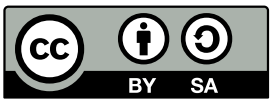
合同式について

Kris Walton https://kris.fail

2023 年 12 月 28 日



1　定義

合同という概念を数学に導入する．

参考. 幾何学の合同よりもこちらの整数の合同のほうが歴史的には古いものである．

定義 1.1. $n \in \mathbb{N}$ を法[*1]として整数 a, b が合同 ($a \equiv b \pmod{n}$) は，以下のように定義される．

$a \equiv b \pmod{n} \overset{\text{def}}{\Leftrightarrow} \exists k \in \mathbb{Z}; a - b = kn \iff \exists p, q, r \in \mathbb{Z}; a = pn + r \wedge b = qn + r \wedge 0 \leq r < n$

日本語で書けば，「$a - b$ が n の倍数，すなわち a を n で割った余りと b を n で割った余りが等しい」ということである．

注. $a \equiv b \pmod{n}$ を，法が明らかか，議論が法に依存しない時には単に $a \equiv b$ と書くことができる．

注. 当然のことながら，(反射律)$a \equiv a$, (対称律)$a \equiv b \to b \equiv a$, (推移律)$a \equiv b \wedge b \equiv c \to a \equiv c$ が定義 1.1 より成り立つ．推移律の証明を書いてみよ．

2　性質

定理 2.1. $a, b, c, d \in \mathbb{Z}$ で $a \equiv b \wedge c \equiv d \pmod{n}$ ならば $a \pm b \equiv c \pm d$ $ab \equiv cd \pmod{n}$

系 2.2. 定理 2.1 より $a \equiv b \to a^n \equiv b^n$ が直ちに従う．

注. これが言っているのは，余りを考える時，割り算を除く四則演算はそのままできるということである．

定理 2.3. $a \perp n$，すなわち a と n が互いに素なとき，$ab \equiv ac \to b \equiv c$ が成立する．

証明 (定理 2.1 の証明)**.** 定義 1.1 から明らか． □

証明 (定理 2.3 の証明)**.** $ab \equiv ac \to ab - ac \equiv 0 \to a(b - c) \equiv 0 \to b - c \equiv 0$ ($\because$ $a \perp n$ 故 $b - c$ は n の倍数) よって $b \equiv c$ □

注 (定理 2.3 について)**.** 以下，mod 15 で考える．

法と互いに素でない数で合同式の割り算をすることに意味はない．

例えば $18 \equiv 3$ であるが，これの両辺を 15 と合同でない 3 で割って $6 \equiv 1$ などと結論することはできない．

注. ところで，法を 15 ではなく 5 とした $6 \equiv 1 \pmod{5}$ が成り立っているのは，定義 1.1 より，$18 \equiv 3 \pmod{5}$ は $18 = 15 \cdot 1 + 3$ を含意していて，これの両辺を 3 で割ると，$6 = 5 \cdot 1 + 1$ になるからであり，一般に次のようなことが言える．

定理 2.4. $a, b \in \mathbb{Z}$ $p, q \in \mathbb{N}$ $pa \equiv pb \pmod{pq} \to a \equiv b \pmod{q}$

証明は定義 1.1 を用いればすぐにわかるので略．これが有用な定理かどうかは疑問である．

[*1] この" 法 "は modulus (Latin)/module (Franses) で割る数の意味．なぜこれが法と訳出されるのかは，軽く調べたが分からなかった．

3 応用

ここでは，初等整数論における定理であるフェルマーの小定理とオイラーの定理の証明を述べる．

3.1 フェルマーの小定理

定理 3.1 (フェルマーの小定理)**.** $a \in \mathbb{N}, p : \text{prime}, (a \perp p)\, a^{p-1} \equiv 1 \pmod{p}$

日本語で主張を書けば「正整数 a と素数 p (ただし a と p は互いに素) に対して a の $p-1$ 乗は p で割って 1 余る」ということである．

証明. $A = \{1, 2, \cdots, p-1\}$ と $B = \{a, 2a, \cdots, (p-1)a\}$ を考える．まず，この集合 A, B が p を法として合同，すなわち，A の要素と B の要素が p を法として一意に対応する[*2]ことを示す．

今，B には p を法として 0 に合同な (p の倍数の) 要素はなく，$p-1$ 個の要素があるから，これには B の異なる要素に p を法として合同なものがないことを示せばよい[*3]から，それを背理法で示す．

$1 \leq i, j \leq p-1, i \neq j$ で $ia \equiv ja$ なる場合を考えよう．このとき a と p は互いに素であるから，先程示した定理 2.3 から $i \equiv j$ が直ちに従う．

さて，$1 \leq i, j \leq p-1$ の条件のもとでこれを考えると，明らかに $i = j$ であるが，これは i と j が異なる，つまり別の要素を取ってきたという前提に反する．よって B の異なる要素で p を法として合同なものは存在しない．

よって A と B には一対一の合同な組が存在するので，集合全体の積も合同になる．

すなわち $(p-1)! \equiv a^{p-1}(p-1)!$ であり，p が素数であるから p と $(p-1)!$ は互いに素なので，再び定理 2.3 を用いて，$a^{p-1} \equiv 1$ が示された． □

定理 3.2 (フェルマーの小定理の別表現)**.** $a \in \mathbb{N}, p : \text{prime}, a^p \equiv a \pmod{p}$

(略証)a が素数 p と互いに素でない場合，つまり a が p の倍数のときは成り立つ．そうでない場合はフェルマーの小定理 (3.1) より成り立つ．

3.2 オイラーの定理

定理 3.3. $a, n \in \mathbb{N} \wedge a \perp n \to a^{\phi(n)} \equiv 1 \pmod{n}$ ただし $\phi(n)$ は n 以下の n と互いに素な自然数の個数.

証明. A を n 以下の n と互いに素な自然数の集合，B を A の各要素に a を掛けたものとして，先と同様の議論をすればよい． □

注. n が素数のとき，$\phi(n) = n - 1$ が成り立つので，フェルマーの小定理はオイラーの定理の特別な場合である．

[*2] つまり，B の要素を p で割った余りが 0 以外のすべてを取り得る

[*3] B の要素数が $p-1$ なので，合同なもの (余りが同じもの) がなければ，余りは 1 から $p-1$ までのすべてを取ることになる．

4　演習問題

4.1　問 1

2^{2021} を 3, 127 で割った余りをそれぞれ求めよ.

4.1.1　答

(3 で割った余り)

以下　mod 3 で考える.

$2 \equiv -1$[*4]より，$2^{2021} \equiv (-1)^{2021} \equiv 2$ よって余り 2

(127 で割った余り)

以下　mod 127 で考える.

$127 = 2^7 - 1$，すなわち $2^7 \equiv 1$ に注目して

$2^{2021} = 2^{7 \cdot 288} \cdot 2^5 \equiv 32$ よって余り 32

注. フェルマーの小定理よりわかる $2^{126} \equiv 1$ を利用する方法もある.

$2^{2021} = 2^{126 \cdot 16} \cdot 2^5 \equiv 32$

4.2　問 2

p が素数のとき $p^4 + 14$ が素数ではないことを示せ. (京都大学, 2021 年度学部入試 (文系))

4.2.1　答

まず $p \neq 3$ なる場合について考えると，p は 3 の倍数ではないから $p \equiv \pm 1 \pmod 3$

故に $p^4 \equiv 1$ であるから，$p^4 + 14 \equiv 0$ となる．よって，$p^4 + 14$ は，$p \geq 2$ であることも考えると 3 より大きな 3 の倍数であり，素数ではない.

次に $p = 3$ のときだが，$p^4 + 14 = 95 = 5 \cdot 19$ は明らかに素数ではない.

故に題意は示された.　□

注. このように，余りによる分類を合同式で議論すると答案がきれいにまとまる．特に素数や平方が絡む場合は効果的であることが多い.

[*4] $2 = 3 - 1$ と見て考えている．負数も考えると，絶対値の大きな四則演算を行わずにすむことが多い.