☆二項定理

$$(a+b)^n = {}_nC_0 a^n + {}_nC_1 a^{n-1}b + \cdots + {}_nC_{n-1} a b^{n-1} + {}_nC_n b^n$$

☆二項係数

$${}_nC_k = \frac{n!}{(n-k)!k!} = \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 2\cdot 1}$$

↳ 本問とは関係ないものの、大事な性質があるので、okkeで確認！（「Cの性質」）

(1) 二項定理より、

$$(a+b)^p - a^p - b^p$$
$$= {}_pC_1 a^{p-1}b + {}_pC_2 a^{p-2}b^2 + \cdots + {}_pC_{p-2} a^2 b^{p-2} + {}_pC_{p-1} a b^{p-1} \quad \cdots ①$$

ここで、kを $1 \leqq k \leqq p-1$ を満たす整数として、

$${}_pC_k = \frac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots 2\cdot 1}$$ を考える。

pは素数ゆえ、$1 \sim k$ は p と共通な素因数を持たず、また ${}_pC_k$ は整数なので、

pコからkコを選ぶ場合の数と考えて、自明

${}_pC_k$ は p で割り切れる。

a, b は整数ゆえ、① の右辺の各項が p で割り切れることになり、

$(a+b)^p - a^p - b^p$ は p で割り切れる。□

(2) (1)を使うというよりも、同じ考え方で示せそうな気配がする。

(1)と同様にして、二項定理より

$$(a+2)^p - a^p$$
$$= {}_pC_1 a^{p-1}\cdot 2 + {}_pC_2 a^{p-2} 2^2 + \cdots + {}_pC_{p-1} a\cdot 2^{p-1} + 2^p$$

ここで、${}_pC_1 \sim {}_pC_{p-1}$ は整数、

aも整数ゆえ、右辺の各項は偶数となる。

よって $(a+2)^p - a^p$ は偶数である。

(3) (1) → pで割った
(2) → 2で割った
ミックスすればいけそう。

(2)と同様に、

$$(a+2)^p - a^p$$
$$= {}_pC_1 a^{p-1}\cdot 2 + {}_pC_2 a^{p-2} 2^2 + \cdots + {}_pC_{p-1} a\cdot 2^{p-1} + 2^p \quad \cdots②$$

これを$2p$で割った余りを考える。

(1)で示したことより、$b=2$とおくと、

$(a+2)^p - a^p - 2^p$ は p で割り切れる。

展開して、

$${}_pC_1 a^{p-1}\cdot 2 + {}_pC_2 a^{p-2}\cdot 2^2 + \cdots + {}_pC_{p-2} a^2\cdot 2^{p-2} + {}_pC_{p-1} a\cdot 2^{p-1}$$

はpで割り切れる。 $\cdots③$

よって②の右辺、つまり

$${}_pC_1 a^{p-1}\cdot 2 + {}_pC_2 a^{p-2} 2^2 + \cdots + {}_pC_{p-1} a\cdot 2^{p-1} + 2^p$$ について

↳ ここまで p で割り切れる。

(2)の議論より 第 $p-1$ 項までの和は偶数、かつ③より p で割り切れる。…④

→ ここで $2p$ で割り切れるとは言い切れない。2と p は互いに素ではないケースがある!! よって場合分けが生じる。

ここで、2と p が互いに素になるかどうかについて場合分けを行う。

(i) $p=2$ のとき、

$(a+2)^2-a^2=4a+4$ となり、

$2p$、つまり4の倍数となるので求める余りは $\underline{0}$。

(ii) $p \geqq 3$ のとき、p と2は互いに素なので、④より②の右辺の第 $p-1$ 項までの和は $2p$ で割り切れる。

よって $(a+2)^p-a^p$ を $2p$ で割った余りは 2^p を $2p$ で割った余りに等しい。

以下これを求める。→ 実験してあたりを付ける。

☆問題をシンプル化!

※フェルマーの小定理を知っているとラクに答えが求まるので、最後に。

p	3	5	7
$2p$	6	10	14
2^p	8	32	128
余り	2	2	2

→ 2っぽい!!

2^pを$2p$で割った余り → pは素数だし、帰納法もうまくいかなさそう。

↓

(1)(2)の流れをくんで、二項定理で!

$$2^p = (1+1)^p$$
$$= {}_pC_0 + {}_pC_1 + \cdots + {}_pC_{p-1} + {}_pC_p$$
$$= {}_pC_1 + \cdots + {}_pC_{p-1} + 2 \quad \cdots ⑤$$

→ (1)で出てきた!

(1)の議論より、${}_pC_1 + \cdots + {}_pC_{p-1}$は$p$で割り切れる。 → あとは偶数であればOK!

さらに、⑤を変形して

${}_pC_1 + \cdots + {}_pC_{p-1} = 2^p - 2$となるので、右辺が偶数より左辺も偶数。

よって${}_pC_1 + \cdots + {}_pC_{p-1}$は$2p$の倍数となり($\because$ pと2は互いに素)

$2p > 2$であることから、2^pを$2p$で割った余りは2となる。

以上(i)(ii)より、

$$\begin{cases} p=2 \text{ のとき余りは } 0 \\ p \geq 3 \text{ のとき余りは } 2 \end{cases}$$

となる。

※フェルマーの小定理（発展）

証明は古賀真輝さんの動画などで…

「p：素数、aとpが互いに素のとき、
a^{p-1}をpで割った余りは1」

これを使うと、

$p \geqq 3$のとき、2^{p-1}をpで割った余りは1

$2^{p-1} = pm + 1 \ (m \in \mathbb{Z})$と表せて、

$2^p = 2pm + \underbrace{2}$ $< 2p$よりこれが余り。