余りの美しさ

いきなりですが，「余り」についてのとても不思議で美しい定理を紹介しよう．

▷Point◁

a，b が互いに素であるとする．

このとき，$b-1$ 個の相異なる整数

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

を b で割った余りには，1 から $b-1$ までの整数が 1 回ずつすべて（順不同で）現れる．

なんのこっちゃ？　サッパリわからん

この定理はとても重要でいろいろな場面で活躍するので，ここでは「基本定理」と呼ぶことにしよう．

それにしても本当にこんなことがおこるのでしょうか．ちょっと信じがたいですが，まずは具体的な数字で確認してみよう．

はへい　そうします

具体例での確認

まずは互いに素な 2 数として，$a=3$，$b=8$ としよう．7 個の整数

$$1\times3,\ 2\times3,\ 3\times3,\ 4\times3,\ 5\times3,\ 6\times3,\ 7\times3$$

を，8 で割った余りを求めると，

$1\times3=3$ ⟶ 余り 3
$2\times3=6$ ⟶ 余り 6
$3\times3=9$ ⟶ 余り 1
$4\times3=12$ ⟶ 余り 4
$5\times3=15$ ⟶ 余り 7
$6\times3=18$ ⟶ 余り 2
$7\times3=21$ ⟶ 余り 5

1〜7までの数字が全部ある!!　美しい!!

確かに，余りに，1，2，3，4，5，6，7 が 1 回ずつ現れています．

次に，互いに素でない 2 数として，$a=6$，$b=8$ の場合で基本定理を確認してみよう．7 個の整数

$$1\times6,\ 2\times6,\ 3\times6,\ 4\times6,\ 5\times6,\ 6\times6,\ 7\times6$$

を 8 で割った余りを求めると，

$1\times6=6$ ⟶ 余り 6
$2\times6=12$ ⟶ 余り 4
$3\times6=18$ ⟶ 余り 2
$4\times6=24$ ⟶ 余り 0
$5\times6=30$ ⟶ 余り 6
$6\times6=36$ ⟶ 余り 4
$7\times6=42$ ⟶ 余り 2

さっきと様子がちがうぞ…　アレッ？　なんでぇ？

となり，余りは 0，2，4，6 しかありません．

なんとも不思議な結果ですね．どうしてこんなことが起こるのでしょうかね（他の数字の場合も試してみよう．やればやるほど不思議さが実感できるしょう）．

それでは基本定理を証明しよう．

基本定理の証明

$b-1$ 個の整数

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

を b で割った余りは，1，2，…，$b-1$ のいずれかの数である．よって，$b-1$ 個の余りが全て異なることを示せばよい．

重要なポイント

la，ma（$1\leqq l<m\leqq n-1$）を b で割った余りが同じであると仮定すると，

$$la=bq_1+r$$
$$ma=bq_2+r$$

$$\therefore\ (m-l)a=b(q_2-q_1)$$

a と b が互いに素なので，$m-l$ は b の倍数である．ところが，$1\leqq l<m\leqq b-1$ より，$1\leqq m-l\leqq b-2$ だから，$m-l$ は b の倍数にはならない．よって，矛盾．

したがって，$b-1$ 個の整数

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

を b で割った余りは全て異なるので，題意は証明された．

思ったよりシンプルな証明やな　それにしても何でこれでエエの？　なんでぇ？

■

⇒注　この証明の最大のポイントは最初の部分です．どうして「b で割った余りが，1 から $b-1$ までの整数が 1 回ずつすべて（順不同で）現れること」が，「余りが全部異なること」を示すことで証明できるのか分かりますか．

$b-1$ 個の箱に $\boxed{1}$ から $\boxed{b-1}$ のカードを 1 枚ずつ入れる，とイメージしよう．

「どの箱にも違うカードが入る」ならば，1 枚ずつ全部バラバラに入ることになります．箱の個数とカードの枚数が同じであることが重要なのです．

いずれにしても，**この証明の考え方がとても重要**なので，しっかりと理解しておこう．マジで大切．

さて，**基本定理**から導かれる重要な性質を 2 つ紹介しよう．

▷Point◁

$\boxed{\text{定理 ①}}$

a，b が互いに素

$\Longleftrightarrow$　$ax+by=1$ となる整数 x，y が存在する．

$\boxed{(\Longrightarrow)\text{ の証明}}$

a，b が互いに素のとき，基本定理より，

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

の中に，b で割ると余りが 1 になるものが必ず存在する．それを ka，そのときの商を q とおくと，

$$ka=bq+1$$

$$\therefore\ \ ak+b(-q)=1$$

ここで，$k=x$，$-q=y$ とおけば題意は成立する．

$\boxed{(\Longleftarrow)\text{ の証明}}$

a，b が互いに素でないと仮定すると，共通の素因数 p が存在し，$a=pa'$，$b=pb'$ となる．このとき，

$$\begin{aligned} &ax+by=1\\ \Longleftrightarrow\ &pa'x+pb'y=1\\ \Longleftrightarrow\ &p(a'x+b'y)=1 \end{aligned}$$

p は素数なので，この式は矛盾である．

■

つまり，例えば

$$3x+5y=1$$

のような不定方程式は，式の数より文字の数が多いにもかかわらず，必ず整数解 x，y をもつのです．どんな整数解なのかは分かりませんが，とにかく「存在する」ことが保証されたわけです．これはすごいことです．

このように，**基本定理**はただ単に余りが全部異なることを主張しているだけではなく，「余りが 1 になるものが必ず存在すること」の証明にもなっています．つまり，**基本定理**を利用すれば，具体的にいつ余りが 1 になるかは分からないが，「**必ずある**」ということは断言できるのです．

このような「存在証明」は数学の中でも難問の部類に入りますが，その攻略方法としてこの**基本定理**が有効であることをしっかり頭に入れておこう．

⇒注　上にあげた $\boxed{\text{定理 ①}}$ を互いに素であることの定義とする場合もあります．

$\boxed{\text{例題}}$　a を 2 以上の自然数とするとき，a と a^2+1 は互いに素であることを $\boxed{\text{定理 ①}}$ を利用して示せ．

解　$a\times(-a)+(a^2+1)\times 1=1$ より，$ax+(a^2+1)y=1$ をみたす整数 x，y が存在するので，a と a^2+1 は互いに素である．

■

一般に「互いに素であることを証明せよ」と言われたら，この方法で証明することは避けたほうが良いですが，互いに素であるかどうかチェックする手法として知っておくと便利でしょう．

$\boxed{\text{定理 ①}}$ から次の事実が導き出されます．

▷Point◁

$\boxed{\text{定理 ②}}$

a，b が互いに素であるとき，$ax+by$（x，y は整数）は任意の整数値をとることができる．つまり，$ax+by$ の形ですべての整数を表現することができる．