

- 集合 $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ の元を整数という。 $\mathbb{Z}$ には大小の順序と加減乗を(すでに知っているように)定める。
- $\mathbb{Z}$ は除法について閉じていない。たとえば $3 \div 4$ は $\mathbb{Z}$ の元と等しくない。ただし、 $\mathbb{Z}$ には "余りを出す除法" (これを整除ともいう) がある。

定理1: 整数 a と正の整数 b に対して、

$$a = bq + r \quad \text{かつ} \quad 0 \leq r < b$$

を満たす整数 q, r がただ一つ存在する。

定義: a, b に対して q, r を求めることを「 a を b で整除する」あるいは単に「 a を b で割る」といい、 q を商、 r を余りという。

- $\mathbb{Z}$ の部分集合 $\mathbb{N} = \{1, 2, 3, \dots\} = \{x \in \mathbb{Z} \mid x > 0\}$ の元を自然数という。これは日本の高校の教科書などの習慣に従ったが、 $\{0, 1, 2, 3, \dots\}$ を $\mathbb{N}$ とする流儀もある。このテキストでは集合 $\{0, 1, 2, 3, \dots\}$ を $\mathbb{Z}_{\geq 0}$ と表し、その元を非負整数と呼ぶ。

0 を自然数とみなす。みなさないはそのときどきの立場によるもので、どちらかが絶対的に正しいと断言的に決まっているものではない。

定理2: $\mathbb{N}$ の任意の部分集合 A は、最小元を持つ。

定義: m が集合 A の最小元であるとは、
 (1) $m \in A$, (2) 任意の $x \in A$ について $m \leq x$ がともに成立することである。

- $\mathbb{N}$ は加法・乗法について閉じている。減法・除法については閉じていない。
- 整数 k と自然数 l によって $\frac{k}{l}$ と表される数を有理数といい、その全体の集合を $\mathbb{Q}$ と表す。つまり $\mathbb{Q} = \{\frac{k}{l} \mid k \in \mathbb{Z}, l \in \mathbb{N}\}$ 。

定理3: $\mathbb{Q}$ は四則演算について閉じている。

問題1 左ページの定理1を証明せよ。

このシリーズ全体で「証明せよ」つまり「証明を文章で記述せよ」という問題も意識して多く出題し、授業中でも長く時間を取って記述してもらった。

なんとなく当たり前だと感じていることを言語化して客観視する経験は学問全般において大切。また、抽象学問である数学にあっては言語が唯一のツール。

横着なのか自信がなくなってきたがらない生徒は多いのだが、それではいけないと強調する。

問題2 左ページの定理2を証明せよ。

問題3 $\mathbb{Q}$ は加法について閉じていることを証明せよ。(定理3の一部)

「いかにも当然のこと」「理由を問うまでもなさそうなこと」を代表できるインパクトのある命題として、これを初回の授業に配置した。これが2枚目、3枚目などでexplicitに役立つことも見越している。

- 当たり前のことを「なぜ?」と訊かれたときにどうなるのか。
- 当たり前のことが役立つ理場はどこくらいあるのか。

を実感してもらうことが(上位の)目的。

- 2つの整数 a, b について, $a = kb$ となる整数 k が存在するとき,
「 a は b で割り切れる」「 b は a を割り切る」
「 b は a の約数 (因数) である」
「 a は b の倍数である」
などという.
- ± 1 はすべての整数の約数である. 0 はすべての整数の倍数である.

定理4: 2つの整数 a_1, a_2 が整数 b の倍数であるとき,
任意の整数 t_1, t_2 に対して, $t_1 a_1 + t_2 a_2$ は b の倍数である.

定理5: 3つの整数 a, b, c について, b が a の約数であり,
かつ, c が b の約数であるならば, c は a の約数である.

- 整数 d が整数 $a_1, a_2, \dots, a_n$ すべての約数であるとき, d は $a_1, a_2, \dots, a_n$ の公約数であるという. 「 b が a の約数であれば $|b| \leq a$ 」.
 $a_1, a_2, \dots, a_n$ の公約数は有限個しかない (なぜか?). だから, そのうち正のものも有限個しかない. そのうち最大のものを最大公約数という.

- 整数 m が整数 $a_1, a_2, \dots, a_n$ すべての倍数であるとき, m は $a_1, a_2, \dots, a_n$ の公倍数であるという.
 $a_1, a_2, \dots, a_n$ の公倍数のうち正のものを考えると, そのうち最小のものがある (なぜか?). それを最小公倍数という.

定理2!
定理6: いくつかの整数の公約数は, 最大公約数の約数である. ←

定理7: いくつかの整数の公倍数は, 最小公倍数の倍数である. 定理6の証明は, けっこう難しい.

- 上述の2定理はここまでの知識で証明できるが, 多くの人には, 素因数分解を用いて考えるほうがわかりやすいだろう. 以下もたぶんそう.

定理8: 3整数 a, b, c の最大公約数は, 「 a, b の最大公約数」と c の最大公約数である. (最小公倍数も同様.)

定理9: 2整数 a, b の最大公約数を g , 最小公倍数を l とすると,
 $ab = gl$ である.

定理6, 8, 9のここまでの知識のみによる証明は生徒の意欲にやだねた.

問題4: 左ページの定理4を証明せよ.

"定義にもとづいた議論" の練習.
文字式の有用性を再認識する.

※この定理は中学校でも既習. しかし, ここで「きちんと論述する」ことを強調した.

問題5: (1) 左ページの定理5を証明せよ.

(2) 「3つの整数 x, y, z について, y が x の倍数であり, かつ, z が y の倍数であるならば, z は x の倍数である」ことを, 定理5をもとにして, 一言で示せよ.

同上.

さらに, (2) が定理5と同内容であることを理解する, この場合では左ページ $\otimes$ を真に理解する, ことを重視.

問題6: 左ページの定理7の証明を, 以下に続けて完成させよう.

<証明> 整数 $a_1, a_2, \dots, a_n$ の最小公倍数を l とする. m が $a_1, a_2, \dots, a_n$ の公倍数であるとしよう.

m を l で割ったときの商を q , 余りを r とすると,

$$m = lq + r \dots ①, \quad 0 \leq r < l \dots ②$$

である. ①より $r = m - lq$ である. これに定理4を適用すると, r が

本文中の生徒の感想,

がんばって証明した定理が, 普通には見えてないところまでじつまが合っていることに気づき, 「ちょっと感動した」

の1つの事例. 定理1で保証された, 特に②をみたす r の存在が, 議論を支えている.

問題7 左ページの定理10を、以下の方針で証明せよ。

● ここでは2つの整数 a, b の最大公約数を $G(a, b)$ と書くことにする。 $G(a, b)$ を求めるには、 a, b の因数から探ったり素因数分解を用いたりすることもあるが、次の定理10を繰り返し使うこともある。**定理10** $G(a, b) = G(a-b, b)$. (a, b は整数)

● たとえば"253 と 322 の最大公約数を

$$\begin{aligned}
 G(253, 322) &= G(253, 322-253) = G(253, 69) \\
 &= G(253-69, 69) = G(184, 69) \\
 &= G(184-69, 69) = G(115, 69) \\
 &= G(115-69, 69) = G(46, 69) \\
 &= G(46, 69-46) = G(46, 23) \\
 &= G(46-23, 23) = G(23, 23) \\
 &= G(23-23, 23) = G(0, 23) \\
 &= 23
 \end{aligned}$$

定理10も
その証明の理解も
非常に大切。
数学を学ぶ続けたい
何回も理れる。

と求められる(最後の数行は不要という人もいるだろう)。

① では「69を引く」作業が3回行われる。これをまとめて

$$G(253, 69) = G(253 - 69 \times 3, 69) = G(46, 69)$$

とよいだろう。253を69で整除すると商が3, 余りが46, ということだ。
整除はひきざんの繰り返し。

● ①, ②を整除で短く処理すると、上述の計算は

$$\begin{aligned}
 322 &= 253 \times 1 + 69 \\
 253 &= 69 \times 3 + 46 \\
 69 &= 46 \times 1 + 23 \\
 46 &= 23 \times 2 + 0
 \end{aligned}$$

となる。ある行で割る数だったものが次の行では割られる数になり、余りだったものが次の行では割る数になる。

この一連の計算アルゴリズムを、(ユークリッドの)互除法という。

"優秀"な
アルゴリズム
あることも
授業では
強調は。

● a, b が正の整数であるとき、互除法を進めると、各ステップでの余りは前ステップより小さくなる(なぜか?)。だから、いつか必ず余りが0になる。そこで互除法は終わる。
整除の定義から。

● 定理10は、 a, b が「整数値をとる文字式」であっても使える!(1) $G(a, b) = d_1, G(a-b, b) = d_2$ とおく。(2) d_1 が $a-b$ を割り切ること、そして d_2 を割り切ること示す。(3) d_2 が a を割り切ること、そして d_1 を割り切ること示す。(4) ということは... $d_1 | d_2$ かつ $d_2 | d_1 \Rightarrow \dots$

問題8 (1) 1632 と 2652 の最大公約数を求めよ。

(2) 1632 と 2652 と 7293 の最大公約数を求めよ。

問題9 (1) 多項式 $P(x) = x^2 + 5$ を多項式 $Q(x) = x + 25$ で割ったときの商と余りを求めよ。(2) 自然数 n のうち、 $n^2 + 5$ と $n + 25$ の最大公約数をもっとも大きくするものは、何か。

以前に習った「多項式の割りざん」が
整数の問題の解決に直結する。
数学のいろいろな物事の連関を感じてもらいたい。

互除法というアルゴリズムが「終わる」ことの理由が、
整除の可能性、さらには数の大小に依存ことを意識
してもらう。ここでも1枚目への回帰。

● 以下, 登場する文字はすべて整数を表すとする.

● a, b の最大公約数が 1 のとき (同じことだが, a, b の正の公約数が 1 しかないとき), a, b は互いに素 (relatively prime) だという.

定理 10 a, b が互いに素であるとき, x, y の 1 次方程式 $ax+by=1$ は, 整数解を持つ.

高校生の「整数」の理解においては一つの到達点。

● a, b が具体的に与えられているとき, $ax+by=1$ の解を 1 つ見つけるのに, 互除法が利用できる. 実際は → 問題 10 etc..

● 定理 10 の理論的な重要性は, 分かりしれないが... 互除法を用いない抽象的証明もある.

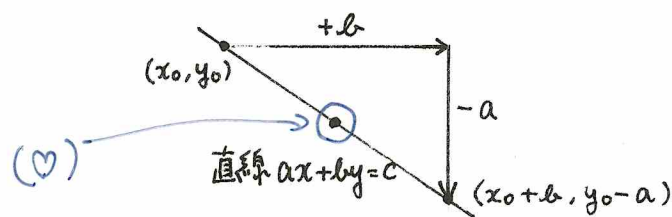
● $ax_0+by_0=1$ のとき, $a(cx_0)+b(cy_0)=c$ である. これと定理 10 から, 次の定理 11 がすぐわかる (なぜか?)

定理 11 a, b が互いに素であるとき, 任意の整数 c に対して, 1 次方程式 $ax+by=c$ は, 整数解を持つ.

● a, b が互いに素でない場合は次のようになる.

定理 12 a, b の最大公約数を g とする. 方程式 $ax+by=c$ は,
 $\left\{ \begin{array}{l} c \text{ が } g \text{ の倍数であれば整数解を持ち,} \\ c \text{ が } g \text{ の倍数でなければ整数解を持たない.} \end{array} \right.$

● ここまでは解が「1 つはある」話だったが, では, 解をすべて求めるにはどう考えるか.



1 次方程式 $ax+by=c$ は傾き $-\frac{a}{b}$ の直線を表す. 格子点 (x_0, y_0) がこの直線上にあるとき, そこから $\begin{pmatrix} b \\ -a \end{pmatrix}$ だけ平行移動した

格子点 (x_0+b, y_0-a) も直線上にある. こう考えれば, $ax+by=c$ の整数解はすべて挙げられ... てないかも...

問題 10 (1) 互除法を用いて, 70 と 19 の最大公約数を求めよ:

$$\begin{array}{l} 70 = 19 \times 3 + 13 \\ 19 = 13 \times 1 + 6 \\ 13 = 6 \times 2 + 1 \end{array} \quad \begin{array}{l} \text{となる. これを} \\ 13 = 70 - 19 \times 3 \\ 6 = 19 - 13 \times 1 \\ 1 = 13 - 6 \times 2 \end{array} \quad \begin{array}{l} \uparrow \\ \text{と見て,} \end{array}$$

「 A に P を代入, I に I を代入」することによって,

$1 = 70 \times \square + 19 \times \square$ という数式を作れ.

(これで「 $70x+19y=1$ の整数解を 1 つ作ったことになる」)

(2) $70x+19y=4$ の整数解を 1 つ見つけよ.

これがユークリッドの互除法という
具体的なアルゴリズムから証明できる!

↑
(1) から (2) がすぐ
わかるのは, ぜひ
観察してほしい.
授業では標語的に
「1 を作れば
なんでも作れる」と
強調した.

問題 11 (1) 方程式 $10x-6y=2$ の整数解をすべて求めよ. (左ページ 定理 11)

(2) 方程式 $10x-6y=14$ の整数解をすべて求めよ.

この部分は,
いますぐポイント
来なくても,
いつか (より
抽象的思考に
慣れたころに)
わかってくれば
よいとして, 載せた.

これは, 中学入試の経験が
ある開成中からの進学者は
すぐわかる. 図中にさりげなく
(♡) の点を打ってある.

文字が多いので生徒の
理解にはやや時間か
かかる. しかし一方で, いわゆる
「数学らしい推論」が
行われるところなので,
興味深く受講する生徒が
多かった.

1 枚目 ~ 4 枚目がひとつの
まとめ. しかし実は, 5 枚目,
6 枚目で再び定理 10 が
現れる!

- 自然数は「1」「素数」「合成数」の3種に分類される。
1と自分自身のみを正の約数とする自然数を素数という。
1でも素数でもない自然数を合成数という。

- p が素数のとき、任意の自然数 a に対して

p と a が互いに素でない $\iff a$ は p の倍数である,

p と a が互いに素である $\iff a$ は p の倍数でない

が成立する(なぜか?). これを用いて、次の定理13を示せる。

定理13 2つの整数 a, b の積 ab が素数 p の倍数であれば、
 a, b の少なくとも一方は p の倍数である。

定理13の対偶もよく使う。

定理13' 2つの整数 a, b 両方が素数 p の倍数でなければ、
積 ab は p の倍数でない。

- 素数は無限個存在する。いろいろな証明があるが、有限個しかないを仮定すると、それらすべての積に1をたしたものが...と考えるのが、ユークリッド『原論』にも載っている古い証明。

- 高校生としては、次の定理は認めて使ってよいだろう。ほかの証明方針については少しだけ言及。

定理14 (素因数分解の存在と一意性)

1でない自然数は素数である因数(素因数という)の積に書き表せる。その書き表し方は1通りしかない。

- 素因数分解を用いて簡明になることは多い。たとえば...

★ 自然数 a の素因数分解が $a = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$ であれば、

a の正の約数は $p_1^{f_1} p_2^{f_2} \dots p_t^{f_t}$ ($0 \leq f_i \leq e_i$) である。

など。これで、定理6～定理9はすべて、当然に思えるだろう。

→ ということは、「素因数分解の存在と一意性」も、1枚目のプリントから管々と積み上げた推論の賜物なのだ、と生徒に伝えた。

問題12 定理13を次のように示せ。

- (1) 定理13の仮定のもと、 a が p の倍数でないとする。

このとき、 $px + ay = 1$ となる整数 x, y がとれる。なぜか?

- (2) (1)より $px + ay = 1$ である。これと仮定から...

4枚目の定理10より!

この言証明は、普通は、予備知識の
ない人が思いつけるようなものでは
ない。先人の知恵に感嘆しよう。
(ただし「1を作ればなんでも作れる」ではある。)

問題13 2つの自然数 a, b の積は10800で、最小公倍数は360である。

- (1) a, b の最大公約数を求めよ。

- (2) あり得る (a, b) の組で $a < b$ をみたすものをすべて求めよ。

高校の授業でこの証明が
議論されることは少ない。
しかし、問題12に見るように、
ここで前回強く推した
定理がいまなり役立つ! q は
かなりインパクトがあり、生徒
からも「いかにも数学」と
好評だった。

問題14 p は素数とする。

- (1) $pC_1, pC_2, \dots, pC_{p-1}$ はすべて p の倍数であることを示せ。

- (2) 2^p を p で割ったときの余りはいくらか。

生徒から見れば「異文化交流」に見えよことを期待した。
実際、授業中にも「なんで 2 は p の倍数?」という声があちこちで上がった。(2)の解き方で

$$(1+1)^p =$$

と書いたところではじめてからくり気づいた生徒が現れ、けっこうな馬鹿者になった。

- (不思議なことだが) 整除の商を見ずに、余りだけ見ると整数の問題が解決してしまうことがある。
- 「整数 a を自然数 m で割ると余りが r である」というとき、商を q とすると $a = mq + r$ である。ここで、 q にあまり気をつかわないで「おけば」、「余りに注目した表現」ということになる。
- 割る数 m を固定して議論するときには、合同式 という数式の表現が便利である。

「余りだけ見る」
この
動機づけ。

問題15 (1) 奇数の平方を4で割ると1余り、偶数の平方は4で割り切れることを示せ。

(2) $x^2 + y^2 = 1003$ をみたす整数の組 (x, y) はあるか。

事例. なぜか(2)が簡単に解決してしまう。

← 授業では「余りといえば合同式」... と限定しない、と言った。

問題16 定理15を証明せよ。

プリントシリーズ全体の「数学の流れ」とは別に、「論述の技術と磨く流れ」においては、この問題16は重要だった。

- 横着せずにはにかく書く。簡単なことを丁寧に。
- 定義1の方がわかりやすと感じるかもしれないが、ここでは定義に基づいて考える方が記述がわかりやすい。

その他、(2)の証明で $ac - bd = ac - bc + bc - bd = \dots$ とするところは、いわゆる「うける」ところ。

問題17 (1) $4x + 13y = 1$ の整数解を1組みつけよ。

(2) $4x \equiv 1 \pmod{13}$ をみたす整数 x を $\text{mod } 13$ で求めよ。

(3) $4x \equiv 9 \pmod{13}$ をみたす整数 x を $\text{mod } 13$ で求めよ。

これができれば定理16の証明はわかったも同然。

合同式のことは一般に高校生にも知っている者が多い。考えれば、そんな対象の考察に、またまた、4枚目の定理10! 「 $4x + 13y = 1$ の整数解」と言われ2もたいしたこととは思えないが、「 $4x \equiv 1 \pmod{13}$ の解」となるととたんに興味を感じる生徒は多い。この感覚のギャップを基礎事項の積み上げで埋められたいは面白い。

- 実数では $\frac{b}{a}$ とは $ax = b$ をみたす x のことである。だったら、整数の合同式の世界で $ax \equiv b \pmod{m}$ をみたす x があれば、それは $\frac{b}{a}$ 、 $b \div a$ に相当するといえよう。
- しかし、たとえば $2x \equiv 3 \pmod{4}$ をみたす整数 x は存在しない。また、 $2x \equiv 2 \pmod{4}$ は $x \equiv 1$ または $x \equiv 3 \pmod{4}$ と同値であり、 $\text{mod } 4$ で見ても x は一通りに決まらない。
- $\text{mod } m$ で $\frac{b}{a}$ に相当するものが一意に決まるには、条件を要する。
- 定理16 a と m が互いに素であれば、 $ax \equiv b \pmod{m}$ をみたす x は、 $\text{mod } m$ でただ1つ存在する。

「加減乗」と
ければ
「除」を
考えれば、そんな対象の考察に、またまた、4枚目の定理10! という
数学に
おける
「自然な
発想の
提示」