1　素数とは何か

1 かそれ自身以外に約数をもなたない、2 以上の自然数を素数という。たとえば、$2,3,5,7,11$ などが素数である。ここで、割り算について復習しておこう。
整数 a を 0 でない整数 b で割ったときの商を q 、剰余を r とするとき、これらは

$$a = qb + r, \quad 0 \leq r < |b|$$

をみたす。q, r は整数であると仮定する。たとえば

$$207 = 4 \cdot 51 + 3, \quad 51 = 27 \cdot 3 + 0$$

b が a の約数とは、剰余 r が 0 になるときにいうのであった。このとき、a は b の倍数という。

2 つの整数 a, b の公約数とは、共通の約数のことであり、そのなかで最大のものを最大公約数という。a, b の公倍数とは、共通の倍数のことであり、そのなかで、正の最小のものを最小公倍数という。2 つの素数の最大公約数は 1 で、最小公倍数はそれらの積である。a, b の最大公約数は (a, b) と書かれる。たとえば

$$(2,3) = 1, \quad (207,51) = 3$$

定理　素数は無限にある。

Euclid の証明を紹介する。素数が有限個しかないとして矛盾を導く。素数を小さい順に列挙し、
$p_1 < p_2 < \ldots < p_n$ としよう。それらの積に 1 を加えた数

$$a = p_1 p_2 \ldots p_n + 1$$

はどのような数を約数とするか考えてみよう。$b \neq 1$ を a の約数の一つとする。b の約数のなかで、1 より大きい最小のものを p とすると、p は素数である。実際、 p の約数を $q \neq 1$ とすると、q は b の約数であり、 p の最小性から、 $q = p$ を得るからである。p は a の約数でもある。p は $p_1, \ldots, p_n$ のどれかのはずだが、すると、a を割ったときの剰余は 1 となり、矛盾である。したがって、素数が有限個であるとしたことは誤りである。

この方法ですでにある素数達から新しい素数をみつけることができる。たとえば、

$$2 + 1 = 3, \quad 2 \cdot 3 + 1 = 7, \quad 2 \cdot 3 \cdot 7 + 1 = 43, \quad 2 \cdot 3 \cdot 7 \cdot 43 + 1 = 13 \cdot 139$$

素数 2 からつぎつぎに素数 $3, 7, 13, 43, 139$ を得ている。しかし、この方法では小さい順に素数を見つけるということは難しい。たとえば、5 はいつ現れるのかわからない。もうすこし、試してみよう。

$$2 \cdot 3 \cdot 7 \cdot 13 \cdot 43 \cdot 139 + 1 = 3263443$$

は素数である。

$$2 \cdot 3 \cdot 7 \cdot 13 + 1 = 547, \quad 3 \cdot 13 + 1 = 2^3 5, \quad 3 \cdot 7 + 1 = 2 \cdot 11$$

素数 $5, 11$ がようやく現れた。

2　篩、素数の分布

素数を小さい順にみつける方法をここに紹介する。Eratosthenes の篩という方法である。素数でない、1 より大きな整数を合成数というが、合成数を消去して、素数を得る方法である。関数 `sieve[N_]` を用いて `sieve[1000]` を実行すれば、1000 までの素数 168 個が得られる。

mathematica では素数をとりだす Prime 関数がある。これを使えば、上の結果は

```
Prime[Range[168]]
```

によって簡単に得られる。

例　Prime[Range[1000]] を実行してみよう。

S. Wagon によるつぎのプログラムは、所与の数以上の素数で最小のものをみつける。

```
FirstPrimeAbove[N_]:= Module[{k},
  k=N;
  While[!PrimeQ[k],k+=2];
  k]
```

ただし N は奇数に限る。これによれば、$10^{30}+1$ 以上の最小の素数は
$1000000000000000000000000000057$ であることがわかる（？）。

無限に存在する素数は一体どんな分布をしているのだろうか。正の実数 x 以下の素数全体の個数は $\pi(x)$ と通常書かれる。これはもちろん単調非減少である。 mathematica では PrimePi という関数名である。

```
Plot[PrimePi[x],{x,1,10^6}]
```

で、$\pi(x)$ の増加の様子がわかる。$\pi(x)$ は漸近的に $x/\log x$ になる。$x=10^{10}$ でその比は 1.0478 となる。

3　合同式

偶数奇数のように、整数を分類して考察する方法のひとつに合同式がある。m を 0 でない整数とする。二つの整数、a, b が $\bmod m$ に関して合同であるとは、$a-b$ が m でわりきれるとき、すなわち m の倍数のときにいう。

$$a \equiv b \bmod m \Longleftrightarrow m|(a-b)$$

ここで、$f|g$ は f が g を割りきることを意味する。f の倍数全体を $f\mathbf{Z}$ と書く。すると、$f|g$ は $g \in f\mathbf{Z}$ と書くこともできる。この記号を使えば、$a \equiv b \bmod m$ は $a-b \in m\mathbf{Z}$ ということになる。
合同式の基本的な性質を列挙する。

1)　$a \equiv a \bmod m$
2)　$a \equiv b \bmod m, b \equiv c \bmod m \Rightarrow a \equiv c \bmod m$
3)　$a \equiv b \bmod m \Rightarrow ka \equiv kb \bmod m$
4)　$a \equiv b \bmod m, n|m \Rightarrow a \equiv b \bmod n$

a を $b \neq 0$ で割ったときの商、剰余をそれぞれ、$q.r$ とすると、

$$a = qb + r$$

であるから、$a \equiv r \bmod b$ となる。割り算を繰り返すと、

$a = qb + r$
$b = q_2 r + r_2$　(もし、$r \neq 0$ ならば)
$r = q_3 r_2 + r_3$　(もし、$r_2 \neq 0$ ならば)
$r_2 = q_4 r_3 + r_4$　(もし、$r_3 \neq 0$ ならば)
$\cdots$

いつか剰余が 0 になる。なぜなら、剰余は非負整数で割り算の実行毎に減少するからである。いま、はじめて、r_{n+1} が 0 になったとする。

$$r_{n-1} = r_n q_{n+1}$$

最大公約数をみてみると、

$$(a,b) = (b,r) = (r,r_2) = \ldots = (r_{n-1}, r_n) = r_n$$

したがって、a,b の最大公約数が r_n であることがわかる。また、r_n が $ax+by$ の形式に表現できることもわかる。たとえば、

$$207 = 4 \cdot 51 + 3, \quad 51 = 27 \cdot 3 + 0$$

から、$3 = (207, 51) = 207 - 51 \cdot 4$ を得る。x, y が整数全体を動くとき、$ax+by$ 全体を $a\mathbf{Z} + b\mathbf{Z}$ で表す。すると、集合として

$$(a,b)\mathbf{Z} = a\mathbf{Z} + b\mathbf{Z}$$

を得る。

例 1　上述の方法によって、つぎの最大公約数をもとめよ。

1) $(46,\ 218)$
2) $(461,\ 1218)$
3) $(693,\ 2982)$
4) $(2^5 - 1,\ 2^{10} - 1)$
5) $(2^7 - 125,\ 3^7 - 432)$

a,b が互いに素であるとは a,b の最大公約数が 1 であるときにいう。このことは、$ax + by = 1$ をみたす x, y が存在することを意味するが、b を mod としてみてみると、$ax \equiv 1 \bmod b$、すなわち、x は a の逆数のような働きをする。たとえば、$3 \cdot 5 \equiv 1 \bmod 7$ であるから、方程式

$$3t + 2 \equiv 0 \bmod 7$$

の解 t は $t \equiv 5 \cdot (-2) \equiv -10 \equiv 4 \bmod 7$ となる。
p を素数とするとき、p の倍数でないどんな整数も $\bmod p$ に関して逆数をもつ。

例 2　与えられた a, p について a の $\bmod\ p$ に関する逆数を求めよ。

1)　$a = 3,\ p = 11$
2)　$a = 11,\ p = 17$
3)　$a = 4,\ p = 23$
4)　$a = 5,\ p = 37$
5)　$a = 44,\ p = 59$

4　Fermat の小定理

a,b がともに c　とお互いに素であるとき、ab, c　は互いに素である。実際、$ax \equiv 1, by \equiv 1 \bmod c$　を掛け合わせば、$abxy \equiv 1 \bmod c$ となるからである。
いま、p　を素数とし、$1, 2, \ldots, p-1$　の積をつくれば、それは $(p-1)!$　と書かれるのだが、p　と互いに素である。また、a　を p　の倍数でない整数として、$a, 2a, \ldots, (p-1)a$　の積　$a^{p-1}(p-1)!$ は $\bmod p$　に関して、$(p-1)!$ と合同である。このことから、

$$a^{p-1} \equiv 1 \bmod p$$

この結果を Fermat　の小定理という。Fermat の小定理は一般の mod に拡張される。$m \geq 2$ の自然数とする。$1, 2, \ldots, m-1$ のなかで m と互いに素な数を $a_1, a_2, \ldots, a_n$　としよう。これらの積は m と互いに素である。a　を m と互いに素な整数とすると、aa_i, は $a_1, a_2, /ldots, a_n$ のどれかに $\mathrm{mod} m$ に関して合同で、m と互いに素である。aa_i　をすべて掛け合わせれば、$\mathrm{mod} m$　に関して　$a_1, a_2, /ldots, a_n$ と合同になる。これより、

$$a^n \equiv 1 mod m$$

を得る。n　は　m　によって決定され、$n = \varphi(m)$　と書かれる。これを　Euler　関数という。とくに、m　が素数のとき、$\varphi(m) = m - 1$　が素数のとき、が成り立つ。

例１素数 p に関する整数　$a \neq 0$ の位数　ord　を

$$a^r \equiv 1 mod p$$

をみたす自然数　r　で最小のものとして定義する。以下　p　に関する整数 $p = 37$　として、位数をもとめよ。

1)　$ord\ 2$

2)　$ord\ 3$

3)　$ord\ 6$

4)　$ord\ 7$

5)　$ord\ 9$

report 素数 p に関する位数は $p-1$ の約数であることを証明せよ。(いろいろな本にのっているので参照すればよい。証明を理解するよう努力してください。)

Euler 関数は特徴的な公式をもつ。もし、m, m'　が互いに素であれば、$\varphi(mn') = \varphi(m)\varphi(m')$ が成立する。このような性質をもつ関数を数論では乗法的関数という。$1, \ldots, m-1$ の中で、m と互いに素な数達を $a_1, \ldots, a_r$ とし、$1, /ldots, m' - 1$ の中で、m と互いに素な数達を $a'_1, \ldots, a'_s$　とする。

$r = \varphi(m), s = \varphi(m')$　である。すると、$a'_i m + a_j m'$ は mm' に素であり、逆に　mm' に素な数はこのような数に $\mathrm{mod} mm'$ で合同である。また異なる i, j の組に対して、$a'_m + a_j m'$ は　$\mathrm{mod} mm'$ に関して合同ではない。

例２この公式を使って、次の Euler 関数の値をもとめよ。

1)　$\varphi(45)$

2)　$\varphi(52)$

3)　$\varphi(160)$

4)　$\varphi(324)$

5)　$\varphi(713)$

Euler　関数に関する公式をもうひとつ。

$$\sum_{d|n} \varphi(d) = n$$

これは、この関数の乗法的性質から得られる。

Mathematica では、 `EulerPhi` が利用できる。 たとえば

```
EulerPhi[324]     108
EulerPhi[713]     660
```

4.1　循環節

分数を小数に展開すると、いわゆる循環節が現れる。たとえば、

$$\frac{10}{17} = 0.[5882352941176470]588\ldots$$

では、循環節が [] で囲まれている。以降、これの繰り返しが現れる場合、節の長さは 16 で丁度 17-1 に等しい。

$$\frac{10}{41} = 0.[24390]243902439024390\ldots$$

では節の長さが 5 で、41-1 の約数である。小数をもとめるとき、剰余が出現すれば循環節がみえてくる。節の長さを m とし、剰余 r が繰り返し出現したとする。このことは $r10^m \equiv r \bmod b$　を意味する。簡単なため b を素数とすると、$10^m \equiv 1 \bmod b$、したがって、m は 10 の mod$b$ に関する位数である。

```
Mod[10^5,41]=1
```

5　有限体上の多項式環

5.1　有限体

素数 p に対して集合 $\{0,1,\ldots,p-1\}$ には mod$p$ によって四則演算を考えることができる。演算も考慮して、この集合を $GF(p)$ で表す。和差積はつぎのように定義される。

$$a+b=c \overset{\text{def}}{\Longleftrightarrow} a+b \equiv c \bmod p, \quad a-b=c \overset{\text{def}}{\Longleftrightarrow} a-b \equiv c \bmod p, \quad ab=c \overset{\text{def}}{\Longleftrightarrow} ab \equiv c \bmod p$$

議論が p に関するものであることが前提であるので、$\equiv$ を $=$ にして、mod$p$ を省略したのである。整数巾については a^{-1} は $a \neq 0$ の場合存在し、この場合一般の整数 n について巾 a^n が考えられる。1 次合同方程式

$$ax+b \equiv 0 \bmod p$$

は

$$ax+b=0$$

と書き換えられる。$a \neq 0$ ならば、この解は

$$x=-ba^{-1}$$

である。有限体の乗積表をみてみると、非零元を掛けると非零元全体の置換が得られる。

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

各列には異なる数がすべて現れていることに注意。実験計画法でこの事実が用いられる。

5.2　多項式

1 変数 x に関する $GF(p)$ 係数の多項式全体を $GF(p)[x]$ と書く。多項式の演算は通常と同様である。たとえば、$p=3$ のとき、

$$(x^3+2x+1)(x-2)-(x+1)(x^2-x)=(x^4-2x^3+2x^2-4x+x-2)-(x^3-x^2+x^2-x)=x^4-x^3+x-2$$

多項式 $f(x)$ の次数 $\deg f(x)$ は $f(x)$ に含まれる単項式 x^k のなかで最高の k のことを指す。上の多項式の次数は 4 になる。

例 **1**　$p=3$ のとき、$(x+1)^3=x^3+1$ が成り立つ。一般に $GF(p)$ において $(x+a)^p=x^p+a$ が成立する。

割り算もほとんど同様。しかし、計算の途中に出てくる逆数には注意。多項式 $f(x)$ を多項式 $g(x)$ で割ったときの商 $q(x)$ 剰余 $r(x)$ をつぎによって定義する。

$$f(x)=q(x)g(x)+r(x),\quad r(x)=0 \text{ または } \deg r(x)<\deg g(x)$$

剰余が 0 のとき、$f(x)$ は $g(x)$ で割りきれるといい、$g(x)|f(x)$ と表す。$q(x)$ の次数は、もし、$q(x)\neq 0$ ならば、 $f(x)$ のそれから、$g(x)$ の次数を差し引いたものである。$\deg q(x)=\deg f(x)-\deg g(x)$

例 **2**　$GF(5)$ において x^5+4x^3+1 を $2x^3+x+3$ で割る。$2^{-1}=3$ であることに注意して

$$x^5+4x^3+1=3(x^2+1)(2x^3+x+3)+x^2+2x+2$$

練習 : 左の式を右の式で割る。

1. $x^5+4x^3+1,\ 2x^3+x+3$　over $GF(7)$
2. $2x^4-2x^3+3x,\ x^2-x+1$　over $GF(7)$
3. $11x^5-x^4+7,\ 4x^2+5$　over $GF(13)$
4. $3x^6+x^5-2x^3+4x^2-1,\ 3x^3-x^2+2$　over $GF(5)$

多項式 $f(x)$ を $x-\alpha,\ \alpha\in GF(p)$ で割ったときの余りは $f(\alpha)$ である。$f(\alpha)=0$ であるとき、α を方程式 $f(x)=0$ の解という。このとき、$f(x)$ は $x-\alpha$ によって割りきれる。この事実から、$f(x)=0$ の $GF(p)$ における解の個数は $\deg f(x)$ を越えないことがわかる。

例 **3**　$GF(p)$ における $x^p-x=0$ の解全体は $GF(p)$ に一致する。したがって、

$$x^{p-1}-1=(x-1)(x-2)\cdots(x-p+1)$$

この式で、特に $x=0$ と置けば、Wilson の公式

$$(p-1)!\equiv -1 \bmod p$$

を得る。

5.3　原始元

$GF(p)$ の元で指数 $p-1$ であるものを原始元という。これがいつも存在することを示そう。

まず、$a,b\in GF(p)$ の指数がそれぞれ h,k であり、$(h,k)=1$ とするとする。このとき、ab の指数は hk である。実際、$(ab)^s=1$ とすれば、$1=a^{hs}b^{hs}=b^{hs}$ であるから、$k|hs$ よって $k|s$ を得る。同様に、$k|s$ を得る。

さて、原始元が存在しないとしよう。指数全体で最大のものを $c=\ \mathrm{ind}\, a$ とする。方程式 $x^c=1$ の $GF(p)$ における解はぜいぜい c 個であるから、解ではない元 b がある。$d=\ \mathrm{ind}\, b$ は c の約数ではない。そうであれば、$b^c=1$ となるからである。d を割りきるが、c を割りきらない素数 q がある。$e=b^{d/q}$ の指数は q に等しい。そこで、ae を考えると、この指数は cq になる。これは c の最大性に反する。したがって、原始元の存在がいえた。

原始元は全部で $\varphi(p-1)$ 個ある。原始元を a とするとき、$a^0,a^1,\ldots,a^{p-2}$ は $\bmod p$ の 0 以外の剰余である。$p-1$ を指数とする元は $a^f\ (f=0,\ldots,p-2)$ の形をもつ。$(f,p-1)=d$ とすると、$a^{f(p-1)/d}=1$ よ

り、$\mathrm{ind}\, a^f \leq (p-1)/d$ 。したがって、$\mathrm{ind}\, a^f = p-1$ ならば、$(f, p-1) = 1$ である。逆はもちろん真である。

例 **4**　原始元をすべてもとめよう。

1. p=5
2. p=7
3. p=11
4. p=13

6　相互法則

p が奇素数のとき、$GF(p)$ で 2 次方程式が解けるための条件をもとめてみよう。

$$ax^2 + bx + c = 0$$

ここで $a \neq 0$ とする。p が奇素数であるから、$2ab' = 1$ をみたす $b' \in GF(p)$ が存在する。

$$x^2 + 2bb'x + 2b'c = 0$$

を変形して、

$$(x + bb')^2 = (bb')^2 - 2b'c$$

を得る。
したがって、問題は簡単な 2 次方程式

$$x^2 = a$$

の解法に帰着する。この式がもし、解をもつなら、$a \neq 0$ のとき、$a^{(p-1)/2} = x^{p-1} = 1$ が成立する。逆に $a^{(p-1)/2} = 1$ ならば、b を原始元とし、$a = b^r$ と表せば、$(p-1)|r(p-1)/2$ したがって、$2|r$、すなわち a は平方数。よって、a が非平方数であるためには $a^{(p-1)/2} = -1$ であることが必要十分である。0 でない平方数、非平方数はともに全部で $(p-1)/2$ 個ある。
Legendre symbol はつぎのように定義される。

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} = 0 \ (a = 0), \quad 1 \ (a \neq 0 \text{ が平方数}), \quad -1(\text{ほか})$$

Legendre symbol の簡単な性質を述べる。

1. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
2. $\left(\frac{a^2}{p}\right) = 1$
3. $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$

ほかの奇素数 q に対する Legendre symbol との関係を得るため、議論をもとの整数の領域に戻す。整数 a の $\mathrm{mod} n$ に関する絶対最小剰余とは、$-n/2 < r \leq n/2$ を満たす剰余 r のことである。通常の剰余が $n/2$ より大きければ、それから n を減じて得られる。

[**Gauss's Lemma**]　$(a, p) = 1$ とする。集合 $Q = \{a, 2a, \ldots, a(p-1)/2\}$ の要素で、その $\mathrm{mod} p$ に関する絶対最小剰余が負であるものの個数を t とするならば、

$$\left(\frac{a}{p}\right) = (-1)^t$$

Q の要素の $\mathrm{mod} p$ に関する絶対最小剰余からなる集合を $\{r_1, r_2, \ldots, -s_1, -s_2, \ldots\}$ とすると、$r_i \neq s_j$ であり、

$$\{r_1, r_2, \ldots, s_1, s_2, \ldots\} = \{1, 2, \ldots, p-1\}$$

となる。これより、

$$a2a \cdots \frac{p-1}{2}a \equiv (-1)^t \left(\frac{p-1}{2}\right)!, \quad a^{(p-1)/2} \equiv (-1)^t \bmod p$$

この結果を利用すれば、

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

実際、$t = (p-1)/2 - [p/4]$ である。

定理　[相互法則]　p, q を異なる奇素数とするとき、

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

Gauss's lemma を用いて証明の概略を示す。そこでの関係式

$$\left(\frac{p}{q}\right) = (-1)^t, \quad \left(\frac{q}{p}\right) = (-1)^s$$

の t, s がどのようなものかを調べる。t は

$$1 \leq j \leq \frac{q-1}{2}, \quad -\frac{q}{2} < jp - iq < 0$$

をみたす整数の組み（格子点とよぶ）(i, j) の個数であり、s は

$$1 \leq i \leq \frac{p-1}{2}, \quad -\frac{p}{2} < iq - jp < 0$$

をみたす整数の組み（格子点とよぶ）(i, j) の個数である。これらは共通点をもたない。合わせれば、領域

$$0 < x < \frac{p}{2}, \quad 0 < y < \frac{q}{2}, \quad \frac{qx}{p} - \frac{q}{2p} < y < \frac{qx}{p} + \frac{1}{2}$$

に含まれる格子点全体になる。この領域の格子点の点 $P(\frac{p+1}{4}, \frac{q+1}{4})$ に関する対称点はまたこの領域に含まれる。一致するのは、$p \equiv q \equiv 3 \bmod 4$ の場合だけで、その格子点は P のみである。よって、この場合のみ、$t + s$ は奇数になる。

[**Jacobi symbol**]　$n > 1$ が奇数で、$n = p_1 p_2 \ldots$ を素因数分解とするとき、$(m, n) = 1$ なる整数 m に対して

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right)\left(\frac{m}{p_2}\right)\cdots$$

と定義する。すると、Legendre symbol と同様の関係式を得る。

例 **1**

$$\begin{aligned}\left(\frac{219}{383}\right) &= -\left(\frac{383}{219}\right) = -\left(\frac{164}{219}\right) = -\left(\frac{41}{219}\right) = -\left(\frac{219}{41}\right) = -\left(\frac{14}{41}\right) \\ &= -\left(\frac{2}{41}\right)\left(\frac{7}{41}\right) = -\left(\frac{7}{41}\right) = -\left(\frac{41}{7}\right) = -\left(\frac{-1}{7}\right) = 1\end{aligned}$$

練習

1．$\left(\frac{17}{23}\right)$　2．$\left(\frac{3}{31}\right)$　3．$\left(\frac{5}{73}\right)$　4．$\left(\frac{3}{73}\right)$

5．$\left(\frac{226}{563}\right)$　6．$\left(\frac{429}{523}\right)$　7．$\left(\frac{3766}{5987}\right)$　8．$\left(\frac{3149}{5987}\right)$

report　`mathematica` の package "NumberTheory` NumberTheoryFunctions" に `JacobiSymbol` がある。これを使って上の練習の結果を確かめてみよう。

7　Pell 方程式

7.1　連分数

連分数はつぎのような分数である。

$$[q_0, q_1, q_2, \ldots] = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots}}}$$

$q_0, q_1, q_2, \ldots$ が整数で、$q_1, q_2, \ldots$ が自然数であるとき、連分数は単純であるという。
形式をみればすぐに分かるように、

$$[q_0, q_1, \ldots, q_k, \ldots] = [q_0, q_1, \ldots, [q_k, \ldots]]$$

このことからつぎの結果を得る。

定理　q_n $(n > 0)$ を自然数とし、a_n, b_n をつぎによって定義する。

$a_0 = q_0, \quad a_1 = q_0 q_1 + 1, \quad a_{n+2} = a_{n+1} q_{n+2} + a_n$

$b_0 = 1, \quad b_1 = q_1, \quad b_{n+2} = b_{n+1} q_{n+2} + b_n$

すると

(i)　$[q_0, \ldots, q_n, \alpha] = \dfrac{\alpha a_n + a_{n-1}}{\alpha b_n + b_{n-1}}$

(ii)　$[q_0, q_1, \ldots, q_n] = \dfrac{a_n}{b_n}$

さらに、

(iii)　$a_n b_{n+1} - a_{n+1} b_n = (-1)^{n+1}$

(iv)　$(a_n, b_n) = 1$

(v)　$n > 0$ のとき $b_{n+1} > b_n \geq n$

(vi)　$\dfrac{a_0}{b_0} < \dfrac{a_1}{b_1} < \ldots < \dfrac{a_{2n}}{b_{2n}} < \ldots < \dfrac{a_{2n+1}}{b_{2n+1}} < \ldots < \dfrac{a_1}{b_1}$

(v)　すべての単純連分数は収束する

(i) が分かればあとは定義とそれからすぐに得られる。帰納法によれば

$$[q_0, q_1, \ldots, q_n, \alpha] = [q_0, q_1, \ldots, q_{n-1}, q_n + \alpha^{-1}] = \frac{(q_n + \alpha^{-1}) a_{n-1} + a_{n-2}}{(q_n + \alpha^{-1}) \alpha b_{n-1} + b_{n-2}}$$

であるから、分母を払えば、これは

$$\frac{(q_n \alpha + 1) a_{n-1} + \alpha a_{n-2}}{(q_n \alpha + 1) \alpha b_{n-1} + \alpha b_{n-2}} = \frac{\alpha(q_n a_{n-1} + a_{n-2}) + a_{n-1}}{\alpha(q_n b_{n-1} + b_{n-2}) + b_{n-1}} = \frac{\alpha a_n + a_{n-1}}{\alpha b_n + b_{n-1}}$$

(ii) は $\alpha \to \infty$ とすればよい。

実数 α に対して

$$\alpha_0 = \alpha, \quad q_n = [\alpha_n], \quad \alpha_n = (\alpha_{n-1} - q_n)^{-1}$$

を α_n が 0 にならない間引き続いて行えば、α の連分数展開が得られる。

$$\left| \alpha - \frac{a_n}{b_n} \right| < \frac{1}{b_n b_{n+1}} < \frac{1}{b_n^2}$$

α が有理数の場合、この操作は Euclid の互除法に他ならない。したがって連分数展開は有限で、得られる分数 a_n/b_n は既約分数になる。

例 **1**

$$\frac{355}{113} = [3,7,16], \quad 1+\sqrt{2} = [2,2,2,\ldots], \quad 1+\sqrt{3} = [2,1,2,1,\ldots],$$

1． $\frac{22}{7}$

2． $\frac{24}{17}$

3． $\sqrt{41}$

4． $(1+\sqrt{5})/2$

定理　2 次無理数は無限循環単純連分数で表される。

$\alpha = (c_0+\sqrt{d})/e_0$ を正の 2 次無理数とする。c_0, e_0 は整数で、$e_0 \neq 0, e_0 | d - c_0^2$ と仮定してよい。もし、そうでなければ、$\alpha = (c_0 e_0 + \sqrt{d e_0^2})/e_0^2$ を採用する。

$$\alpha_0 = \alpha, \quad q_n = [\alpha_n], \quad c_{n+1} = q_n e_n - c_n, \quad e_{n+1} = \frac{d - c_{n+1}^2}{e_n}, \quad \alpha_{n+1} = \frac{c_{n+1}+\sqrt{d}}{e_{n+1}}$$

と定義する。e_{n+1} は整数で $e_{n+1} | d - c_{n+1}^2$ をみたす。定義から、$\alpha_n - q_n = 1/\alpha_{n+1}$　したがって $\alpha_{n+1} > 0$ $\alpha = [q_0, q_1, \ldots]$ が得られる。$\sqrt{d}$ を $-\sqrt{d}$ に置き換える操作を $'$ で記すことにすれば、十分大きなすべての n で

$$\alpha_n' = \frac{c_n - \sqrt{d}}{e_n} = -\frac{b_{n-2}}{b_{n-1}} \frac{\alpha' - \frac{a_{n-2}}{b_{n-2}}}{\alpha' - \frac{a_{n-1}}{b_{n-1}}} < 0$$

これより、$0 < \alpha_n - \alpha_n' = 2\sqrt{d}/e_n$ したがって、$e_n > 0$ を得る。そして、

$$e_n \leq e_n e_{n+1} = d - c_{n+1}^2 < d, \quad c_{n+1}^2 < c_{n+1}^2 + e_n e_{n+1} = d$$

であるから、ある $n, k > 0$ で $\alpha_n = \alpha_{n+k}$ が成立する。

$$\alpha_n = [q_n, \ldots, q_{n+k-1}, \alpha_{n+k}] = [\dot{q}_n, \ldots, \dot{q}_{n+k-1}]$$

7.2　Pell 方程式

定理　d を平方数でない自然数とすると、方程式

$$x^2 - dy^2 = 1$$

は整数解 x, y をもつ。

前小節の記号を用いる。$\alpha = \sqrt{d}$ とし、$\alpha_n = (c_n + \sqrt{d})/e_n$ であったが、

$$\sqrt{d} = \frac{\alpha_n a_{n-1} + a_{n-2}}{\alpha_n b_{n-1} + b_{n-2}} = \frac{(c_n+\sqrt{d})a_{n-1} + e_n a_{n-2}}{(c_n+\sqrt{d})b_{n-1} + e_n b_{n-2}}$$

これより

$$b_{n-1}c_n + b_{n-2}e_n = a_{n-1}, \quad a_{n-1}c_n + a_{n-2}e_n = d b_{n-1}$$

そして、

$$a_{n-1}^2 - d b_{n-1}^2 = (-1)^n e_n$$

ある n, k に対して $\alpha_n = \alpha_{n+k}$ であったから、この式は無限個の n で成立し、$e_n < d$ に注意すれば、ある e に対し

$$u^2 - dv^2 = e$$

が無限個の解をもつ。ことなる解の組みを $(u_1, v_1), (u_2, v_2)$ とし、

$$x = \frac{u_1 u_2 - d v_1 v_2}{e}, \quad y = \frac{u_1 v_2 - u_2 v_1}{e}$$

と置けば、(x,y) は求める解である。

x_0, y_0 を正の解で $D = x_0 + y_0\sqrt{d}$ を最小のものとすれば、ほかの解が D の巾で与えられる。x_0, y_0 を基本解という。

例 2　つぎの Pell 方程式の基本解をもとめよ。

1．　$x^2 - 31y^2 = 1$　　$[5, \dot{1}, 1, 3, 5, 3, 1, 1, 1\dot{0}]$
2．　$x^2 - 30y^2 = 1$　　$[5, \dot{2}, 1\dot{0}]$
3．　$x^2 - 29y^2 = 1$　　$[5, \dot{2}, 1, 1, 2, 1\dot{0}]$
4．　$x^2 - 61y^2 = 1$　　$[7, \dot{1}, 4, 3, 1, 2, 2, 1, 3, 4, 1, 1\dot{4}]$

8　素数判定

8.1　$p-1$ 法

$n-1$ を素因数分解して

$$n - 1 = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$$

とする。もし、$1 \le i \le r$ に対して

$$a_i^{(n-1)/p_i} \not\equiv 1, \quad a_i^{n-1} \equiv 1 \bmod n$$

をみたす a_i が存在するならば n は素数である。

実際、a_i の $\bmod n$ に関する位数（素数の場合と同様の定義）を m_i とするとき

$$m_i = p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}, \quad 0 \le f_j \le e_j, \quad f_i = e_i$$

したがって $p_i^{e_i} | m_i$ である。$m_i | \varphi(n)$ (Fermat の小定理) であるから、$n-1 | \varphi(n)$、よって $n - 1 \le \varphi(n)$ を得る。$n \ge 2$ の場合 $\varphi(n) < n$ であるから、$\varphi(n) = n - 1$。一方 n が合成数ならば、すなわち素数でなければ $\varphi(n) < n - 1$ であるから、n は素数である。

Report　n が合成数であるとき $\varphi(n) < n - 1$ であることを証明せよ。もしできれば、n が素数巾でない合成数ならば $\varphi(n) \le n - 2\sqrt{n} + 1$ であることを証明せよ。

この方法で $n = 3547114323481$ が素数であることがわかる。

$$n - 1 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 108275773$$

であるから、つぎのように原始根をもとめることになる。

$17^{n-1} \equiv 1$,　$17^{(n-1)/2} \not\equiv 1$,　$3^{n-1} \equiv 1$,　$3^{(n-1)/3} \not\equiv 1$,
$2^{n-1} \equiv 1$,　$2^{(n-1)/5} \not\equiv 1$,　$2^{(n-1)/7} \not\equiv 1$,　$2^{(n-1)/13} \not\equiv 1$,　$2^{(n-1)/13} \not\equiv 1$,　$2^{(n-1)/108275773} \not\equiv 1$

8.2　$p+1$ 法

奇数 N が素数であることを $N+1$ が素因数分解できるときに判定できることを示す。いま

$$N + 1 = \prod_{i=1}^{r} p_i^{e_i} \quad (e_i > 0)$$

と表されるとき、a, b をつぎの条件をみたすものとする。

$$(N, b(a^2 + 4b)) = 1, \quad \left(\frac{a^2 + 4b}{N}\right) = -1$$

さらに

$$y_0 = 0, \quad y_1 = 1, \quad y_{i+1} = ay_i + by_{i-1}$$

とおく。すると、

$$y_{N+1} \equiv 0 \bmod N, \quad y_{(N+1)/p_i} \not\equiv 0 \bmod N \ (i = 1, 2, \ldots, r)$$

ならば、N は素数である。
実際、2 次方程式 $x^2 - ax - b = 0$ の解を $\alpha = (a + \sqrt{d})/2, \beta = (a - \sqrt{d})/2$ とする。ここで、$d = a^2 + 4b$ である。すると、$y_n = (\alpha^n - \beta^n)/\sqrt{d}$ を得る。$x_n = \alpha^n + \beta^n$ と置けば、これらの数は

$$x_n^2 - dy_n^2 = 4(-b)^2, \quad \alpha^n = \frac{x_n + \sqrt{d}y_n}{2}, \quad \beta^n = \frac{x_n - \sqrt{d}y_n}{2}$$

$$2x_{n+m} = x_n x_m + dy_n y_m, \quad 2y_{n+m} = x_n y_m + x_m y_m$$

$$x_n = y_{n+1} + by_{n-1}$$

をみたす。

$$y_n = \frac{1}{2^{n-1}} \sum \binom{n}{2k+1} a^{n-2k-1} d^k, x_n = \frac{1}{2^{n-1}} \sum \binom{n}{2k} a^{n-2k} d^k$$

上述の仮定のもとで、q を N の（奇数）素因子としよう。このとき

$$2^{q-1} y_q \equiv d^{(q-1)/2} \equiv \pm 1, \ 2^{q-1} x_q \equiv a^q \equiv a \bmod q$$

$2^{q-1} \equiv 1$ であるから、$x \equiv a$ となる。
$d^{(q-1)/2} \equiv -1$ の場合 $y_q \equiv -1$ であり、

$$y_{q+1} = ay_q + by_{q-1} \equiv -a + (x_q - y_{q+1}) \equiv -y_{q+1} \equiv 0 \bmod q$$

$d^{(q-1)/2} \equiv 1$ の場合 $y_q \equiv 1$ であり、同様の方法で $y_{q-1} \equiv by_{q-1} \equiv -y_{q-1} \equiv 0 \bmod q$ となることがわかる。
w を $y_w \equiv 0 \bmod N$ をみたす最小の自然数とする。仮定から $w \leq N + 1$ である。$y_n \equiv 0 \bmod N$ は $w|n$ と同値である。なぜなら、$w|n$ とすれば、$2y_n = x_{n-w} y_w + x_w y_{n-w}$ より $y_n \equiv 0$ を得る。逆に $y_n \equiv 0$ とすれば $(x_n, N) = 1$ より、$y_{n-w} \equiv 0$ を得、同様に $y_{n-2w} \equiv y_{n-3w} \equiv \ldots \equiv 0$ $w = N + 1$ を得る。さて、

$$y_n \equiv 0 \bmod q^f \ (f \geq 1) \Longrightarrow y_{nq} \equiv \bmod q^{f+1}$$

が成立する。なぜなら、$(x_{nq} + \sqrt{d}y_{nq})/2 = (x_n + \sqrt{d}y_n)^n/2^q$ を用いて、$2^{q-1} y_{nq} \equiv 0 \bmod q^{f+1}$ を得るから。

$$y_{q_i^{f_1-1}(q_i \pm 1)} \equiv 0 \bmod q^f$$

いま、$N = q_1^{f_1} q_2^{f_2} \cdots q_s^{f_s}$ とおく。$q_i^{f_1-1}(q_i \pm 1)$ $(i = 1, 2, \ldots, s)$ の最小公倍数を L とおくと、
$y_L \equiv 0 \bmod N$ したがって $N + 1|L$ となる。

$$N + 1 \leq L \leq \frac{N(q_1 + 1)(q_2 + 1) \cdots}{2^{s-1} q_1 q_2 \cdots} \leq 2N(2/3)^s$$

より $s = 1$ である。また、$q_1^{f_1} + 1 | q_1^{f_1-1}(q_1 \pm 1)$ より $f_1 = 1$ すなわち $N = q_1$ は素数である。
$(y_{q_1+1} \equiv 0 \bmod q_1$ であり、$d^{(q_1-1)/2} = -1$ によって a, b の条件が必要になる。$)$

$(N, bd) = 1$ を満たす a, b に対して上述と同様に y_n を構成する。d が $\bmod q$ に関して平方剰余か否かにしたがって $y_{q-1} \equiv 0 \bmod q$ または $y_{q+1} \equiv 0 \bmod q$ が成立する。後者の場合 $y_{k(q-1)} \equiv 0$ となる。$q + 1$ が小さな素数の積 m ならば、$y_m \equiv 0$ となる。よって、$1 < (y_m, N) < N$ となるかもしれない。これを $p + 1$ 法という。

8.3 Lucas test

p を素数とするとき、$M_p = 2^p - 1$ のかたちの素数を Mersenne 数という。Lucas test は

$$S_1 = 4, \quad S_{i+1} = S_i^2 - 2$$

を計算し、$S_{p-1} \equiv 0 \bmod M_p$ であるか否かによって Mersenne 数か否かを決定する方法である。証明は上述とほぼ同様。1992 年の段階では $p = 216091$ がレコードであったが、1996 年に $p = 1398269$ に更新された。

9 暗号

9.1 RSA

2 つの素数の積を計算するのは簡単だが、与えられた数を素因数分解することはやっかいだ、というだけの原理の暗号法である。
暗号系の加入者は十分大きな 2 つの異なる素数 p, q を選び（選び方に素数判定が必要）、その積 $n = pq$ を計算する。整数 e, d をつぎのように選択する。$(e, \varphi(n)) = 1$ なるようにとればよい。

$$ed \equiv 1 \bmod \varphi(n), \quad \varphi(n) = (p-1)(q-1)$$

(e, n) が暗号化鍵になり、公開ファイルに登録され、(d, n) は秘密の復号化鍵になる。
暗号化はつぎのように行う。平文を $n-1$ 以下の非負整数 P で表す。P を $\bmod n$ で e 乗する。したがって、暗号化関数は

$$E(P) \equiv P^e \bmod n, \quad 0 \le E(P) < n$$

で定義される。復号化は暗号文 $C = E(P)$ を $\bmod n$ で d 乗することにより行える。

$$D(C) \equiv C^d \bmod n, \quad 0 \le D(C) < n$$

実際、

$$D(E(P)) \equiv P^{ed} \bmod n$$

$ed = 1 + a\varphi(n)$ となる整数 a があるので、

$$P^{ed} = PP^{a\varphi(n)} \equiv P \bmod n$$

例 1　$n = 9991 = 97 \cdot 103, e = 131, d = 299$ としよう。平文 $P = 7332$ は 5550 にうつる。

1)　$n = 11 \cdot 13, e = 71$ のとき、d をもとめ、適当な平文を暗号化せよ。
2) $n = 13 \cdot 17, e = 97$ のとき、同様。

9.2 Discrete log

Diffie-Hellman 鍵は離散対数の計算の難しさを利用する。いま有限体の原始根 g をひとつ固定する。users A, B が秘密の鍵 $0 < a, b < p$ をもつとし、g^a, g^b を公開する。そして共通の秘密鍵を g^{ab} とする。一般のひとは公開鍵 g^a, g^b を知っているが g^{ab} を知ることは難しい。A は g^b, a をしっているので、g^{ab} を計算することができる。B についても同様。$x = g^k$ のとき、$k = \log_g x$ と書く。

例 2　$p = 19, g = 2$ として、つぎを計算せよ。
1) $\log_2 5$

2) $\log_2 6$
3) $\log_2 7$
4) $\log_2 8$

例 3　$p = 53, g = 2, a = 29, b = 19$ での秘密鍵は $2^{29 \cdot 19} \equiv 21 \bmod 53$

9.3　ElGamal

有限体 F_p の要素 g をひとつ決める。user A は任意に $0 < a < p-1$ を選び、秘密復号化鍵とする。公開暗号化鍵は g^a とする。message $0 < P < p-1$ を A に送るには、整数 k をランダムに選び、A に

$$(g^k, Pg^{ak})$$

を送る。$g^{ak} = (g^a)^k$ は簡単に計算できる。message を受け取った A は

$$Pg^{ak}/(g^k)^a = P$$

によって復号化して平文を得る。他のひとが解読する場合の困難さは g^k, g^a から g^{ak} を見つけることにある。

9.4　remark

有限体は素数に対してだけ考えられるわけではない。素数の巾 p^r の個数の要素をもつ有限体も考えられる。その場合にも原始元が存在することが証明され、ここに述べた内容は同様に遂行される。

有限体の非零元全体は可換群になり、以上の議論は可換群の特徴を生かしたものといえる。Pell 方程式や楕円曲線を用いた暗号はこの考えに基づいている。

10　有限幾何

10.1　射影平面

有限集合 P （点の集合）と有限集合 L （直線の集合）およびそれらの間の関係 $\in$ （結合関係という）からなりたつ組 $\mathbf{P}$ がつぎのような公理をみたすとき、有限射影平面という。ここで、$A \in P, a \in L$ で $A \in a$ のとき A は a 上にある、または a は A を通る、という。

1)　2 点を通る直線は唯一である。直線上には点が少なくとも 2 点ある。
2)　2 直線は唯 1 点で交わる。点は少なくとも 2 直線の交点である。
3)　どの 3 点も直線上にないような 4 点が存在する。

定理　有限射影平面にはつぎのような整数 $n \geq 2$ が存在する。n を射影平面の位数という。

i)　各直線はちょうど $n+1$ 個の点を含む。
ii)　各点はちょうど $n+1$ 本の直線の上にある。
iii)　点の総数は n^2+n+1 個、直線の総数は n^2+n+1 本である。

条件 3) を満たす 4 点を考え、その一つを A とする。A を通る直線を $a_1, a_2, \ldots, a_m$ とする。条件 1) により $m \geq 3$ である。a_i 上の A 以外の点の個数を n_i (≥ 1) とする。A を通らない直線は、条件 2) により、a_i, a_j $(i \neq j)$ 上の点によって決定されるから、それらの個数は $n_i n_j$ である。よって、$n_i = n$ は一定である。B を A 以外の点とし、たとえば a_1 上の点とする。B を通る a_1 以外の直線を b とすれば b 上の点の個

数は同様の方法により、$n+1$ であり、a_i との交点を数えれば、m である。よって、$m=n+1$ を得る。どの点も A を通る直線上にあるから、すべての点の個数は $n(n+1)+1$ となる。またどの直線も a_1 と交点をもつから、すべての直線の個数は $n(n+1)+1$ である。条件 3) より、$n^2+n+1 \geq 4$ したがって、$n \geq 2$

例 1　位数 2 の射影平面は Fano 平面とよばれる。それはまた一種類しかない。結合関係を行列で表せばつぎのようになる。

$$\begin{array}{c} \\ P_0 \\ P_1 \\ P_2 \\ P_3 \\ P_4 \\ P_5 \\ P_6 \end{array} \begin{array}{c} \begin{array}{ccccccc} l_0 & l_1 & l_2 & l_3 & l_4 & l_5 & l_6 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

Report　位数 3 の射影平面をつくってみよう。

10.2　アフィン平面

点の有限集合 P と直線の有限集合 L および、それらの間の関係 $\in$ から成り立つ組 $\mathbf{A}$ でつぎの条件を満たすものを有限 affine 平面という。

1)　2 点を通る直線が唯一存在する。直線上には点が少なくとも 2 点ある。
2)　1 点はある 2 直線の交点である。
3)　直線 a と点 A に対して、A を通り、a と交わらない直線が唯一つ存在する。
4)　1 直線上にない 3 点が存在する。

2 直線 a,b は $a=b$ または、共通点をもたないとき、平行であるといわれる。平行関係は同値関係である。この同値関係による類を平行類という。平行類 C に属さない直線 a は C の各直線に 1 点で交わる。a がある $b \in C$ と交点をもたなければ、a は b に平行、したがって、$a \in C$ となり仮定に反する。

定理　有限 affine 平面はつぎのような整数 n （位数とよぶ）をもつ。

i)　1 点を通る直線は $n+1$ 本ある。
ii)　1 直線上の点は n 個ある。
iii)　点の総数 n^2 個であり、直線の総数は n^2+n 本である。

$\mathbf{A}$ の平行類を $C_1,\ldots,C_m$ とし、対応して新たに点 $\infty_1,\ldots,\infty_m$ および直線 l_∞ を追加する。C_i に属する直線は少なくとも 2 本ある（条件 3) 4) による）。C_i の直線は ∞_i を通るとし、どの ∞_i も l_∞ 上にあるとして、結合関係を拡張する。このようにして得られた 3 つ組は射影平面となる。得られた射影平面の位数を n とすれば、$m=n+1$ で、定理の結果が得られる。affine 平面からみれば、それらは無限遠点、無限遠直線といわれる。得られた射影平面の位数を n とすると、逆に射影平面から、その任意の直線とその上の点をすべて除去すれば affine 平面が得られる。

11　射影幾何

11.1　Vector spaces

p を素数とし、$K=F_p$ とおく。$V=F_p^n=\{(x_0,\ldots,x_n) \ : \ x_i \in F_p\}$ につぎのような演算を定義する。

$$(x_0,\ldots,x_n)+(y_0,\ldots,y_n)=(x_0+y_0,\ldots,x_n+y_n), \quad a(x_0,\ldots,x_n)=a(x_0,\ldots,ax_n) \quad (a \in K)$$

演算をこめて V はベクトル空間とよばれる。V の部分集合 W は、この演算に関してベクトル空間なば、V の部分ベクトル空間といわれる。
$v_1, \ldots, v_m \in V$ の線形結合とは

$$a_1 v_1 + \cdots + a_m v_m, \quad a_i \in K$$

の形のベクトルのことを指す。これらのベクトル全体からなる V のベクトル部分空間は、v_i たちによって生成されるといわれる。すべての成分が 0 のベクトル $0 = (0, \ldots, 0)$ を零ベクトルという。零ベクトルだけからなる集合は部分空間である。これを簡単に 0 と書く。$v_1, \ldots, v_m \in V$ が線形独立であるとは

$$a_1 v_1 + \cdots + a_m v_m = 0, \quad a_i \in F_p$$

ならば、$a_1 = \ldots = a_m = 0$ が成立するときにいう。もし、部分空間 $W \neq 0$ に属するベクトルたちで、W を生成し、線形独立なものがあれば、それらは w の基底とよばれる。

$$e_i = (0, \ldots, 1, \ldots, 0) \qquad (\text{第 } i \text{ 番目が } 1)$$

全体は V の基底をなす。実際

$$(x_1, \ldots, x_n) = x_1 e_1 + \cdots + x_n e_n$$

となるからである。どの部分空間 $W \neq 0$ も基底をもつ。実際、つぎのような特別な形の基底が存在する。

$$f_i = (\text{第 } n_i \text{成分が } 1 \text{ で、第 } k > n_i \text{成分はすべて } 0), \quad n_1 < n_2 < \ldots < n_r$$

さらに、f_i の第 n_k $(k < i)$ 成分は 0 というようにとれば、このような f_i たちは一意的に確定する。このとき、r を W の次元という。

例 1　$p = 3$ で、$(1,1,0,2), (2,1,0,1), (1,2,1,1)$ で生成される部分空間の基底として
$(1,1,0,0), (2,0,1,0), (0,0,0,1)$ がとれ、その次元は 3 である。

11.2　linear equations

n 成分のベクトルに $n \times m$ 型行列を右からかければ m 成分のベクトルになる。

$$(x_1, \ldots, x_n)A = (y_1, \ldots, y_m) \quad A = (a_{ij})$$

積はつぎのように定義される。

$$y_i = x_1 a_{1i} + \cdots + x_n a_{ni}$$

方程式を簡単に $vA = w$ のように記述しよう。w が与えられたとき、この関係式 (方程式) をみたす v は解とよばれる。もし、ひとつの解 v_0 が知られたなら、$(v - v_1)A = 0$ であるから、方程式の解法は方程式 $vA = 0$ の解法に帰着する。この方程式の解全体は部分空間 (解空間という) になる。その次元を解の次元という。

例 2　$p = 3$ のとき、方程式

$$(x_1, x_2, x_3) \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 2 & 1 & 1 \\ 2 & 1 & 1 & 2 \end{pmatrix} = 0$$

の解空間の基底をもとめよ。$p = 5, 7, 11$ ではどうか。

例 3　$p = 7$ のときつぎの方程式を解け。

1. $x_1 - x_2 + x_3 + 2x_4 = 0, 2x_1 + x_2 - 4x_3 + 4x_4$
2. $2x_1 + 3x_2 - 3x_3 = 0, x_1 - x_2 + 5x_3 = 0$
3. $x_1 - 2x_2 + x_3 = 0, 2x_1 + x_2 + 5x_3 = 0$
4. $x_1 - x_2 + x_3 = 0, 2x_1 + 3x_2 + 4x + 3 = 0, 4x_1 + 5x_2 + 2x_3 = 0$

11.3　3次元射影幾何

F_p^4 につぎのような同値関係を導入する。0でない2つのベクトル v, w に関して

$$v \equiv w \Longleftrightarrow \text{ある } a \in F_p (a \neq 0) \text{ で } av = w$$

この同値関係による商空間を F_p^4 上の3次元射影幾何 $PG(3,p)$ という。点は全部で
$1 + p + p^2 + p^3 = \frac{p^4-1}{p-1}$ 個ある。$v \in F_p^4$ が属す同値類を $[v]$ で表そう。2点 $[v_1], [v_2]$ を通る直線は点

$$[av_1 + bv_2] \qquad (a, b \in F_p,\ a, b \text{のどちらかは} 0 \text{でない})$$

の集合によって定義される。3点 $[v_1], [v_2], [v_3]$ を通る平面は

$$[av_1 + bv_2 + cv_3] \qquad (a, b, c \in F_p,\ a, b, c \text{のどれか1つは} 0 \text{でない})$$

$PG(3,p)$ の任意の直線と平面は、一点で交わるか、包含関係にある。

11.4　閾値暗号系

$PG(3,p)$ の直線 m および m と一点 P で交わる平面 H を任意にとる。H 上の k 個の点 $Q_1, \ldots, Q_k$ をランダムに選ぶ。ただし、$k+1$ 個の点 $P, Q_1, \ldots, Q_k$ のどの3点も同一直線上に内ものとする。
さて、直線 m を公開し、平面 H を非公開としよう。k 人の管理者に $Q_1, \ldots, Q_k$ の座標（含んでいる F_p^4 の点の座標、斉次座標という）を共有鍵として配り、点 P の座標を秘密鍵とする。このとき、もし、k 人のうち3人が集まれば、平面 H が決まり、点 P の座標を知ることができる。しかし、2人以下の管理者では点 P の座標を知ることはできない。