着眼点

この問題は，ガウス記号や ord という指数の関数の性質を使って，二項係数 ${}_N\mathrm{C}_r$ が整数となることの別証明と，素数（べき）で割った余りを考える際，ある素数に着目し，その素因数を除いたものを議論するという見方が要求されます。この方法はあまり見られないものなので，勉強になったかと思います。

解答例

(1)　$a=[a]+a'$， $b=[b]+b'$ と表すと， $0\leqq a'<1$， $0\leqq b'<1$ 。このとき，

$$[a+b]=[[a]+a'+[b]+b']=[a]+[b]+[a'+b']$$

ここで， $0\leqq a'$， $0\leqq b'$ より $0\leqq a'+b'$，つまり， $0\leqq[a'+b']$。したがって，

$$[a+b]\geqq[a]+[b]$$

が成り立つ。

(2)　k を自然数とするとき，条件より $\left[\dfrac{N}{p^k}\right]$ は 1 から N までの自然数の中で p^k の倍数であるものの個数を示している。

一方， p^{k+1} の倍数でない p^k の倍数には，素因数 p はちょうど k 個あり，その k 個は $\left[\dfrac{N}{p}\right]$， $\left[\dfrac{N}{p^2}\right]$，…， $\left[\dfrac{N}{p^k}\right]$ の中に 1 つずつ数えられている。したがって

$$\mathrm{ord}_pN!=\left[\frac{N}{p}\right]+\left[\frac{N}{p^2}\right]+\cdots$$

が成り立つ。

(3)　${}_N\mathrm{C}_r$ の定義より ${}_N\mathrm{C}_r=\dfrac{N!}{r!(N-r)!}$ である。

$k=0$ のとき，定義から $0!=1$ となって成り立つ。

$k\neq 0$ のとき，(2)より素数 p に対して

$$\mathrm{ord}_pN!=\left[\frac{N}{p}\right]+\left[\frac{N}{p^2}\right]+\cdots$$

$$\mathrm{ord}_pr!=\left[\frac{r}{p}\right]+\left[\frac{r}{p^2}\right]+\cdots$$

$$\mathrm{ord}_p(N-r)!=\left[\frac{N-r}{p}\right]+\left[\frac{N-r}{p^2}\right]+\cdots$$

であり，自然数 m に対して $\dfrac{N}{p^m}=\dfrac{r}{p^m}+\dfrac{N-r}{p^m}$ であるから，(1)より，

$$\left[\frac{N}{p^m}\right]\geqq\left[\frac{r}{p^m}\right]+\left[\frac{N-r}{p^m}\right]$$

したがって

$$\mathrm{ord}_pN!\geqq\mathrm{ord}_pr!+\mathrm{ord}_p(N-r)!$$

これはすべての素数 p で成り立つので， $N!$ は $r!(N-r)!$ の倍数，つまり，

${}_NC_r=\dfrac{N!}{r!(N-r)!}$ は整数である。

(4) $\mathrm{ord}_p\,{}_{2pN}\mathrm{C}_{pN}=\mathrm{ord}_p\dfrac{(2pN)!}{(pN)!(pN)!}$

$$=\mathrm{ord}_p(2pN)!-2\cdot\mathrm{ord}_p(pN)!$$
$$=\left[\frac{2pN}{p}\right]+\left[\frac{2pN}{p^2}\right]+\left[\frac{2pN}{p^3}\right]+\cdots-2\left(\left[\frac{pN}{p}\right]+\left[\frac{pN}{p^2}\right]+\left[\frac{pN}{p^3}\right]+\cdots\right)$$
$$=[2N]+\left[\frac{2N}{p}\right]+\left[\frac{2N}{p^2}\right]+\cdots-2\left([N]+\left[\frac{N}{p}\right]+\left[\frac{N}{p^2}\right]+\cdots\right)$$
$$=2N+\left[\frac{2N}{p}\right]+\left[\frac{2N}{p^2}\right]+\cdots-2N-2\left(\left[\frac{N}{p}\right]+\left[\frac{N}{p^2}\right]+\cdots\right)$$
$$=\left[\frac{2N}{p}\right]+\left[\frac{2N}{p^2}\right]+\cdots-2\left(\left[\frac{N}{p}\right]+\left[\frac{N}{p^2}\right]+\cdots\right)$$
$$=\mathrm{ord}_p(2N)!-2\cdot\mathrm{ord}_pN!$$
$$=\mathrm{ord}_p\,{}_{2N}\mathrm{C}_N$$

(5) $${}_{2N}\mathrm{C}_N=\frac{(2N)!}{N!N!}=2\cdot\frac{(2N-1)!}{(N-1)!N!}=2\cdot{}_{2N-1}\mathrm{C}_N$$

と表せる。ここで，(3)より ${}_{2N-1}\mathrm{C}_N$ は整数なので $\mathrm{ord}_2\,{}_{2N-1}\mathrm{C}_N\geqq 0$ 。したがって，

$$\mathrm{ord}_2\,{}_{2N}\mathrm{C}_N=\mathrm{ord}_2 2+\mathrm{ord}_2\,{}_{2N-1}\mathrm{C}_N\geqq 1$$

次に， $\mathrm{ord}_p\,{}_{2N}\mathrm{C}_N=1$ について，

$$\mathrm{ord}_2(2N)!-2\cdot\mathrm{ord}_2N!=\left[\frac{2N}{2}\right]+\left[\frac{2N}{2^2}\right]+\cdots-2\left(\left[\frac{N}{2}\right]+\left[\frac{N}{2^2}\right]+\cdots\right)$$
$$=\left(\left[\frac{2N}{2}\right]-2\cdot\left[\frac{N}{2}\right]\right)+\left(\left[\frac{2N}{2^2}\right]-2\cdot\left[\frac{N}{2^2}\right]\right)+\cdots$$

ここで，(4)の性質より N は奇数として考えてよいので， $N=2m+1$ （ m は自然数）とおくと，式の一番左の（　）の中は，

$$\left[\frac{2N}{2}\right]-2\cdot\left[\frac{N}{2}\right]=\left[\frac{2(2m+1)}{2}\right]-2\cdot\left[\frac{2m+1}{2}\right]=(2m+1)-2m=1$$

であり，条件を満たすには残りの（　）の中がすべて 0，つまり，すべての自然数 k において， $\left[\dfrac{N}{2^k}\right]$ が偶数となる。

これは， N を 2 進数展開したとき，一の位以外すべて 0 となることを意味しているので， $N=1$ 。

以上より，(4)から N は 2 のべき乗となる。

(6) 条件より k を自然数として， $N=2^k$ と表せる。

$k\geqq 3$ のとき， 1 から 2^k までの自然数の総乗から 2 の指数をすべて割って除き，それらを 8 で割った余りをみると， 1，3，5，7 の 4 種類が現れる。

これらのうち，元の数において奇数であるところや 2 の倍数からなるところ，…， 2^{k-3} の倍数からなるところでは， 1，3，5，7 が同じ数だけ現れる。

一方， 2^{k-2} の倍数からなるものには 1，3 が 1 つずつ現れ， 2^{k-1} の倍数， 2^k の倍数からなるものには 1 のみ現れる。

ここで，$1\cdot3\cdot5\cdot7\equiv1 \pmod 8$ であるので，$(2^k)!$ から2の指数をすべて割って除き，それらを8で割った余りは k の値によらず，$1\cdot3\equiv3 \pmod 8$ となる。

このことから，${}_{2N}\mathrm{C}_N=\dfrac{(2N)!}{N!N!}$ の分子および分母をそれぞれ2の指数をすべて割って除き，それらを8で割った余りについて考えると，分子は1，3，5，7の組いくつかと，1，3の組が2つ，5，7の組が1つあり，分母は1，3，5，7の組いくつかと1，3の組が2つある。

したがって，(5)より $\mathrm{ord}_2\,{}_{2N}\mathrm{C}_N=1$ から $\dfrac{{}_{2N}\mathrm{C}_N}{2}\equiv5\cdot7\equiv3 \pmod 8$。

すなわち，${}_{2N}\mathrm{C}_N\equiv2\cdot3\equiv6 \pmod 8$ より，求める余りは6。

$\boxed{\text{コメント}}$

本問の後半は，Wolstenholmeの定理

n が奇素数のとき，${}_{2n-1}\mathrm{C}_n$ は n^3 で割ると余りが1となる

の逆についての一部証明となっており，逆自体は未解決問題です。本問では，n が偶数のとき，逆が成立しないことを意味しています。

なお，この定理の逆が証明されると，素数を表す多項式で知られるMatiyasevich多項式（19変数）が7変数に改良できるようです。