二項係数に関する整数問題

以下 p は素数を表す．自然数は正の整数を表す.

定義 1　自然数 n を素因数分解したときに含まれる素因数 p の個数を

$$N_p(n)$$

と表す.

定理 1　自然数 a, b について,

$$N_p(ab) = N_p(a) + N_p(b)$$

である.

[証明略]（自明）

定理 2　自然数 a が自然数 b で割り切れるとき,

$$N_p\left(\frac{a}{b}\right) = N_p(a) - N_p(b)$$

である.

[証明略]（自明）

定理 3

$$N_p(0!) = 0$$

である.

[証明略]（自明）

定理 4　負でない整数 n について,

$$N_p\left((p^n)!\right) = \frac{p^n - 1}{p - 1}$$

である.

[証明] $n \geq 1$ のとき，1 から p^n までの自然数のなかに，p の倍数は p^{n-1} 個あり，p^2 の倍数は p^{n-2} 個ある．これを続けていくと,

$$N_p((p^n)!) = 1 + p + p^2 + \cdots + p^{n-1}$$

である．右辺は等比数列であるから,

$$N_p((p^n)!) = \frac{p^n - 1}{p - 1}$$

この式は $n = 0$ でも成り立つ.　[証明おわり]

定理 5　p の冪で表せない 自然数k について

$$N_p(k!) < \frac{k-1}{p-1}$$

が成り立つ.

[証明] k 以下の最大の p の冪を p^m とすると,

$$N_p(k!) = \left[\frac{k}{p}\right] + \left[\frac{k}{p^2}\right] + \left[\frac{k}{p^3}\right] + \cdots + \left[\frac{k}{p^m}\right]$$

である．ただし [　] はガウス記号を表す.．ガウス記号で表された式はその中身をこえることはないので，次の不等式が成り立つ.

$$N_p(k!) \leqq \frac{k}{p} + \frac{k}{p^2} + \frac{k}{p^3} + \cdots + \frac{k}{p^m}$$

等号が成り立つのは k が p^m の倍数であるときであるが，後ほどこの等号は消えてしまうので，この等号成立条件はこの定理に関しては意味がない．この不等式の右辺は等比数列であるから.

$$N_p(k!) \leqq k\frac{1-\dfrac{1}{p^m}}{p-1} = \frac{k-\dfrac{k}{p^m}}{p-1}$$

が成り立つ．また,

$$\frac{k}{p^m} > 1$$

より

$$-\frac{k}{p^m} < -1$$

よって,

$$N_p(k!) < \frac{k-1}{p-1}$$

[証明おわり]

この定理はもちろん正しいのであるが，次の定理はもう少しだけ厳しい値を与える.

定理 6　自然数 k が p のべきで表せないとき，k 以下の最大の p のべきを p^m とする．$k = p^m + j$ とすると,

$$N_p(k!) = N_p((p^m)!) + N_p(j!) = \frac{p^m-1}{p-1} + N_p(j!) \leq \frac{k-2}{p-1}$$

が成り立つ.

[証明]

$$\begin{aligned}
N_p(k!) &= \left[\frac{k}{p}\right] + \left[\frac{k}{p^2}\right] + \left[\frac{k}{p^3}\right] + \cdots + \left[\frac{k}{p^m}\right] \\
&= \left[\frac{p^m+j}{p}\right] + \left[\frac{p^m+j}{p^2}\right] + \left[\frac{p^m+j}{p^3}\right] + \cdots + \left[\frac{p^m+j}{p^m}\right] \\
&= p^{m-1} + p^{m-2} + p^{m-3} + \cdots 1 + \left[\frac{j}{p}\right] + \left[\frac{j}{p^2}\right] + \left[\frac{j}{p^3}\right] + \cdots + \left[\frac{j}{p^m}\right] \\
&= \frac{p^m-1}{p-1} + N_p(j!) \\
&\leq \frac{p^m-1}{p-1} + \frac{j-1}{p-1} = \frac{k-2}{p-1}
\end{aligned}$$

[証明終わり]

問題 1　素数 p と自然数 n について次のことを証明せよ.

$$n \text{ が } p \text{ のベキである}$$

ことの 必要十分条件 は
$1 \leq k \leq n-1$ を満たすすべての自然数 k について

$$N_p({}_n\mathrm{C}_k) > 0$$

が成り立つことである.

[解]

$$n = p^i$$

とすると.

$${}_n\mathrm{C}_k =_{p^i} \mathrm{C}_k = \frac{(p^i)!}{k!(p^i-k)!}$$

定理 4 より上式の分子に含まれるそいんすう p の個数は

$$N_p((p^i)!) = \frac{p^i-1}{p-1}$$

である．また定理 4,5 より，分母に含まれる p の個数は

$$N_p(k!(p^i-k)!) \leq \frac{k-1}{p-1} + \frac{p^i-k-1}{p-1} = \frac{p^i-2}{p-1}$$

つまり分母の p の個数は分子の p の個数に並ぶことはできない．つまり分母の p の個数は少なくとも 1 個は少ない．よって約分した結果，p が少なくとも一つ残る．式で表すと，

$$N_p({}_n\mathrm{C}_k) \geq \frac{p^i-1}{p-1} - \frac{p^i-2}{p-1} = \frac{1}{p-1} > 0$$

n が p のべきで表せないとき，$n = p^m + j$ とすると，

$${}_n\mathrm{C}_j = \frac{n!}{(p^m)!j!}$$

定理 6 より上式の分子に含まれるそいんすう p の個数は

$$N_p(n!) = \frac{p^m-1}{p-1} + N_p(j)$$

分母の p の個数も

$$N_p((p^m)!j!) = \frac{p^m-1}{p-1} + N_p(j)$$

n が p のべきで表せないとき $N_p({}_n\mathrm{C}_k) = 0$ となる k が存在する.　[証明おわり]
この証明の過程から次の定理が導けたことになる.

定理 7　$k < p^m$ のとき,

$$N_p({}_{p^m+k}\mathrm{C}_{p^m}) = 0$$

である.

定理 8　互いに素である自然数 a, b について，$a < b$ であるとき，$b - a$ と b も互いに素である.

[証明] $b - a$ と b が公約数 p をもつと仮定すると,

$$b - a = cp, b = dp$$

と書ける．二つの式より,

$$a = dp - cp = p(d - c)$$

と表せ，a, b が互いに素であることと矛盾する．よって $b - a$ と b も互いに素である.　[証明おわり]

定理 9　j, m を自然数とする．$j < p^m$ であるとき,

$$N_p(p^m - j) = N_p(j) \tag{1}$$

である.

[証明]

$$j = ap^i$$

とする．ただし，$0 \leq i < m$ で,a は p 以外の素因数の積である．$i = 0$ は j が素因数 p をもたないことを表す.
(1) の右辺は

$$N_p(j) = i$$

である．また,

$$p^m - j = p^m - ap^i = p^i(p^{m-i} - a)$$

と表せる．定理 8 より $p^{m-i} - a$ は p を約数にもたないので左辺も,

$$N_p(p^m - j) = i$$

$$\therefore N_p(p^m - j) = N_p(j)$$

[証明おわり]

定理 10　p を素数，m を自然数とすると，$1 \leqq k \leqq p^m - 1$ を満たすすべての自然数 k について

$$1 \leq N_p({}_{p^m}\mathrm{C}_k) \leq m$$

である.

[証明]

$$\begin{aligned} {}_{p^m}\mathrm{C}_k &= \frac{(p^m)!}{k!(p^m - k)!} \\ &= \frac{p^m(p^m - 1)(p^m - 2)\cdots\{p^m - (k-1)\}}{1 \cdot 2 \cdot 3 \cdots (k-1)k} \end{aligned}$$

定理 9 より

$$\begin{aligned} N_p({}_{p^m}\mathrm{C}_k) &= N_p\left(\frac{p^m(p^m-1)(p^m-2)\cdots\{p^m-(k-1)\}}{1\cdot 2\cdot 3\cdots(k-1)k}\right) \\ &= N_p\left(\frac{p^m}{k}\right) \\ &= N_p(p^m) - N_p(k) \\ &= m - N_p(k) \end{aligned}$$

明らかに,

$$0 \leq N_p(k) < m$$

であるので,

$$1 \leq N_p({}_{p^m}\mathrm{C}_k) \leq m$$

[証明おわり]

定理 11　p を素数，m を自然数とすると，$1 \leqq k \leqq p^m$ を満たすすべての自然数 k について

$$N_p(k \cdot_{p^m} \mathrm{C}_k) = m$$

である.

[証明] 定理 10 の証明の過程から

$$N_p({}_{p^m}\mathrm{C}_k) = m - N_p(k)$$

であるので，明らかである.　[証明おわり]

$k = p^m$ についてもこの定理は使える．$k = 0$ のときは使えない．パスカルの三角形の左端は使えないが右端は使える.

Maxima で $k \cdot_{2^5} \mathrm{C}_k$ を計算してみると，定理 11 の通りになっていることが観察できる.

```
(%i1) load(functs);
(%i2) for k:0 thru 2^5 do
print("&k=",k,"=",factor(k),"&&k*combination(2^5,k)=",factor(k*combination(2^5,k)),\\);
```

途中に入っている"&" や"\"の記号は TEX の行揃えや改行のためであって，Maxima のコマンドには関係がない.

$k = 0 = 0$	$k * combination(2^5, k) = 0$
$k = 1 = 1$	$k * combination(2^5, k) = 2^5$
$k = 2 = 2$	$k * combination(2^5, k) = 2^5 * 31$
$k = 3 = 3$	$k * combination(2^5, k) = 2^5 * 3 * 5 * 31$
$k = 4 = 2^2$	$k * combination(2^5, k) = 2^5 * 5 * 29 * 31$
$k = 5 = 5$	$k * combination(2^5, k) = 2^5 * 5 * 7 * 29 * 31$
$k = 6 = 2 * 3$	$k * combination(2^5, k) = 2^5 * 3^3 * 7 * 29 * 31$
$k = 7 = 7$	$k * combination(2^5, k) = 2^5 * 3^2 * 7 * 13 * 29 * 31$
$k = 8 = 2^3$	$k * combination(2^5, k) = 2^5 * 3^2 * 5^2 * 13 * 29 * 31$
$k = 9 = 3^2$	$k * combination(2^5, k) = 2^5 * 3^3 * 5^2 * 13 * 29 * 31$
$k = 10 = 2 * 5$	$k * combination(2^5, k) = 2^5 * 3 * 5^2 * 13 * 23 * 29 * 31$
$k = 11 = 11$	$k * combination(2^5, k) = 2^5 * 3 * 5 * 11 * 13 * 23 * 29 * 31$
$k = 12 = 2^2 * 3$	$k * combination(2^5, k) = 2^5 * 3^2 * 5 * 7 * 13 * 23 * 29 * 31$
$k = 13 = 13$	$k * combination(2^5, k) = 2^5 * 3 * 5^2 * 7 * 13 * 23 * 29 * 31$
$k = 14 = 2 * 7$	$k * combination(2^5, k) = 2^5 * 3 * 5^2 * 7 * 19 * 23 * 29 * 31$
$k = 15 = 3 * 5$	$k * combination(2^5, k) = 2^5 * 3^3 * 5^2 * 19 * 23 * 29 * 31$
$k = 16 = 2^4$	$k * combination(2^5, k) = 2^5 * 3^2 * 5 * 17 * 19 * 23 * 29 * 31$
$k = 17 = 17$	$k * combination(2^5, k) = 2^5 * 3^2 * 5 * 17 * 19 * 23 * 29 * 31$
$k = 18 = 2 * 3^2$	$k * combination(2^5, k) = 2^5 * 3^3 * 5^2 * 19 * 23 * 29 * 31$
$k = 19 = 19$	$k * combination(2^5, k) = 2^5 * 3 * 5^2 * 7 * 19 * 23 * 29 * 31$
$k = 20 = 2^2 * 5$	$k * combination(2^5, k) = 2^5 * 3 * 5^2 * 7 * 13 * 23 * 29 * 31$
$k = 21 = 3 * 7$	$k * combination(2^5, k) = 2^5 * 3^2 * 5 * 7 * 13 * 23 * 29 * 31$
$k = 22 = 2 * 11$	$k * combination(2^5, k) = 2^5 * 3 * 5 * 11 * 13 * 23 * 29 * 31$
$k = 23 = 23$	$k * combination(2^5, k) = 2^5 * 3 * 5^2 * 13 * 23 * 29 * 31$
$k = 24 = 2^3 * 3$	$k * combination(2^5, k) = 2^5 * 3^3 * 5^2 * 13 * 29 * 31$
$k = 25 = 5^2$	$k * combination(2^5, k) = 2^5 * 3^2 * 5^2 * 13 * 29 * 31$
$k = 26 = 2 * 13$	$k * combination(2^5, k) = 2^5 * 3^2 * 7 * 13 * 29 * 31$
$k = 27 = 3^3$	$k * combination(2^5, k) = 2^5 * 3^3 * 7 * 29 * 31$
$k = 28 = 2^2 * 7$	$k * combination(2^5, k) = 2^5 * 5 * 7 * 29 * 31$
$k = 29 = 29$	$k * combination(2^5, k) = 2^5 * 5 * 29 * 31$
$k = 30 = 2 * 3 * 5$	$k * combination(2^5, k) = 2^5 * 3 * 5 * 31$
$k = 31 = 31$	$k * combination(2^5, k) = 2^5 * 31$
$k = 32 = 2^5$	$k * combination(2^5, k) = 2^5$

この計算結果を見ると，最初の行を除いて上下対称になっているのがわかる．これは一般に，

$$k \cdot_n \mathrm{C}_k = n \cdot_{n-1} \mathrm{C}_{k-1}$$

であるために当然の結果であるのだが，このことから逆に次の定理が導ける．

定理 12　p を素数，m を自然数とすると，$0 \leqq k \leqq p^m - 1$ を満たすすべての自然数 k について

$$N_p({}_{p^m-1}\mathrm{C}_k) = 0$$

である．

このことを Maxima を用いて ${}_{2^6-1}\mathrm{C}_k$ の場合について調べてみると次のようになる．

```
(%i3) for k:0 thru 2^6/2-1 do
                  print("&combination(2^6-1,",k,")=",factor(combination(2^6-1,k)),\\);
```

$$combination(2^6-1,0)=1$$
$$combination(2^6-1,1)=3^2*7$$
$$combination(2^6-1,2)=3^2*7*31$$
$$combination(2^6-1,3)=3*7*31*61$$
$$combination(2^6-1,4)=3^2*5*7*31*61$$
$$combination(2^6-1,5)=3^2*7*31*59*61$$
$$combination(2^6-1,6)=3*7*29*31*59*61$$
$$combination(2^6-1,7)=3^2*19*29*31*59*61$$
$$combination(2^6-1,8)=3^2*7*19*29*31*59*61$$
$$combination(2^6-1,9)=5*7*11*19*29*31*59*61$$
$$combination(2^6-1,10)=3^3*7*11*19*29*31*59*61$$
$$combination(2^6-1,11)=3^3*7*19*29*31*53*59*61$$
$$combination(2^6-1,12)=3^2*7*13*19*29*31*53*59*61$$
$$combination(2^6-1,13)=3^3*7*17*19*29*31*53*59*61$$
$$combination(2^6-1,14)=3^3*5^2*17*19*29*31*53*59*61$$
$$combination(2^6-1,15)=3^2*5*7^2*17*19*29*31*53*59*61$$
$$combination(2^6-1,16)=3^3*5*7^2*17*19*29*31*53*59*61$$
$$combination(2^6-1,17)=3^3*5*7^2*19*29*31*47*53*59*61$$
$$combination(2^6-1,18)=3*5*7^2*19*23*29*31*47*53*59*61$$
$$combination(2^6-1,19)=3^3*5^2*7^2*23*29*31*47*53*59*61$$
$$combination(2^6-1,20)=3^3*5*7^2*11*23*29*31*47*53*59*61$$
$$combination(2^6-1,21)=3^2*5*7*11*23*29*31*43*47*53*59*61$$
$$combination(2^6-1,22)=3^3*5*7^2*23*29*31*43*47*53*59*61$$
$$combination(2^6-1,23)=3^3*5*7^2*29*31*41*43*47*53*59*61$$
$$combination(2^6-1,24)=3^2*5^2*7^2*29*31*41*43*47*53*59*61$$
$$combination(2^6-1,25)=3^3*7^2*13*29*31*41*43*47*53*59*61$$
$$combination(2^6-1,26)=3^3*7^2*19*29*31*41*43*47*53*59*61$$
$$combination(2^6-1,27)=7^2*19*29*31*37*41*43*47*53*59*61$$
$$combination(2^6-1,28)=3^2*7*19*29*31*37*41*43*47*53*59*61$$
$$combination(2^6-1,29)=3^2*5*7^2*19*31*37*41*43*47*53*59*61$$
$$combination(2^6-1,30)=3*7^2*17*19*31*37*41*43*47*53*59*61$$
$$combination(2^6-1,31)=3^2*7^2*11*17*19*37*41*43*47*53*59*61$$

また，定理 12 が成り立っていることは ${}_{5^2-1}\mathrm{C}_k$ の末尾に 0 が全くつかないことからも観察できる．

```
(%i4)
for k:0 thru 12 do print("&combination(24,",k,")=",
                         factor(combination(5^2-1,k)),"=",combination(5^2-1,k),"\\");
```

$$
\begin{aligned}
&combination(24,0) = 1 = 1\\
&combination(24,1) = 2^3 * 3 = 24\\
&combination(24,2) = 2^2 * 3 * 23 = 276\\
&combination(24,3) = 2^3 * 11 * 23 = 2024\\
&combination(24,4) = 2 * 3 * 7 * 11 * 23 = 10626\\
&combination(24,5) = 2^3 * 3 * 7 * 11 * 23 = 42504\\
&combination(24,6) = 2^2 * 7 * 11 * 19 * 23 = 134596\\
&combination(24,7) = 2^3 * 3^2 * 11 * 19 * 23 = 346104\\
&combination(24,8) = 3^2 * 11 * 17 * 19 * 23 = 735471\\
&combination(24,9) = 2^4 * 11 * 17 * 19 * 23 = 1307504\\
&combination(24,10) = 2^3 * 3 * 11 * 17 * 19 * 23 = 1961256\\
&combination(24,11) = 2^4 * 3 * 7 * 17 * 19 * 23 = 2496144\\
&combination(24,12) = 2^2 * 7 * 13 * 17 * 19 * 23 = 2704156
\end{aligned}
$$

よく見ると ${}_{24}\mathrm{C}_7$ には素因数 7 が無く,${}_{24}\mathrm{C}_8$,${}_{24}\mathrm{C}_9$,${}_{24}\mathrm{C}_{11}$ にはそれぞれ 2,3,11 が無い．これは定理 7 から当然のことである．
これらのことから次の定理が容易に導け，さらにそれを使ってフェルマーの小定理を導くこともできる．

定理 13 （ライプニッツの公式）任意の整数 a, b に対して

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

が成り立つ．さらに

$$(a_1 + a_2 + a_3 + \cdots + a_n)^p \equiv a_1^p + a_2^p + a_3^p + \cdots + a_n^p \pmod{p}$$

が成り立つ．

[証明略]

定理 14 （フェルマーの小定理）p の倍数でない整数 a に対して

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

が成り立つ．

[証明略]

参考文献

[1] 小林昭七『なっとくするオイラーとフェルマー』（講談社，2003 年）