数チャレ 第267回(2023年4月)

pは素数とする．次の問いに答えよ．

問1　jを$0<j<p$である整数とすると，二項係数${}_p\mathrm{C}_j$はpで割り切れることを示せ．

問2　自然数mに対して$(m+1)^p-m^p-1$はpで割り切れることを示せ．

問3　自然数mに対してm^p-mはpで割り切れることを示せ．さらにmがpで割り切れないときには，$m^{p-1}-1$がpで割り切れることを示せ．

ここで，次の集合Sを考える．

$$S=\{4n^2+4n-1 \mid n\text{は自然数}\}$$

例えば，$n=22$とすると$4n^2+4n-1=2023$なので2023はSに属する．
次の問いに答えよ．

問4　整数aがSに属し，$a=4n^2+4n-1$ (nは自然数) と表されているとする．このとき，aと$2n+1$は互いに素であることを示せ．

問5　pは3以上の素数とする．pがSに属するある整数aを割り切るならば，$2^{\frac{p-1}{2}}-1$はpで割り切れることを示せ．

出典：2023年 大阪公立大学 理系

解答

問1

$${}_p\mathrm{C}_j=\frac{p}{j}{}_{p-1}\mathrm{C}_{j-1}$$

および${}_{p-1}\mathrm{C}_{j-1}$は整数であるから

$p\cdot{}_{p-1}\mathrm{C}_{j-1}$は$j$で割り切れる。

$0<j<p$ (pは素数)であることより，pとjは互いに素であり，${}_{p-1}\mathrm{C}_{j-1}$がjで割り切れ，

$\dfrac{{}_{p-1}\mathrm{C}_{j-1}}{j}$は整数

である。よって，${}_p\mathrm{C}_j=p\cdot\dfrac{{}_{p-1}\mathrm{C}_{j-1}}{j}$は$p$で割り切れる。

(証明おわり)

ⓒ早稲田数学フォーラム

問 2　二項定理より

$$(m+1)^p - m^p - 1 = \sum_{j=1}^{p-1} {}_p\mathrm{C}_j\, m^j$$

であるから，問 1 より p で割り切れる。　(証明おわり)

問 3　$m^p - m$ が p で割り切れることを(自然数 m についての)数学的帰納法で示す。

1°　$m=1$ のとき，$1^p - 1 = 0$ は p で割り切れる。

2°　$m^p - m$ が p で割り切れるとすれば，問 2 より

$$(m+1)^p - (m+1) = (m+1)^p - m^p - 1 + m^p - m$$

も p で割り切れる。

$1^\circ, 2^\circ$ より，すべての自然数 m に対して $m^p - m$ は p で割り切れる。

p は素数であるから，m が p で割り切れないときは m と p は互いに素であり，$m^p - m = m(m^{p-1} - 1)$ が p で割り切れることより $m^{p-1} - 1$ は p で割り切れる。

(証明おわり)

問 4　$4n^2 + 4n - 1 = (2n+1)^2 - 2$ より

$$gcd(4n^2 + 4n - 1,\ 2n+1) = gcd(2n+1,\ 2)$$

$2n+1$ は奇数であるから

$$gcd(2n+1,\ 2) = 1$$

であり，$4n^2 + 4n - 1$ と $2n+1$ は互いに素である。　(証明おわり)

問 5　素数 p が S に属するある整数 a を割り切るならば，

$$4n^2 + 4n - 1 \equiv 0 \pmod{p}$$

を満たす自然数 n が存在する。$4n^2 + 4n - 1 = (2n+1)^2 - 2$ であるから

$$2 \equiv (2n+1)^2 \pmod{p}$$

問 4 より $2n+1$ は p で割り切れないから，問 3 より

$$(2n+1)^{p-1} \equiv 0 \pmod{p}$$

よって，

$$2^{\frac{p-1}{2}} \equiv \left\{(2n+1)^2\right\}^{\frac{p-1}{2}} \equiv (2n+1)^2 \equiv 1 \pmod{p}$$

が成り立ち，$2^{\frac{p-1}{2}} - 1$ は p で割り切れる。　(証明おわり)

(注)　S の要素 $4n^2 + 4n - 1$ はすべて奇数であるから，仮定 $p \neq 2$ は不要である。

(参考)　専門的な整数論によると，奇素数 p に対して

$$p \text{ を法として 2 が平方剰余} \iff p \equiv 1 \text{ または } 7 \pmod{8}$$

であることが知られているので，本問の問 5 により

S に属する整数の素因数 p は $p \equiv 1$ または $7 \pmod{8}$ に限られる

ことになる。

ⓒ 早稲田数学フォーラム