m を正の整数とするとき，次の問いに答えよ。

(1)　二項係数の和 ${}_mC_0+{}_mC_1+{}_mC_2+\cdots\cdots+{}_mC_{n-1}+{}_mC_m$ を求めよ。

(2)　m が素数であるとき，$1\leqq k\leqq m-1$ を満たす整数 k に対して，${}_mC_k$ は m の倍数であることを示せ。

(3)　m が素数であるとき，2^m-2 は m の倍数であることを示せ。

＜ '11 関西大 ＞

【戦略】

(1) はコンビネーションの $\sum$ ですから，二項定理をインスピレーションします。

(2) は $k\,{}_mC_k=m\,{}_{m-1}C_{k-1}$ が常識になっているかどうかで決まります。

常識になっていれば「証明」スタイルになりますので，左辺，右辺を計算して一致することを確認すればよいです。

もし，常識になっていなければ，ひとまずは ${}_mC_k=m\times$(整数) という形を目指すことになります。

コンビネーションを階乗を用いて書き下すと

${}_mC_k=\dfrac{m!}{k!(m-k)!}$ **であり，ここから m を取り出すことを考えると**

${}_mC_k=m\cdot\dfrac{(m-1)!}{k!(m-k)!}$ **となります。**

この形を見て，先ほどの目論見である ${}_mC_k=m\times$(整数) の (整数) の部分が階乗型の分数である ${}_{\bigcirc}C_{\triangle}$ の形に似ていることを皮切りに，${}_{\bigcirc}C_{\triangle}$ の形を登場させよう登場させようという意識をもてば

$$\begin{aligned}{}_mC_k&=\frac{m!}{k!(m-k)!}\\&=\frac{m}{k}\cdot\frac{(m-1)!}{(k-1)!\{(m-1)-(k-1)\}!}\\&=\frac{m}{k}\cdot{}_{m-1}C_{k-1}\end{aligned}$$

となります。

当初の目論見である ${}_mC_k=m\times$(整数) ではありませんが，分母を払えば

$k\,{}_mC_k=m\,{}_{m-1}C_{k-1}$ **を得ることになります。**

m が素数という条件はここから効いてきます。

$k\,{}_mC_k=m\,{}_{m-1}C_{k-1}$ **から，$k\,{}_mC_k$ が m の倍数となりますが，m が素数であれば，$k=1,2,\cdots,m-1$ とは互いに素ですから ${}_mC_k$ が m の倍数となるしかありません。**

(3) がこの問題のオチですが，(1) から

$2^m-2={}_mC_0+{}_mC_1+\cdots\cdots+{}_mC_{m-1}+{}_mC_m-2$ **と見て，-2 という部分は ${}_mC_0+{}_mC_m$ を消してくれるため**

$2^m-2={}_mC_1+\cdots\cdots+{}_mC_{m-1}$ **となり，(2) から各項が m の倍数と言えるので解決です。**

【解答】

(1)　二項定理より，$(1+x)^m={}_mC_0+{}_mC_1x+{}_mC_2x^2+\cdots\cdots+{}_mC_mx^m$

よって，$x=1$ を代入して，${}_mC_0+{}_mC_1+\cdots\cdots+{}_mC_m=2^m$ … 答

(2)　m が素数であるとき，

m と k $(1\leqq k\leqq m-1)$ は互いに素である．… ①

$$\begin{aligned}{}_mC_k&=\frac{m!}{k!(m-k)!}\\&=\frac{m}{k}\cdot\frac{(m-1)!}{(k-1)!\{(m-1)-(k-1)\}!}\\&=\frac{m}{k}\cdot{}_{m-1}C_{k-1}\end{aligned}$$

よって，$k\,{}_mC_k=m\,{}_{m-1}C_{k-1}$

左辺は m の倍数であるが，① より ${}_mC_k$ が m の倍数とならなければならない。

よって題意は示された。

(3)　$\begin{aligned}2^m-2&={}_mC_0+{}_mC_1+\cdots\cdots+{}_mC_{m-1}+{}_mC_m-2\\&={}_mC_1+{}_mC_2+\cdots\cdots+{}_mC_{m-1}\\&=(m\text{ の倍数})\quad(\because(2))\end{aligned}$

で題意は示された。

【総括】

フェルマーの小定理

p を素数とするとき，任意の自然数 a に対して

$$a^p \equiv a \ (\mathrm{mod}\ p) \cdots (*)$$

が成り立つ。

がオチで，多くの大学で出題されています。

さらに

a と p が互いに素であるとき

$$a^{p-1} \equiv 1 \ (\mathrm{mod}\ p) \cdots (**)$$

が成り立つ

ということが言えます。

【証明】～数学的帰納法～

以下，合同式における法は p であるとする。

(i)　$a=1$ のとき $1^p \equiv 1$ より，$(*)$ は成り立つ。

(ii)　$a=k$ $(k=1, 2, \cdots)$ のとき $k^p \equiv k$ であると仮定する。

$$\begin{aligned}(k+1)^p &= k^p + {}_pC_1 + {}_pC_2 + \cdots + {}_pC_{p-1} + 1 \\ &\equiv k^p + 1 \quad (\because \text{本問(2)の結果から } {}_pC_i \equiv 0) \\ &\equiv k + 1 \quad (\because \text{帰納法の仮定})\end{aligned}$$

となり，$a=k+1$ のときも $(*)$ は成り立つ。

(i)，(ii) より，$(*)$ が成り立つ。

また，$(*)$ より $a(a^{p-1}-1) \equiv 0$ だから，$a(a^{p-1}-1) = pK$ (K は整数)

と表せるため，$a(a^{p-1}-1)$ は p の倍数である。

a と p が互いに素のとき，$a^{p-1}-1$ が p の倍数とならなければならない。

ゆえに，$a^{p-1}-1 \equiv 0$，すなわち $a^{p-1} \equiv 1$ が成り立つため，$(**)$ が成り立つことが示された。

【証明その２】

補題

a と p が互いに素であるとき，

$$a,\ 2a,\ 3a,\ \cdots,\ (p-1)a$$

という $p-1$ 個の数を p で割った余りは異なる

<補題の証明>

以下，合同式における法は p であるとする。

$ka \equiv \ell a$ $(1 \leqq k < \ell \leqq p-1)$ を満たす自然数 k，ℓ が存在すると仮定する。

このとき，$(\ell - k)a \equiv 0$

これより $(\ell - k)a = pN$ (N は整数) と表すことができる

したがって，$(\ell - k)a$ は p の倍数であるが，a，p は互いに素であるので，$\ell - k$ が p の倍数となる。

ゆえに，$\ell - k \equiv 0$，すなわち $\ell \equiv k$

$1 \leqq k < \ell \leqq p-1$ であることに注意すると，$\ell = k$ となるしかないが，これは k，ℓ が異なる自然数であることに反する。

<$(**)$ の証明>

a，$2a$，$3a$，$\cdots$，$(p-1)a$ は全て p と互いに素である。

ゆえに，a，$2a$，$3a$，$\cdots$，$(p-1)a$ を p で割った余りは 0 ではない。

a，$2a$，$3a$，$\cdots$，$(p-1)a$ を p で割った余りをそれぞれ

$$r_1,\ r_2,\ r_3,\ \cdots,\ r_{p-1}$$

とする

補題より

集合 $\{r_1, r_2, r_3, \cdots, r_{p-1}\} = \{1, 2, 3, \cdots, p-1\}$ は一致する。

ゆえに，これらの積を考えると

$$r_1 r_2 r_3 \cdots\cdots r_{p-1} = (p-1)!$$

よって，$a \times (2a) \times (3a) \times \cdots \times \{(p-1)a\} \equiv r_1 r_2 r_3 \cdots\cdots r_{p-1}$

ゆえに，$(p-1)!\, a^{p-1} \equiv (p-1)!$

$(p-1)!(a^{p-1}-1) \equiv 0$ であり，$(p-1)!(a^{p-1}-1) = pM$ (M は整数)

p は素数ゆえ，p と $(p-1)!$ は互いに素であるから

$a^{p-1}-1$ が p の倍数となるので，$a^{p-1}-1 \equiv 0$，すなわち $a^{p-1} \equiv 1$ が成り立つため，$(**)$ が成り立つことが示された。

これを拡張した「オイラーの定理」というものも有名です。

オイラーの定理

n と互いに素である整数 a を考えるとき，

$$a^{\varphi(n)} \equiv 1 \pmod{n} \cdots (***)$$

が成り立つ。

注意：$\varphi(n)$ とは $1, 2, \cdots, n$ のうち n と互いに素であるものの個数

【証明】

簡単のため，$\varphi(n)=k$ とおく。

また，以下における合同式の法は n とする。

$1, 2, 3, \cdots, n$ のうち，n と互いに素であるものは k 個あり，

それらを小さいほうから順に $x_1, x_2, \cdots, x_k$ とする。

補題

$x_1a, x_2a, x_3a, \cdots, x_ka$ を n で割った余りは全て異なる。

＜補題の証明＞

$x_ka \equiv x_\ell a$ となる $1 \leqq k < \ell \leqq k$ を満たす整数 k, ℓ が存在すると仮定する。

このとき，$(x_\ell - x_k)a \equiv 0$ であり，$(x_\ell - x_k)a = nM$（M は整数）と表せる。

a と n は互いに素であるため，$x_\ell - x_k$ が n の倍数となる必要がある。

ゆえに $x_\ell - x_k \equiv 0$，すなわち $x_\ell \equiv x_k$

x_ℓ, x_k は $1, 2, \cdots, n-1$ のいずれかであること，及び

x_ℓ, x_k を n で割った余りが等しいということを考えると

$$x_\ell = x_k$$

一方，小さいほうから $x_1, x_2, \cdots, x_k$ としていたのだから $x_k < x_\ell$ であり，矛盾する。

＜(***)の証明＞

a と n は条件から互いに素であり，

$x_1, x_2, \cdots, x_k$ は n と互いに素であるものと定めたため

$x_1a, x_2a, x_3a, \cdots, x_ka$ は全て n と互いに素である。

$x_1a, x_2a, x_3a, \cdots, x_ka$ を n で割った余りをそれぞれ

$r_1, r_2, \cdots, r_k$ とする。

この $r_1, r_2, \cdots, r_k$ は全て n と互いに素である。…(☆)

なぜなら，$r_i\ (1 \leqq i \leqq k)$ と n が互いに素でないと仮定すると，

r_i と n の共通素因数 p が存在し，M_i を整数として，$r_i = pM_i$ と表せる。

このとき，整数 Q_i を用いて $ax_i = nQ_i + r_i$ と表せるため，
$ax_i = nQ_i + pM_i$

r_i と n の共通素因数を p としているため，ax_i も素因数 p をもつことになり，a か x_i のどちらかが素因数 p をもつことになり，どちらにしても a，x_i がともに n と互いに素であることに矛盾する。

このことから，

集合 $\{x_1, x_2, \cdots, x_k\}$ は n 未満で n と互いに素である整数全てを要素にもつ集合

一方，補題，及び(☆)より

$k\ (=\varphi(n))$ **個という時点で「全て」と言えます。**

集合 $\{r_1, r_2, \cdots, r_k\}$ は n 未満で n と互いに素である整数全てを要素にもつ集合

ゆえに，集合として

$$\{x_1, x_2, \cdots, x_k\} = \{r_1, r_2, \cdots, r_k\}$$

であり，

$$(x_1a)(x_2a)\cdots(x_ka) \equiv r_1r_2\cdots r_k$$

$$a^k x_1x_2\cdots x_k \equiv x_1x_2\cdots x_k$$

$x_1x_2\cdots x_n$ は n と互いに素であるから，$a^k \equiv 1$

よって $a^{\varphi(n)} \equiv 1 \pmod{n}$ が示された。

心配しなくても入試であれば何らかの誘導がつくはずです。

ただ，ある程度のシナリオは経験しておいた方が安心はできると思います。

【復習用問題】

次の問いに答えよ。
ただし，正の整数 n と整数 k（$0 \leqq k \leqq n$）に対して，${}_nC_k$ が正の整数である事実を使ってよい。

(1) m が 2 以上の整数のとき，${}_mC_2$ が m で割り切れるための必要十分条件を求めよ。

(2) p を 2 以上の素数とし，k を p より小さい正の整数とする。このとき，${}_pC_k$ は p で割り切れることを示せ。

(3) p を 2 以上の素数とする。このとき，任意の正の整数 n に対し，

$$(n+1)^p - n^p - 1$$

は p で割り切れることを示せ。

＜ '06 早稲田大 ＞

【復習用問題　解答】

(1) $\dfrac{{}_mC_2}{m} = \dfrac{m-1}{2}$ が整数となるための必要十分条件は $m-1$ が偶数，

すなわち

m が奇数であること …㊀

(2)

$$\begin{aligned} {}_pC_k &= \frac{p!}{k!\,(p-k)!} \\ &= \frac{p}{k} \cdot \frac{(p-1)!}{(k-1)!\,\{(p-1)-(k-1)\}!} \\ &= \frac{p}{k} \cdot {}_{p-1}C_{k-1} \end{aligned}$$

これより，$k\,{}_pC_k = p\,{}_{p-1}C_{k-1}$

右辺は p の倍数なので，左辺も p の倍数。

p は素数なので，p，k（$=1, 2, \cdots, p-1$）は互いに素である。

よって，${}_pC_k$ が p の倍数であり，${}_pC_k$ は p で割り切れる。… ㊇

(3) $$\begin{aligned} (n+1)^p - n^p - 1 &= {}_pC_1 n + {}_pC_2 n^2 + \cdots + {}_pC_{p-1} n^{p-1} \\ &= pk_1 + pk_2 + \cdots + pk_{p-1} \quad (k_1 \sim k_{p-1} \text{は整数}) \\ &= p\,(k_1 + k_2 + \cdots + k_{p-1}) \end{aligned}$$

と表せる。（∵ (2) の結果）

ゆえに，$(n+1)^p - n^p - 1$ は p で割り切れる。… ㊇

【復習用問題２】

p は素数，r は正の整数とする。以下の問いに答えよ。

(1) $x_1, x_2, \cdots, x_r$ についての式 $(x_1+x_2+\cdots+x_r)^p$ を展開したときの ${x_1}^{p_1}{x_2}^{p_2}\cdots{x_r}^{p_r}$ の係数を求めよ。ここで，$p_1, p_2, \cdots, p_r$ は 0 または正の整数で，$p_1+p_2+\cdots+p_r=p$ を満たすとする。

(2) $x_1, x_2, \cdots, x_r$ が正の整数のとき，

$$(x_1+x_2+\cdots+x_r)^p - (x_1^p + x_2^p + \cdots + x_r^p)$$

は p で割り切れることを示せ。

(3) r は p で割り切れないとする。このとき，$r^{p-1}-1$ は p で割り切れることを示せ。

＜ '10 大阪大 ＞

【復習用問題２　解答】

(1) $(x_1+x_2+\cdots+x_r)^p$ を展開したときの ${x_1}^{p_1}{x_2}^{p_2}\cdots{x_r}^{p_r}$ の係数は

$$\frac{p!}{p_1!p_2!\cdots p_r!} \quad \cdots ㊀$$

(2) $(x_1+x_2+\cdots+x_r)^p - (x_1^p + x_2^p + \cdots + x_r^p)$ を展開したときに現れる一般項は

$$\frac{p!}{p_1!p_2!\cdots p_r!}\,{x_1}^{p_1}{x_2}^{p_2}\cdots{x_r}^{p_r} \quad (p_1+p_2+\cdots+p_r=p)$$

ただし，$0 \leqq p_k \leqq p-1$（$k=1, 2, \cdots, r$）

${x_1}^p, {x_2}^p, \cdots, {x_r}^p$ **の項はないので，p はあり得ません。**

$a = \dfrac{p!}{p_1!p_2!\cdots p_r!}$ とおくと，$a \cdot p_1! \cdot p_2! \cdot \cdots p_r! = p(p-1)!$

左辺は素数 p の倍数となるが，$0 \leqq p_k \leqq p-1$（$k=1, 2, \cdots, r$）より，p_k（$k=1, 2, \cdots, r$）は p と互いに素

当然，$p_k!$（$k=1, 2, \cdots, r$）も p と互いに素。

したがって，a が p の倍数となり，

$$(x_1+x_2+\cdots+x_r)^p - (x_1^p + x_2^p + \cdots + x_r^p)$$

を展開したときに現れる一般項の係数が p で割り切れる。

ゆえに，$(x_1+x_2+\cdots+x_r)^p - (x_1^p + x_2^p + \cdots + x_r^p)$ は p で割り切れる。

(3) $x_1 = x_2 = \cdots = x_r = 1$ のとき

$$\begin{aligned} (x_1+x_2+\cdots+x_r)^p - (x_1^p + x_2^p + \cdots + x_r^p) &= r^p - r \\ &= r\,(r^{p-1}-1) \end{aligned}$$

これは (2) の結果から p で割り切れる。

r が p で割り切れないとき，$r^{p-1}-1$ が p で割り切れることになり，題意は示された。