整数の除法

気持ちだけ小学校の頃に戻ってみよう。では、問題です。「32 割る 6 はいくつですか？」

$$\text{（式）}32 \div 6 = 5 \ \ldots 2 \qquad \text{（答）}5\text{、余り }2$$

はい、よくできました。でも、大人の世界はそうじゃない。$32 \div 6 = \dfrac{16}{3}$ である。割り切れないときは分数で表すものなのだ。

さあ、眠りから覚めるときである。現実の大人の世界でも $\dfrac{16}{3}$ で良しとすることはあんまりない。32 粒のアーモンドを 6 人で分けるなら、一人あたり 5 粒もらって、余った 2 粒は互いに遠慮し合ったのちに、本当は欲しかった人が「そうですかあ〜。それでは私がいただきます」とか言うものである。小学校の式の方が現実的なのだ。しかし式は現実的でも、その式は数学的とは到底言えない。なぜなら正しい等式になってないから。正しい等式とは

$$32 = 6 \times 5 + 2$$

である。

余談ながら、6 は “人数” で 5 は “一あたり量” なのだから、「（掛ける順が間違っていて）本当に正しい等式は $32 = \underline{5 \times 6} + 2$ である」などと、的確な理由も示さずに言うまぬけがいるかもしれないが、そういう生き物は絶滅してもらってかまわない。いま大事なのは、小学生風の書き方は

$$a \div p = q \ \ldots r \qquad \Rightarrow \qquad a = pq + r \quad (0 \leqq r < p)$$

のように、等式で表すことが現実的かつ正しい書き方であることだ。とくに、余り r は割る数 p より小さい負でない数である、は重要である。

* * *

一あたり量が a で、それが n だけ集まったときは、積を用いて $a \times n$ または $n \times a$ と書ける、というのが一あたり量の計算の本質である。掛ける順序は関係ない。そのため積を和にする場合、たとえば 6×5 は

$$\text{◎ } \underbrace{6 + 6 + \cdots + 6}_{5\text{ 個}} \text{ であるか、◎ } \underbrace{5 + 5 + \cdots + 5}_{6\text{ 個}} \text{ であるか、}$$

どちらもあり得るのだが、もし $6_{(\text{人})} \times 5_{(\text{個}/\text{人})}$ の意味で計算していたなら、それは

$$\times \ \underbrace{6_{(\text{人})} + 6_{(\text{人})} + \cdots + 6_{(\text{人})}}_{5_{(\text{個}/\text{人})}} \text{ ではなく、◎ } \underbrace{5_{(\text{個}/\text{人})} + 5_{(\text{個}/\text{人})} + \cdots + 5_{(\text{個}/\text{人})}}_{6_{(\text{人})}} \text{ であったはずだ。}$$

式 $a \times b$ から、a, b のどちらが一あたり量か知る必要が常にあるなら、必ず、単位を含める（たとえば $6_{(\text{人})} \times 5_{(\text{個}/\text{人})}$ と書く）か、掛ける順序を規定する（たとえば一あたり量が先と決める）必要があろう。しかし、その必要性

はまずなく、積を和に戻すこともほぼない。掛け算の順序にこだわることは、このような滅多にないことへの対応を強要するものでしかないのである。▌

ここまで何となく、a, p, q, r を正の数と見てきたかもしれないが、実際は負の数を含めた整数で考えている。余りを考慮した割り算を、等式と見ることができるなら、

$$a \div p = q \ \ldots r \qquad \Rightarrow \qquad a = pq + r = p(q+1) + (r-p)$$

という式変形もあり得る。具体的には

$$32 \div 6 = 5 \ \ldots 2 \qquad \Rightarrow \qquad 32 = 6 \times 5 + 2 = 6 \times 6 + (-4)$$

などである。しかし、それでは数学的に正しくとも収拾がつかなくなってしまう。そのため日常の感覚と同じく、余りは割る数に満たないと考えるのである。

すると、$p < 0$ の場合は、余り r が割る数 p に満たないことを、どのように解釈したらよいか迷うだろう。割る数 -5 に対して余りが -2 だとしたら、-2 は -5 に満たないと言えるのだろうか？むしろ余りが -7 と言った方が、満たないという意味に近いかもしれない。この混乱を収めるなら

$$a = pq + r \quad (0 \leqq r < |p|)$$

と考えるのがよいだろう。これなら、割る数 -5 に対する余りは正の数に限られ、しかも一意に定まる。余りを考慮した割り算は、余りが等式の性質を決めるのである。

余りの性質

負の数を含めた割り算は、余りを「日常の感覚と同じく」と述べたが、この点を優先すると必ずしも日常的ではない場面が生じる。分割払いを、割賦（かっぷ）月数を固定した上で支払額が決まるのではなく、支払額を固定した上で割賦月数が決まる方式にしたときなどだ。具体的には、29 万円分の負債（-29 万円）を、月々の支払いを 6 万円ずつ（-6 万円）に固定した上で割賦月数を決めると、余りが正の数である制約から

$$-29 \div (-6) = 5 \ \ldots 1 \qquad \Rightarrow \qquad -29 = (-6) \times 5 + 1 \quad (0 \leqq 1 < |-6|)$$

という関係式ができる。これ自体は正しいのだが、関係式を読み下せば「29 万円の負債は、6 万円ずつの支払いを 5ヶ月続け、1 万円を受け取る」となるだろう。しかし、実際は「6 万円ずつの支払いを 4ヶ月続け、さらに 5 万円を支払う」ことになるだろうから、$-29 = (-6) \times 4 + (-5)$ が

日常感覚の等式かもしれない。Microsoft Excel などは、この立場をとっているようである。実際、ワークシートに “=MOD(-29, -6)” と入力すると “-5” が返る。

日常的な感覚で処理する Excel に敬意を払ったとしても、余りがある整数の割り算を等式に書き換える自由度が高すぎるのは困る。そもそも割り算とは “等分すること” が目的であったはずだ。そうであれば、負の数で等分すること—つまり割る数が負の場合—は少々行き過ぎの感がある。そこでこの先は除数 p は正の整数に限ることにし、その際に成り立つ等式は

$$\boxed{a = pq + r \quad (0 \leqq r < p)}$$

であるとしておきたい。ただし、a は負の数であってもよいので、商 q が負の数になることもある。

先の支払い例に当てはめると、割る数が正の数であることから、負債額の一部である 6 万円の支払いは正の数である必要がある。つまり今度は、負債が正の数、貸し出しが負の数の世界で考えることになる。負債を負の数で表すのは単に習慣であり、本質は負債と貸し出しの正負が逆であることだから、負債が正の数であっても何ら問題はない。貸し出しが負の数になるだけの話だ。よって、等式は

$$29 \div 6 = 4 \ \ldots 5 \qquad \Rightarrow \qquad 29 = 6 \times 4 + 5 \quad (0 \leqq 5 < 6)$$

が正しい。この場合の読み下しは「29 万円の負債は、6 万円ずつの支払いを 4ヶ月続け、さらに 5 万円を支払う」となって、現実の感覚に合致する。

* * *

ここまでの話は、29 万円の負債を、支払額を固定した上で割賦月数が決まる方式で考えた。一方で、割賦月数を固定した上で支払額が決まる方式ではどうなるだろう。割賦月数を 6ヶ月に固定すると

$$-29 \div 6 = -5 \ \ldots 1 \qquad \Rightarrow \qquad -29 = 6 \times (-5) + 1 \quad (0 \leqq 1 < 6)$$

となる。ここでは負債を負の数と見ている。しかしこれでは、等式は「29 万円の負債は、6ヶ月に渡って 5 万円ずつ支払い、1 万円を受け取る」と読むことになり、現実的ではないと言うかもしれない。しかし、掛け算の順序にこだわるまぬけであっても足し算の順序にはこだわらないだろう。そこで $-29 = 1 + 6 \times (-5)$ と見れば、「29 万円の負債は、1 万円のキャッシュバックを受け、6ヶ月に渡って 5 万円ずつ支払う」と読むことになって、まことに現代的ではないだろうか。▌

合同式

余りを**非負整数**に限るのは、整数を分類するために重要だからでもある。整数は「何々の倍数」という見方ができるように、ある性質でグループ分けすることができる。たとえば整数を偶数と奇

数で分けると、整数は完璧に分割される。しかし、整数を 2 の倍数と 3 の倍数で分けると、6 の倍数が両方のグループに属すため分割には向かない。

ところが、余りに注目すると分類は完璧になる。たとえば、整数を 3 で割ることを考える。余りは 0, 1, 2 のいずれかで、ある整数が複数のグループに属すことなない。したがって、整数は

$$3n,\ 3n+1,\ 3n+2 \quad (n \text{ は整数})$$

に分けられる。こうすると $3n$ や $3n+1$ の形という具合に、整数を分類することができる。余りによる分類を**剰余類**という。

このような見方を扱い易くする記述が**合同式**と呼ばれるものである。合同式に慣れてもらうために、言葉づかいを定めておこう。まず、

-2 や 7 は、3 で割ると 1 余る　　⇒　　-2 や 7 は、3 を**法として** 1 と**合同**である

と読み替えることにする。このとき “m を法として” を記号 “$(\mathrm{mod}\ m)$” で、“合同” を記号 “$\equiv$” で表して、

$$\begin{aligned} -2 &\equiv 1 \pmod 3 \\ 7 &\equiv 1 \pmod 3 \end{aligned}$$

と書く。これらは、等式 $-2 = 3n+1$ や $7 = 3n+1$ と書くことと同じで、$n = -1$ や $n = 2$ のときを示している。また、これまでの話から、法 m は正の整数に限ることとなる。

*　　*　　*

合同式を Microsoft Excel で表現するのは非常に簡単である。Excel には MOD 関数が用意されているからだ。単に MOD 関数を使うだけでなく、次のようにすると少しは見栄えがよいだろう。

◇	A	B	C	D	E	F
1	整数を入力	≡	(※ C1)	(mod	正の整数を入力	)
2						

※ セルの式
（C1）　=MOD(A1,E1)

A1 セルに整数値、E1 セルに法となる値を入力すると、C1 セルに A1 の値に合同な整数が表示される。A1 セルに負の値を入力してみよう。MOD 関数は余りの制約を守ってくれて、C1 セルには法未満の正の値が表示される。ただし、法の値として E1 セルに負の値を指定すると、MOD 関数は負の値を返す。Excel で合同式を扱う場合は、このような特性を理解して使おう。▌

合同式の性質

一般に a を m で割って r 余ることを $a \equiv r \pmod m$ と書き、a と r は m を法として合同と言うのであった。このことは、a から余り r を除けば、それは m で割り切れることを意味する。す

なわち、q を整数として

$$a \equiv r \pmod{m} \quad \Leftrightarrow \quad a - r = mq$$

が成り立つことである。この関係式から合同式は、実は等式が形を変えて姿を見せたものだと分かる。そうであれば、等式の性質をいくらか受け継いでいるであろう。

合同式の主な性質は次のようなものである。

> ♠ $a \equiv b \pmod{m}$、$c \equiv d \pmod{m}$ のとき
>
> 1. $a + c \equiv b + d \pmod{m}$
> 2. $a - c \equiv b - d \pmod{m}$
> 3. $ac \equiv bd \pmod{m}$
> 4. $a^n \equiv b^n \pmod{m}$ （n は自然数）

仮定 $a \equiv b \pmod{m}$、$c \equiv d \pmod{m}$ より、p, q を整数として、$a - b = mp$、$c - d = mq$ と表せることに注意した上で、まず 1. と 3. を示しておこう。

1. は $(a + c) - (b + d) = ms$（s は整数）を示せばよいので

$$(a + c) - (b + d) = (a - b) + (c - d) = mp + mq = m(p + q) = ms$$

とすればよい。3. も同じく、$ac - bd = mt$（t は整数）を示せばよいので

$$ac - bd = (a - b)c + (c - d)b = mpc + mqb = m(pc + qb) = mt$$

とすればよい。

4. については、$a \equiv b \pmod{m}$ と $a \equiv b \pmod{m}$ の仮定の下で、繰り返し 3. を適用すればよい。

* * *

合同式が等式の性質を受け継ぐと言ったものの、合同式の性質の中に割り算に相当するものはなかった。それは $\frac{a}{c}, \frac{b}{d}$ が必ずしも整数にならないからではない！　きっちり整数になっても具合が悪いからである。たとえば $35 \equiv 27 \pmod{4}$ と $5 \equiv 9 \pmod{4}$ については、互いに左辺どうし、右辺どうしで割り算ができて $7 \equiv 3 \pmod{4}$ としても結果は正しい。しかし、$80 \equiv 8 \pmod{6}$ と $16 \equiv 4 \pmod{6}$ については、同様に割り算をすると $5 \equiv 2 \pmod{6}$ となって結果は正しくない。つまり、辺々が割り切れるからと言って、辺々で割ってよいとは限らないのである。

また、$35 \equiv 15 \pmod{4}$ では両辺を 5 で割った $7 \equiv 3 \pmod{4}$ は正しいが、$35 \equiv 15 \pmod{10}$ では両辺を 5 で割った $7 \equiv 3 \pmod{10}$ は正しくないので、$an \equiv bn \pmod{m}$ は必ずしも $a \equiv b \pmod{m}$ にできるわけではない。

しかし、$an \equiv bn \pmod{mn}$ であった場合は

$$\begin{aligned} an \equiv bn \pmod{mn} \quad &\Rightarrow \quad an - bn = mnK \quad (K \text{ は整数}) \\ &\Rightarrow \quad a - b = mK \\ &\Rightarrow \quad a \equiv b \pmod{m} \end{aligned}$$

であるから、

$$an \equiv bn \pmod{mn} \quad \Rightarrow \quad a \equiv b \pmod{m}$$

は成り立つ。したがって、$35 \equiv 15 \pmod{10}$ の両辺と法の値を 5 で割って、$7 \equiv 3 \pmod{2}$ ならば正しいのである。

さて、以上から分かることがある。n と m が互いに素であれば、$an \equiv bn \pmod{m}$ を等式で表して $(a-b)n = mK$ とした場合、K が n の倍数でなくてはならない。そこで $K = nK'$ と置くと $a - b = mK'$ となるので、$a \equiv b \pmod{m}$ が言える。すなわち

$$\boxed{an \equiv bn \pmod{m} \quad \text{かつ} \quad \gcd(n, m) = 1 \quad \Rightarrow \quad a \equiv b \pmod{m}}$$

であればよいのである。▌