合同式の計算例

合同式が等式を緩やかにしたものとはいえ、実際の使い方を見ないことには理解が深まらないだろう。例を示しながら進めよう。

[問] 99^{111} を 7 で割ったときの余りはいくつか。

[解] これは $99^{111} \equiv ? \pmod 7$ となる ? を求めることである。ところで 99 は、$99 = 7 \cdot 14 + 1$ であるから、$99 \equiv 1 \pmod 7$ と書ける。合同式の性質で、両辺を n 乗することができたので、これの両辺を 111 乗して

$$99^{111} \equiv 1^{111} = 1 \pmod 7$$

より、99^{111} を 7 で割ったときの余りは 1 である。（終り）

この例は十分作為的に見える。そこで、ちょっと数値を変えてみよう。

[問] 97^{111} を 7 で割ったときの余りはいくつか。

[解] $97 = 7 \cdot 13 + 6$ であるから、$97 \equiv 6 \pmod 7$ と書ける。合同式の性質で、両辺を n 乗することができたので

$$97^{111} \equiv 6^{111} \pmod 7$$

である。ところで $6^2 \equiv 1 \pmod 7$ であることに注意すると、

$$6^{111} = (6^2)^{55} \cdot 6^1 \equiv 1^{55} \cdot 6 = 6 \pmod 7$$

より、97^{111} を 7 で割ったときの余りは 6 である。（終り）

合同式は、このように大きな数を扱うのに適している。本当に正しい余りが求められたか気になるだろうが、たとえば Microsoft Excel のワークシート上で検算しようにも、数が大きすぎてオーバーフローを起こしてしまう。プログラム言語の Python など、計算上、桁数に制限がないものがいくつかあるので、興味があれば試すとよいだろう。

* * *

2 つの問いに対する解答の中で、合同記号と等号を使い分けたことに気づいただろうか。たとえば

$$6^{111} = (6^2)^{55} \cdot 6^1 \equiv 1^{55} \cdot 6 = 6 \pmod 7$$

がそうだ。記号の使い分けは、もちろん式変形の違いによる。$6^{111} = (6^2)^{55} \cdot 6^1$ であるのは、両辺ともまったく同じ値であるから等号を使い、$(6^2)^{55} \cdot 6^1 \equiv 1^{55} \cdot 6$ であるのは、値は異なるものの法 7 の下では 6^2 と 1 が同じ剰余類に属するからである。

しかし、まったく同じ値であれば同じ剰余類に属することは明らかなので、等号の代わりに合同記号を使っても構わない。もちろん逆—合同記号の代わりに等号を使うこと—はだめである。もし、使い分けが面倒だと思えば

$$6^{111} \equiv (6^2)^{55} \cdot 6^1 \equiv 1^{55} \cdot 6 \equiv 6 \pmod 7$$

とするのもよいだろう。むしろ、この方が統一感があって見栄えがよいかもしれないが、オススメしているわけではない。▌

ところで、$97 = 7 \cdot 14 - 1$ と見れば、$97^{111} \equiv (-1)^{111} = -1 \pmod 7$ であるから、余りが -1 であることがすぐに分かる。もちろん余り r は $0 \leqq r <$（除数）なので、この場合の余り -1 は 6 と言い換えるべきであるが、合同式は負の余りを積極的に使うことで、計算がスムースに進められることは覚えておきたい。

慣れてくればすぐに分かることだが、正数 n で割ったとき、負の数で見る余りと本来の余りには

負の余り	-1	-2	-3	$\cdots$	$-(n-3)$	$-(n-2)$	$-(n-1)$	0
本来の余り	$n-1$	$n-2$	$n-3$	$\cdots$	3	2	1	0

の関係がある。7 で割っている例では、負の余りとして $-1, -2, -3, \ldots$ を考えると、実際の余りは $6, 5, 4, \ldots$ になるということである。もっと一般的な言い方をすれば、| 負の余り | + (本来の余り) $= n$ が成り立っている。| 負の余り | は、負の余りの絶対値を意味する。

合同式の方程式

合同式でも方程式を考えることができる。ただし、単なる方程式とは解き方がだいぶ違うと感じるはずだ。

[問] $x \equiv 1 \pmod 6$ を解け。

[解] 単に $x = 6n + 1$（n は整数）のことなので、これが解である。（終り）

もちろん単純な方程式ばかりではない。複雑な方程式はいくらでも作れるが、闇雲に作った方程式が必ず解けるわけではない。回りくどい解き方をしているけれど、次の例はどうだろう。

[問] $x^2 \equiv 1 \pmod 6$ を解け。

[解] これは $x^2 - 1 \equiv 0 \pmod 6$ と同じことであるから、$(x-1)(x+1)$ が 6 で割り切れることを意味する。その場合、n, m を整数として

i) $x - 1 = 6n$

ii) $x+1=6n$

iii) $x-1=2n$, $x+1=3m$

iv) $x-1=3n$, $x+1=2m$

が考えられる。まず、i)、ii) より $x=6n\pm1$ は解である。

iii) から $x=2n+1=3m-1$（※）であるが、これは $2(n+1)=3m$ となって、$n+1=3t$, $m=2t$ と表せる。したがって、※に代入して $x=6t-1$ である。

iv) も iii) と同様に $x=6t+1$ が求めらるが、iii)、iv) は結局 i)、ii) と同じ解であるため、最終的には $x=6n\pm1$ が求める解である。（終り）

* * *

方程式の解を具体的に求めるなら、Microsoft Excel でも多少は役に立つ。下は、$x^2\equiv1\pmod 6$ の解を求めた例である。$x^2\equiv1\pmod 6$ ではなく、$x^2-1\equiv0\pmod 6$ として解いている。

◇	A	B	C	D	E	F
1	x	x^2-1	solve? of mod	6		
2	1	(※ B2)	(※ C2)			
3	2	↓下へコピーする	↓下へコピーする			
4	3	↓	↓			
5	4	↓	↓			
6	5	↓	↓			

※ セルの式
（B2） =A2^2-1
（C2） =IF(MOD(B2,D1)=0,"yes","")

適当な行まで “↓下へコピーする” ようにしてほしい。この場合は $x=1, 5, 7, 11, 13, 17, 19, \ldots$ で yes が表示されるので、具体的な解は分かる。しかし、これを眺めて $x=6n\pm1$ が一般解であることに気づくのは難しいかもしれない。Excel は解を求めるものではなく、合同式で求めた解の確認程度に使うのがよいだろう。▌

合同式の利用

ここまでは、単に合同式を用いることが明確になっている問いであった。しかし普通の問題でも、合同式を用いるとよい例を見ることにしよう。

[問] $4x+7y=65$ を満たす整数 x, y の組を求めよ。

この問題は 2 節で見たように、$x=4$, $y=7$ が特殊解であるから、

$$\begin{array}{rrrcl} & 4x & +7y & = & 65 \\ -) & 4\cdot4 & +7\cdot7 & = & 65 \\ \hline & 4(x-4) & +7(y-7) & = & 0 \end{array}$$

のようにして、$x-4$ が -7 の倍数、$y-7$ が 4 の倍数ということが分かる。x と y を整数 n を用いて書き直せたことを思い出せば解にたどり着くのは容易だろうから、この先は省略させてもらいたい。

しかし、合同式を利用して解くのも便利である。その解法を示そう。

> [別解] $4x+7y=65$ より、$4x=-7y+65$ である。ここで、$-7y$ が 7 の倍数であることと、7 で割った余りが 65 と見ることで、7 を法とする合同式
>
> $$4x=-7y+65\equiv 65\equiv 16 \pmod 7$$
>
> が成り立つ。余り 65 をさらに 7 で割った余りを、2 でなく 16 と見たのは、$4x$ と 16 がともに 4 で割り切れることを念頭に置いたためだ。
>
> $4x\equiv 16 \pmod 7$ において、$\gcd(4,\ 7)=1$ であるから、4 で割ることが可能で、$x\equiv 4 \pmod 7$、すなわち $x=7n+4$ である。これを $4x+7y=65$ に代入して、$y=-4n+7$ となる。（終り）

どちらの解法が優れているとか言うのは的外れである。しかし特殊解が容易に見つらないときは、いずれの解法も厳しい。[別解] では特殊解を求めているように見えないが、$65\equiv 2 \pmod 7$ でなく、$65\equiv 16 \pmod 7$ としたところが、特殊解を求めることと同等なのである。方程式の係数や特殊解が大きな数で計算が容易でないときは、後ほど述べる方法を試すとよいだろう。

オイラーの定理と合同式

オイラーの定理と呼ばれる定理は数多く存在する[1]。その中の 1 つに

a と m $(m>1)$ が互いに素であるとき、$a^{\phi(m)}\equiv 1 \pmod m$ が成り立つ

がある。ここで「$\phi(m)$ は、m より小さい自然数の中で m と互いに素なものの個数」とする。

たとえば、次の問題を考えることにする。

> [問] $53x+36y=2$ を満たす整数 $x,\ y$ の組を求めよ。

先に結論を述べると、特殊解の 1 つは $x=34,\ y=-50$ である。これは、そう簡単に見つからないだろう。ところが、いま述べたオイラーの定理を使うと案外うまくいく。

[1] レオンハルト・オイラー（1707–1783）：スイスの数学者・天文学者。

[解] $53x+36y=2$ より、$53x=-36y+2$ であるから、36 を法とする合同式

$$53x=-36y+2\equiv 2 \pmod{36}$$

が成り立つ。

また、53 と 36 は互いに素なのでオイラーの定理より、$53^{\phi(36)}\equiv 1 \pmod{36}$。ここで、$\phi(36)=12$ だから、$53^{12}\equiv 1 \pmod{36}$。よって、$53^{12}\times 2\equiv 2 \pmod{36}$。

$53x\equiv 2 \pmod{36}$ であったので、

$$\begin{aligned} 53x &\equiv 53^{12}\times 2 \pmod{36} \\ x &\equiv 53^{11}\times 2 \pmod{36} \\ &= 53\cdot 2809^5\times 2 \pmod{36} \\ &\equiv 53\cdot 1^5\times 2 \pmod{36} \\ &\equiv 34 \pmod{36}。 \end{aligned}$$

これより、$x=36n+34$ である。これを $53x+36y=2$ に代入して、$y=-53n-50$ となる。（終り）

この解法のよい点は、必ず $ax\equiv a^k \pmod{b}$ となることである。すると、$x\equiv a^{k-1} \pmod{b}$ とでき、x の解が即座に求められるからだ。だから後は、合同式の計算を手際よく行うだけでよい。

ただ m が大きな数の場合、$\phi(m)$ の個数を数えるのに苦労するかもしれない。そのときは、数多（あまた）あるオイラーの定理

1. m が素数のとき、$\phi(m)=m-1$
2. m が素数のとき、$\phi(m^n)=m^{n-1}(m-1)$
3. l, m が互いに素のとき、$\phi(l\cdot m)=\phi(l)\cdot\phi(m)$
4. $\vdots$

などを利用して、素早く求めるとよいだろう。これらを利用して、$\phi(36)$ は

$$\phi(36)=\phi(2^2\cdot 3^2)=\phi(2^2)\cdot\phi(3^2)=2^1(2-1)\cdot 3^1(3-1)=12$$

のように求めることができたのである。