、s=32802701 を得ます。

解読は、　$x \equiv 82813927^{s} \mod n$

即ち　$x \equiv 82813927^{32802701} \mod 92051747$

を解くとｘ=18152226 です。即ち help　という文章が**解読**されたことになります。

［表１］

a	b	c	d	e	F	g	h	i	j	k	l	m
11	12	13	14	15	16	17	18	19	20	21	22	23
n	o	p	q	r	S	t	u	v	w	x	y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

【練習６】公開暗号鍵を作ってみよう。

【練習７】上の表を使って簡単な文の暗号，解読を行ってみよう。

【課題５】ＲＳＡ暗号の暗号化，暗号解読プログラムをつくってみよう。

第７週，第８週

ここでは楕円曲線を使った暗号理論を紹介します。楕円曲線は普通のアフィン平面ではなく射影平面といわれるものの上で定義された３次曲線です。

１．射影平面について

わかりやすく考えるため体は実数体とし，まずアフィン平面として普通のデカルト平面（x_0x_1平面）を考えます。x_0x_1平面の原点を通る直線全体を$\mathbf{P}^1$とします。言い換えると$\mathbf{P}^1$の元は原点を通る直線です。$\mathbf{P}^1$のことを**射影直線**といいます。原点を通る同一直線上の点はその比$(x_0 : x_1)$が等しいのです。したがって，$\mathbf{P}^1$の元は$(x_0 : x_1)$であるということができます。　さて，$x_1 = 1$，$x = \dfrac{x_0}{x_1}$と置くと，$(x_0 : x_1) = (x : 1)$となります。xは実直線に対応しています。同様に$x_0 = 1$，$y = \dfrac{x_1}{x_0}$と置くと，$(x_0 : x_1) = (1 : y)$となります。yは実直線に対応しています。したがって$\mathbf{P}^1$は2つの直線で張り合ったものと考えることができます。

次にデカルト空間（$x_0x_1x_2$空間）を考えます。そして先ほどと同じように原点を通る直線全体を考え，それを$\mathbf{P}^2$をします。$\mathbf{P}^2$を**射影平面**といいます。$\mathbf{P}^2$の元は原点を通る直線なので，同一直線上の点はその比$(x_0 : x_1 : x_2)$が等しくなります。したがって，$\mathbf{P}^2$の元は$(x_0 : x_1 : x_2)$であるということがいえます。さて，$x_2 = 1$，$x = \dfrac{x_0}{x_2}$，$y = \dfrac{x_1}{x_2}$と置くと，$(x_0 : x_1 : x_2) = (x : y : 1)$となります。$(x, y)$は実平面に対応しています。同様に$x_1 = 1$，$s = \dfrac{x_2}{x_1}$，$t = \dfrac{x_0}{x_1}$と置くと，$(x_0 : x_1 : x_2) = (t : 1 : s)$となります。$(s, t)$は実平面に対応しています。同様に$x_0 = 1$，$v = \dfrac{x_1}{x_0}$，$w = \dfrac{x_2}{x_0}$と置くと，$(x_0 : x_1 : x_2) = (1 : v : w)$となります。$(v, w)$は実平面に対応しています。したがって$\mathbf{P}^2$は３つの実平面で張り合ったものと考えることができます。張り合っている部分は，

$$x = \frac{t}{s} = \frac{1}{w}, \quad y = \frac{1}{s} = \frac{v}{w}$$

という状況になっています。

２．射影平面上の曲線

まず$\mathbf{P}^2$上の直線を定義します。$\mathbf{P}^2$は３つの実平面で張り合っていました。その中のxyを座標にもつ平面は，普通の直線になっています。したがってそこでは，$y = ax + b$がその方程式です。$x = \dfrac{x_0}{x_2}$，$y = \dfrac{x_1}{x_2}$だったので，これを代入すると，$x_1 = ax_0 + bx_2$となります。これが$\mathbf{P}^2$上の直線の方程式で，１次斉次多項式イコール0という形をしています。ところでxy平面における２つの直線，$y = ax$，$y = ax + b$　$(a \neq b)$はいわゆる平行といわれるものでした。これを$\mathbf{P}^2$上の方程式で書き直すと，

$$x_1 = ax_0, \quad x_1 = ax_0 + bx_2$$

となります。これをみると，$(1 : a : 0)$で交わっていることがわかります。つまり別な座標の平面（例えばvw平面）上で交わっているのです。このことから$\mathbf{P}^2$上の2直線は必ず1点で交わるこ

とがわかります。

次に一般の n 次曲線の定義を行います。 n 次曲線は

$$x_0, x_1, x_2 \text{ の } n \text{ 次斉次多項式} = 0$$

で与えられます。

例えば，2 次曲線 $x_0{}^2 + x_1{}^2 = x_2{}^2$ は， xy 平面は円の方程式を与えます。他の平面では，双曲線の方程式を与えます。実は体を複素数体に取れば，射影変換により，全ての既約な 2 次曲線は $x_2{}^2 = x_0 x_1$ の形に書くことができます。

３次曲線になると，2 次曲線のようにシンプルな議論はできなくなりますが，それでも３次曲線は次の３つのタイプになります。

① 自分自身で交差する点を 1 個もつ曲線
② 1 点が尖点となっている曲線
③ どの点もスムーズな曲線

③の曲線は**楕円曲線**といわれて， xy 座標で書くと，

$$C : y^2 = x^3 + ax + b \quad （a, b \text{ は定数}）$$

という形になります。この曲線が暗号理論に使われます。この曲線の方程式を斉次座標で書くと

$$x_1{}^2 x_2 = x_0{}^3 + a x_0 x_2{}^2 + b x_2{}^3$$

となります。この曲線には， $(0:1:0)$ が必ず含まれます。

３．楕円曲線暗号について

楕円曲線　$C : y^2 = x^3 + ax + b$ （a, b は定数）は群構造を持っています。以下それを紹介します。

$P, Q \in C$ とします。そして $P + Q$ を次のように定義します。

> R を直線 PQ と C との交点とし，さらに x 軸に対して R と対称な点を R' とします。
> そこで， $P + Q = R'$ とします。

$P = (x_1, y_1)$， $Q = (x_2, y_2)$， $R' = (x_3, y_3)$ とします。直線 PQ を $y = \lambda x + \mu$ とおくと，
$(\lambda x + \mu)^2 = x^3 + ax + b$ となります。これを整理すると，$x^3 - \lambda^2 x^2 + (a - 2\lambda\mu)x + b - \mu^2 = 0$ がえられます。解と係数の関係から， $x_3 = \lambda^2 - x_1 - x_2$ となり， $-y_3 = \lambda(x_3 - x_1) + y_1$ が得られます。

ここで，もし $P \neq Q$ ならば， $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$ であり， $P = Q$ ならば， $\lambda = \dfrac{3x_1{}^2 + a}{2y_1}$ です。

例　楕円曲線をアファイン平面 $\mathbb{Z}_p \times \mathbb{Z}_p$ で考えます。$p = 13$ とし, 楕円曲線は $C : y^2 = x^3 + 2x + 2$ とします。
この楕円曲線上の点は， $(0:1:0)$ を O と書くと，

$$(2,1),\quad (2,12),\quad (3,3),\quad (3,10),\quad (4,3),$$
$$(4,10),\quad (6,3),\quad (6,10),\quad (8,6),\quad (8,7),$$
$$(11,4),\quad (11,9),\quad (12,5),\quad (12,8),\quad O$$

です。 $P = (8,6)$ とすると，

$$2P = (11,4),\quad 3P = (6,10),\quad 4P = (3,10),\quad 5P = (12,5),\quad 6P = (2,12),$$
$$7P = (4,3),\quad 8P = (4,10),\quad 9P = (2,1),\quad 10P = (12,8),\quad 11P = (3,3),$$
$$12P = (6,3),\quad 13P = (11,9),\quad 14P = (8,7),\quad 15P = O$$

となります。
一般に大きな素数 p が与えられたとき，ap の計算をすることは簡単ですが，しかし，(x, y) が分かっているとき $ap = (x, y)$ となる a を見つけることは困難です。
　このような原理から楕円暗号は次の手順で行われます。

① 素数 p と最初の点 P を決め，それを公開する。
② $Q = aP$ とし，Q を公開する。a は秘密鍵である。
③ 平文 m を楕円曲線上の点 R に対応させる。
④ $c_1 = R + kQ,\quad c_2 = kP$ を暗号として送る。ただし k は乱数である。
⑤ $c_1 - ac_2$ を計算し解読する。すなわち，$c_1 - ac_2 = (R + kQ) - akP = R + kaP - kaP = R$ なので解読できる。

【練習８】上の例の楕円曲線と $p = 13, P = (8, 6)$ を使って，$a = 10$ とし，適当な文 R の暗号，解読を行ってみよう。

【練習９】もう少し大きな素数で楕円曲線暗号のシミュレーションを行ってみよう。

【課題６】だ円曲線暗号の暗号化，解読プログラムを作ってみよう。

＊ **第２回レポート提出について。**
【課題５】,【課題６】の中から好きな課題を１つ選んでレポートとして提出せよ。

第９週

１．符号理論について

ロケットを飛ばして火星の写真を撮り，地球に送る際デジタル化，すなわち 0 と 1 の信号に変えて送ることを考えてみましょう。送信の途中で宇宙線などの妨害を受けて間違った情報を得る可能性が考えられます。したがって，この間違いをなるべく正しく訂正する技術，これが符号理論なのです。

２．線形符号

$\mathbb{F}_q$ を，$q(q=p^a, p$ は素数，a は自然数）個の元をもつ有限体とし，$\mathbb{F}_q^{\,n}$ を $\mathbb{F}_q$ 上の n 次元ベクトル空間とします。$\mathbb{F}_q^{\,n}$ の元 $(x_1, x_2, \cdots, x_n)$ を**語**といいます。$\mathbb{F}_q^{\,n}$ の部分空間 C を考え，C のことを**線形符号**（liner code）といいます。n を C の**符号長**といいます。$\mathbb{F}_q^{\,n} \setminus C$ は冗長部分で，この部分を誤り訂正に用います。C が大きい方が多くの情報を伝えることができ，反対に $\mathbb{F}_q^{\,n} \setminus C$ が大きい方が一般に誤り訂正能力が高くなります。相反するこの両方の条件をみたすできるだけ効率の良い符号をつくることをねざしています。

３．ハミング距離

誤りを訂正するために語と語の距離の定義が必要となります。

定義９.１　$\mathbb{F}_q^{\,n}$ の 2 語 $x=(x_1, x_2, \cdots, x_n)$，$y=(y_1, y_2, \cdots, y_n)$ の距離 $d(x, y)$ を次のように定義します。

$$d(x, y) = |\{1 \le i \le n : x_i \ne y_i\}|$$

ここに，集合 S に対し $|S|$ は S の元の個数を表します。

$d(x, y)$ は次の３つの条件をみたします。

① $d(x, y) \ge 0$

② $d(x, y) = d(y, x)$

③ $d(x, y) + d(y, z) \ge d(x, z)$

＊　一般に上の３つの条件そみたすものを距離と呼んでいます。

定義９.２　線形符号 C の**最小距離** d を次のように定義します。

$$d = \min\{d(x, y) : x, y \in C, x \ne y\}$$

誤り訂正は次の原理によって行われます。

命題９.３　d を符号 C の最小距離とする。このとき，$e = \left[\dfrac{d-1}{2}\right]$ ビットの誤りは訂正可能である。ここで，$[x]$ は x の整数部分を表す。

証明　$d(x, y) \le e$ とする。もし，$d(z, y) \le d(x, y)$ なる z があったとすると，

$d(x, z) \le d(x, y) + d(y, z) \le 2d(x, y) \le 2e < d$ となり，d の最小性に矛盾する。□

定義９.４　$\mathbb{F}_q^n$ の語 x に対し，

$$w(x)=d(x,0)$$

とおいて，これを x の**重さ**という。また，線形符号 C の**最小重さ** w を次のように定義する。

$$w=\min\{w(x):x\in C,x\neq 0\}$$

命題９.５　$d=w$ が成立する。

証明　$d(x,y)=d(x-y,0)$ より明らかである。□

＊以下簡単のために，$q=2$ とします。

例）　$C=\{(0,0,0,0,0),(0,0,1,1,1),(1,1,1,0,0,),(1,1,0,1,1)\}$ は最小距離 3 の線形符号である。また C は 2 次元ベクトル空間である。

【練習１０】$C=\left\{\begin{matrix}(0,0,0,0,0), & (0,1,1,0,0), & (0,0,1,1,0), & (0,1,0,1,0),\\ (1,1,1,1,1), & (1,0,0,1,1), & (1,0,1,0,1) & \end{matrix}\right\}$ が線形符号であることを証明せよ。また最小距離と次元を求めよ。

４．生成行列

符号長 n 線形符号 C の次元が k のとき，$[n,k]$ 符号と呼ばれます。さらに最小距離が d のとき，$[n,k,d]$ 符号と呼ばれます。

$[n,k]$ 符号 C の基底を並べて (k,n) 型の行列 G を作ります。G を C の生成行列といいます。逆に，最初に G を決めて，$C=\{xG:x\in\mathbb{F}_2^k\}$ を作ることができます。

例）　$C=\{(0,0,0,0,0),(0,0,1,1,1),(1,1,1,0,0,),(1,1,0,1,1)\}$ の基底は $(0,0,1,1,1),(1,1,1,0,0)$ にとることができます。従って生成行列は，

$$G=\begin{pmatrix}0&0&1&1&1\\1&1&1&0&0\end{pmatrix}$$

となります。
逆に

$$G=\begin{pmatrix}0&0&1&1&1\\1&1&1&0&0\end{pmatrix}$$

を与えると，$(0,0)\begin{pmatrix}0&0&1&1&1\\1&1&1&0&0\end{pmatrix}=(0,0,0,0,0),\quad (1,0)\begin{pmatrix}0&0&1&1&1\\1&1&1&0&0\end{pmatrix}=(0,0,1,1,1),$

$(0,1)\begin{pmatrix}0&0&1&1&1\\1&1&1&0&0\end{pmatrix}=(1,1,1,0,0),\quad (1,1)\begin{pmatrix}0&0&1&1&1\\1&1&1&0&0\end{pmatrix}=(1,1,0,1,1)$ となり，C が得られます。

【練習１１】$G=\begin{pmatrix}1&1&0&0&0\\1&1&1&0&1\\0&0&1&1&0\end{pmatrix}$から線形符号$C$を作れ。またその符号の次元と最小距離を求めよ。

Gは作り方から，Gの２つの行を入れ替えても，２つの列を入れ替えても，またある行（または列）を何倍かして，別の行に加えても，符号Cは変化しません。したがって，Gをこれらの変換によって，$G^*=(I:G')$という形にできます。生成行列のG^*を**標準形**といいます。前の例で$C=\{(0,0,0,0,0),(0,0,1,1,1),(1,1,1,0,0,),(1,1,0,1,1)\}$の生成行列は，

$$G=\begin{pmatrix}0&0&1&1&1\\1&1&1&0&0\end{pmatrix}$$

でした。従って，標準形は，

$$G^*=\begin{pmatrix}1&0&1&1&0\\0&1&1&0&1\end{pmatrix}$$

となります。

５．パリティー検査

今度はCの直行補空間$C^{\perp}$の生成行列Hを考えます。ここで，Cの直行補空間$C^{\perp}$とは，$\mathbb{F}_2{}^n$の中でCの全ての語との内積が 0 である語全体のこといい，勿論これもまた符号となります。また線形代数の定理から，Cの次元がkならば，$C^{\perp}$の次元は$n-k$です。ですから，$C^{\perp}$は$[n,n-k]$符号ということになります。そしてHは$(n-k,n)$型の行列になります。

前回しめしたように$C=\{xG:x\in\mathbb{F}_2{}^k\}$でしたから，$H$を使って表現すると，

$$C=\{x{}^tH=0:x\in\mathbb{F}_2{}^n\}$$

ということになります。HをCの**パリティー検査行列**といいます。

またCの生成行列を最初から標準形$G^*=(I:G')$としておくと，$H=({}^tG',I)$であることがわかります。例えば，すぐ上の例では，
$C=\{(0,0,0,0,0),(0,0,1,1,1),(1,1,1,0,0,),(1,1,0,1,1)\}$の生成行列の標準形が，

$$G^*=\begin{pmatrix}1&0&1&1&0\\0&1&1&0&1\end{pmatrix}$$

なので，

$$H=\begin{pmatrix}1&1&1&0&0\\1&0&0&1&0\\0&1&0&0&1\end{pmatrix}$$

となります。

例）

$$H=\begin{pmatrix}1&1&1&0&0&0&0\\1&0&0&1&0&0&0\\1&0&0&0&1&0&0\\0&1&0&0&0&1&0\\0&1&0&0&0&0&1\end{pmatrix}$$

としてHをパリティー検査行列とする符号Cを求める．Hの標準形は,

$$H^{*}=\begin{pmatrix}1&0&0&0&0&1&1\\0&1&0&0&0&1&0\\0&0&1&0&0&1&0\\0&0&0&1&0&0&1\\0&0&0&0&1&0&1\end{pmatrix}$$

であり，したがってCの生成行列は,

$$G=\begin{pmatrix}1&1&1&0&0&1&0\\1&0&0&1&1&0&1\end{pmatrix}$$

となりこれより,

$$C=\{(0,0,0,0,0,0,0),(1,1,1,0,0,1,0),(1,0,0,1,1,0,1),(0,1,1,1,1,1,1)\}$$

となります。またCは，$[7,2,4]$符号であることがわかります。

さて，$(1,1,1,0,0,1,0)$を送信したとします。途中で何らかの妨害があり，その符合が,
$(1,1,1,0,0,1,1)$となってしまいました。これはCの中で一番近い距離にある$(1,1,1,1,0,1,0)$に訂正されるのです。しかし，受信したものが，$(1,1,0,0,0,0,1)$であった場合は，$(1,1,1,0,0,1,0)$と$(1,0,0,1,1,0,1)$のどちらにも距離３なので，訂正することが出来ない状況にあります。

【練習１２】

$G=\begin{pmatrix}1&0&1&1&0\\0&1&0&1&1\end{pmatrix}$を生成行列にもつ符号$C$のパリティー検査行列を求めよ。

【課題７】なるべく大きな符号長（9 以上）をもつ符号を構成せよ。またその生成行列とパリティー検査行列を求めよ。

第 10 週，第 11 週

１．ハミング符号

前回誤りを訂正できない例を取り扱いました。目指すものは誤りを完全に訂正できる符号です。その符号を**完全符号**といいます。その例の 1 つがハミング符号といわれるものです。

$\mathbb{F}_2^n$ の中で 0 以外の語は全部で 2^n-1 個あります。これらを列ベクトルとして並べた $(n, 2^n-1)$ 型の行列をパリティー検査行列とする符号を**ハミング符号**といいます。ハミング符号のパリティー検査行列は作り方から，どの 2 行をとってきても線形独立で，したがって，線形独立な 2 列を h_1, h_2 とすると，$h_3 = h_1 + h_2$ は必ずどこかの行にあります。このことから C 最小距離は 3 以上であることがわかります。また $h_1 = (1,0,0,\cdots,0)$，$h_2 = (0,1,0,\cdots,0)$，$h_3 = (1,1,0,\cdots,0)$ と最初の 3 行に並べ替えると，$(1,1,1,0,\cdots,0)$ は符号 C の語であることがわかります。したがって C 最小距離は 3 であることがわかります。命題９．３によりハミング符号は完全符号だということがわかります。

例　$\mathbb{F}_2^3$ の中でのハミング符号のパリティー検査行列は

$${}^tH = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$ である。

【練習１３】　$\mathbb{F}_2^4$ の中でのハミング符号のパリティー検査行列を求めよ。

２．完全符号

誤りを完全に訂正できる符号を完全符号であるといいましたが，その正確な定義を述べたいと思います。

$\mathbb{F}_2^n$ の任意の語 x と任意の非負整数 r に対して，

$$S_r(x) = \{y \in \mathbb{F}_2^n : d(x,y) \le r\}$$

を x を中心とする半径 r のハミング球といいます。d を C の最小距離，$e = \left[\frac{d-1}{2}\right]$ とおくと，任意の２つの C の語 x, y に対して，$S_e(x) \cap S_e(y) = \varnothing$ が成り立ちます。$|\mathbb{F}_2^n| = 2^n$ であり，

$$|S_e(x)| = \sum_{r=0}^{e} |\{z : d(x,z) = r\}| = \sum_{r=0}^{e} {}_nC_r$$

です。$\{S_e(x)\}_{x \in C}$ は互いに排反なので，

$$2^n = |\mathbb{F}_2^n| \ge \sum_{x \in C} |S_e(x)| = \sum_{x \in C} \sum_{r=0}^{e} {}_nC_r$$

が成立します。この不等式を**ハミング上界式**といいます。ハミング上界式において等号が成り立つ符号を完全符号といいます。完全符号は，与えられた長さ n と最小距離 d をもつ符号の中で最も符号語の数の多い符号でもあります。

３．巡回符号

有限体 $\mathbb{F}$ 上の多項式　$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$ にベクトル $(a_0, a_1, \cdots, a_n)$ を対応さ

せることによって，$\mathbb{F}^n$ の中に符号を構成することができる。
　そのようにして構成された符号 C が**線形符号**であるとは，任意の $f(x), g(x) \in C$ と $\alpha \in \mathbb{F}$ に対して，
① $f(x)+g(x) \in C$
② $\alpha f(x) \in C$
が成り立つことである。さらに**巡回符号**であるとは，①，②に加えて
③ $xf(x) \in C$
が成り立つことである。

定理１０.１　C を巡回符号，$g(x) \in C$ を最小次数とする。このとき任意の $f(x) \in C$，適当な多項式 $a(x)$ が存在して，

$$f(x) = a(x)g(x)$$

と書くことが出来る。

証明　どんな多項式 $a(x)$ に対しても $f(x) \neq a(x)g(x)$ とする。

$$f(x) = q(x)g(x) + r(x), \quad \deg r(x) < \deg g(x)$$

と書くと，$r(x) = f(x) - q(x)g(x)$ は C の語である。これは，$g(x)$ の最小性に矛盾する。□

定理１０.１の $g(x)$ を C の**生成多項式**といいます。

注意！　C の生成多項式 $g(x)$ のほかに生成多項式 $g'(x)$ があったとすると，$g(x) - g'(x)$ はまた C の語であり，しかも次数が下がることになります。これは $g(x)$ の次数の最小性に矛盾します。このことから，生成多項式は唯一つであるといえます。

　さて以下，巡回符号 C は $\mathbb{F}[x]/(x^n-1)$ の部分空間とします。ここで，$\mathbb{F}[x]/(x^n-1)$ は $\mathbf{F}$ を係数とする多項式を x^n-1 で割った余りの集合とします。このとき，C を $\mathbb{F}[x]/(x^n-1)$ 上の巡回符号といいます。また x^n-1 を**円分多項式**といいます。

定理１０.２　$\mathbb{F}[x]/(x^n-1)$ 上の巡回符号 C の生成多項式は，x^n-1 を割り切る。

証明　$\gcd(g(x), x^n-1) = d(x)$ とすると，

$$a(x)g(x) + v(x)(x^n-1) = d(x)$$

とできる。よって，

$$a(x)g(x) \equiv d(x) \mod x^n - 1$$

である。ところで，$f(x) \in C$ であるならば，

$$f(x) = a(x)g(x) + b(x)(x^n-1)$$

である。$\gcd(g(x), x^n-1) = d(x)$ より $d(x) \mid f(x)$。したがて，$d(x)$ は C の生成多項式となる。よって生成多項式の一意性より，$d(x) = g(x)$ である。□

　上の定理から巡回符号を構成するには，円分多項式 x^n-1 の因数を調べればよく，それが構成する巡回符号の生成多項式になるのです。

４．巡回符号の生成行列とパリティー検査行列

$\mathbb{F}[x]/(x^n-1)$ 上の巡回符号 C において，その生成多項式を $g(x)$ とします。$\deg(g(x)=n-k$ とすると，C は $k-1$ 次以下の全ての多項式と $g(x)$ との積によって得られます。したがって，C の基底は，$g(x), xg(x), \cdots x^k g(x)$ とできます。

$$g(x)=g_0+g_1x+\cdots+g_{n-k}x^{n-k}$$

とおくと，生成行列は，

$$G=\begin{pmatrix} g_0 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_{n-k} & 0 \cdots & 0 \\ 0 & 0 & g_0 & \cdots & g_{n-k} \cdots & 0 \\ & & & \vdots & & \\ 0 & \cdots & 0 & g_0 & \cdots & g_{n-k} \end{pmatrix}$$

となります。

一方，$h(x)=\dfrac{x^n-1}{g(x)}=h_0+h_1x+\cdots+h_kx^k$ とおくと，当然 $g(x)h(x)\equiv 0 \mod x^n-1$ です。

従って，

$$H=\begin{pmatrix} \mathbf{0} & & h_k & \cdots & h_0 \\ & \iddots & \iddots & \iddots & \\ h_k & \cdots & h_0 & & \mathbf{0} \end{pmatrix}$$

が C のパリティー検査行列となります。

例） $\mathbb{F}=\mathbb{F}_2$ 係数の多項式 $x^7-1=(1+x)(1+x+x^3)(1+x^2+x^3)$ より，$g(x)=1+x+x^3$ とする。$\mathbb{F}[x]/(x^7-1)$ 上の巡回符号 C の生成行列は

$$G=\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

である。また，$h(x)=1+x+x^2+x^4$ なので，パリティー検査行列は，

$$H=\begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

である。H をみてわかるようにこれは $\mathbb{F}_2^{\,3}$ の中でのハミング符号です。

C の語を確認してみると，

(1)(0,0,0,0,0,0,0)，(2)(1,0,1,1,0,0,0)，(3)(0,1,0,1,1,0,0)，
(4)(0,0,1,0,1,1,0)，(5)(0,0,0,1,0,1,1)，(6) (1,0,0,0,1,0,1)，
(7)(1,1,0,0,0,1,0)，(8) (0,1,1,0,0,0,1)，(9)(1,0,0,1,1,1,0)，
(10)(0,1,0,0,1,1,1)，(11)(1,0,1,0,0,1,1)，(12) (1,1,0,1,0,0,1)，
(13)(1,1,1,0,1,0,0)，(14)(0,1,1,1,0,1,0)，(15)(0,0,1,1,1,0,1)，
(16)(1,1,1,1,1,1,1)
の 16 個である。

【練習１３】$\mathbb{F}=\mathbb{F}_2$ 係数の多項式 x^7-1 において，生成行列を $g(x)=1+x^2+x^3$ とし，その巡回

符号の生成行列とパリティー検査行列を求めよ。

【課題８】$\mathbb{F}_2$ 係数の多項式 x^9-1 において，生成行列を自分で決め，その巡回符号の生成行列とパリティー検査行列を求めよ。

【課題９】$\mathbb{F}_2$ 係数の多項式 x^9-1 において，生成行列を自分で決め，その巡回符号の全ての語を求めよ。

＊ **第３回レポート提出について。**
【課題７】～【課題９】の中から好きな課題を１つ選んでレポートとして提出せよ。