その計算が
証明になるのはなぜ？

私と数学　2023年6月9日

斎藤　毅

専門は　　　　　整数論

整数論とは

数の性質を調べる

たとえば

フェルマの小定理

もともと整数論に思い入れはなかった

フェルマの小定理

n：自然数　p：素数

n^p-nはpでわりきれる

たとえば　$0^5-0=1^5-1=0=5\times 0$,

p=5　$2^5-2=32-2=30=5\times 6$,

$3^5-3=243-3=240=5\times 48$,

$4^5-4=1024-4=1020=5\times 204$,

・・・・・・

フェルマの小定理　n^p-n はpでわりきれる

証明は？　nに関する帰納法

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

を２項定理を使って計算すると・・

・n^p-n　帰納法の仮定　と

・２項係数　${}_pC_r$（$1 \leq r \leq p-1$）

は素数pでわりきれる

フェルマの小定理 n^p-nはpでわりきれる

証明は？　nに関する帰納法

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

を２項定理を使って計算すると・・

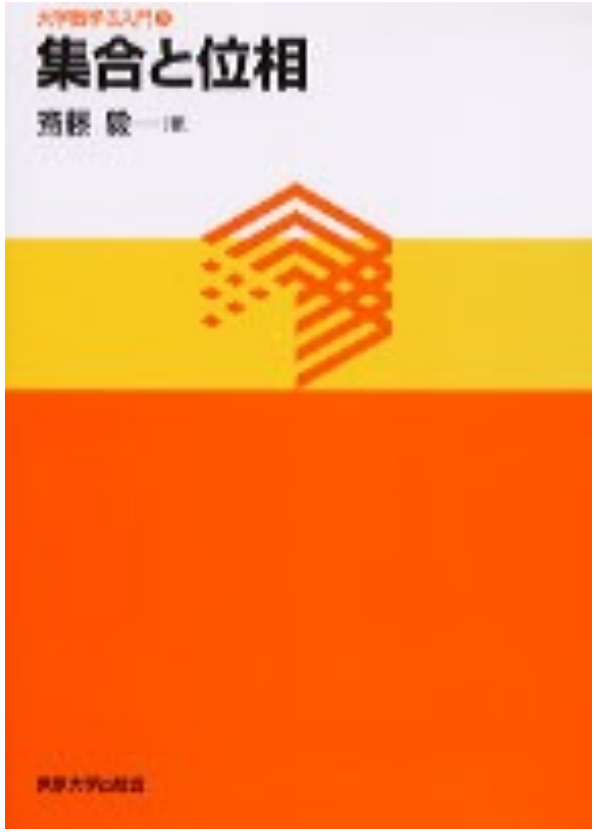
なぜこうすると証明できるのか？

これがわかるとスッキリする！

集合と位相　　数学科2A必修科目

数学科の特徴的な科目
・現代の数学の基礎
個々の数や図形、関数
ではなく、それらを
まとまりとしてとらえ、
相互の関係にも着目する。

集合と位相ー計算しない数学　UP
https://www.ms.u-tokyo.ac.jp/~t-saito/jd/UP.pdf



集合と位相ー計算しない数学　UP

a=bという・・・同じ式を証明するのに、違うやり方がある。
aとbが要素を１つしか含まない集合Aの要素ならば、やはりa=bが得られる。
この方法では、集合Aを設定するところが、実は鍵になっている。

集合と写像　aとbがAの要素ならばa=b

- 写像（関数の一般化）　$a, b: Z \to F_p$

  $Z = \{整数\} = \{0, \pm 1, \pm 2, \cdots\}$

  $F_p = \{0, 1, 2, \cdots, p-1\}$

  $a(n) =$（nをpでわったあまり）

  $b(n) =$（n^pをpでわったあまり）

フェルマの小定理のいいかえ　$a = b$

a=bの証明　　aとbがAの要素ならばa=b

- 写像　a,b: $Z \to F_p$

$Z=\{0, \pm 1, \pm 2, \cdots\}$, $F_p=\{0, 1, 2, \cdots, p-1\}$

　フェルマの小定理のいいかえ　a=b

$A=\{$ 環の射 $Z \to F_p\}$　・Aの要素は1つだけ

　(Aの説明は省略)　・a,b はAの要素

a=bの証明　aとbがAの要素ならばa=b

- 　$A = \{$ 環の射 $\mathbb{Z} \to F_p \}$ の要素は1つだけ
  nに関する帰納法
- (a,)b はAの要素

２項係数 ${}_pC_r$（$1 \leq r \leq p-1$）はpでわりきれる
その計算が証明になるのはなぜ？
見方を変えることでスッキリした！

フェルマの小定理　n^p-nはpでわりきれる

- 証明は？　 nに関する帰納法

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

を２項定理を使って計算すると・・

n^p-n　帰納法の仮定　　と

２項係数　${}_pC_r$（$1 \leq r \leq p-1$）

は素数pでわりきれる

集合と位相　を学ぶのはなぜか？

- A＝{ 環の射$\mathbb{Z} \to \mathbb{F}_p$ }
- 数学の対象とは（個々の数や図形ではなく）

構造のついた集合である　ブルバキ

いちどわかってしまうと

なんでわからなかったがわからなくなる

ほどスッキリとわかってしまう

ブックガイド　と　　読みもの

集合と位相ー計算しない数学　UP
https://www.ms.u-tokyo.ac.jp/~t-saito/jd/UP.pdf

数学への距離感は縮められるか？
駒場祭　2022.11.20
https://www.ms.u-tokyo.ac.jp/~t-saito/jd/KF.pdf

ブルバキと数学原論
数学セミナー　2002.4
https://www.ms.u-tokyo.ac.jp/~t-saito/jd/bourbakib.pdf

数学原論　　UP
https://www.ms.u-tokyo.ac.jp/~t-saito/jd/数学原論.pdf