1 Algorithm

1.1 $\mathcal{O}$ notation

与えられた関数 $g(n)$ に対して、$\mathcal{O}(g(n))$ によって関数の集合

$$\mathcal{O}(g(n)) = \{f(n) : \text{ある正の定数 } c, n_0\text{が存在して、すべての } n \geq n_0\text{に対して } 0 \leq f(n) \leq cg(n) \text{ を満たす } \}$$

を表現する。

入力が一定数以下はオーバーヘッドがあったりで、ノイズなので入力が一定数以上を表現するために n_0 を設けている。

2 整数

2.1 素数

2.1.1 定義

1 以外の自然数で 1 と自身以外に正の約数をもたない数を素数 (prime number) という。

1 でも素数でもない数を合成数 (composite number) という。

2.1.2 素数の判定

素数 $\vee$ 合成数 が成り立つので、合成するを判定することで素数の判定もできる。合成数の判定に合成数の以下の性質を利用する。

$$N \text{ が合成数ならば } 1 < a < \sqrt{N} \text{を満たす約数 } a \text{ を 1 つ以上もつ}$$

$$1 < a < \sqrt{N} \text{を満たす約数 } a \text{ が一つも存在しないならば} \quad N \text{ は合成数でない (対偶)}$$

この性質から、ある整数 N において、$[2, \sqrt{N}]$ の範囲に約数がなければ、N は合成数でない $\equiv$ 素数 が成り立つ。以下証明

N は合成数なので、定義から 1 以外の 2 つの積に分解できる。小さいほうを a とすると

$$\begin{aligned} N &= a \times b \qquad (1 < a \leq b, \quad a, b \in \mathbb{Z}) \\ N &= a \times b \geq a \times a = a^2 \qquad (1 < a \leq b) \\ N &\geq a^2 \\ a &\leq \sqrt{N} \end{aligned}$$

この事実を証明したので、心置きなく、素数判定の for loop に対象判定 N の平方根を終了条件にできる。

2.2 ユークリッド互除法

2.2.1 証明

2 つの整数 a,b が与えられたとき、a,b の最大公約数が知りたい.a,b を以下のように表現したとき、a と b の公約数の集合は a と r の公約数の集合と等しくなる。

$$b = qa + r \ (0 <= r < a)$$

$d|a \wedge d|b \equiv d|a \wedge d|r$ を証明する。

戦略として、 $(d|a \wedge d|b \rightarrow d|a \wedge d|r) \wedge (d|a \wedge d|r \rightarrow d|a \wedge d|b)$ を証明する。

(1) $d|a \wedge d|b \rightarrow d|a \wedge d|r$ の証明

仮定より、$\exists q_a, q_b (a = q_a d, b = q_b d)$

$$\begin{aligned} b &= aq + r \\ q_b d &= (q_a d)q + r \qquad \text{(仮定から a と b を置換)} \\ r &= q_b d - q q_a d \\ r &= d(q_b - q q_a) \end{aligned}$$

ここで、 q_b, q_a, q は整数であり、整数の掛け算、引き算は整数に閉じるので $(q_b - q q_a)$ は整数。したがって、$\exists n (r = dn)$ がいえるので、$d|r$ がいえる。よって、$d|a \wedge d|b \rightarrow d|a \wedge d|r$

(2) $d|a \wedge d|r \rightarrow d|a \wedge d|b$ の証明

仮定より、$\exists q_a, q_r (a = q_a d, r = q_r d)$

$$\begin{aligned} b &= aq + r \\ b &= (q_a d) + q_r d \qquad \text{(仮定から a と r を置換)} \\ b &= d(q_a + q_r) \end{aligned}$$

(1) と同様に、q_a, q_r は整数であり、整数に閉じるので、$(q_a + q_r)$ は整数。したがって、 $\exists n (b = dn)$ がいえるので、 $d|b$ が成り立つ。よって、 $d|a \wedge d|r \rightarrow d|a \wedge d|b$ がいえる。

2.2.2 帰結

ある 2 つの数 a,b が与えられた時、a と b の約数は a と r の約数でもある。そして r は b を a で割ったときの余りなので a よりも小さい。そのため、問題をより小さい問題に言い換えることができる。また a と r の約数は、$a = d_1 r + r_2$ とした場合 r と r_2 の約数でもある。この操作を繰り返すと、diviser(最初の a) が target(最初の b) を割り切る (r=0) ときがきて、そのとき、diviser と 0(r) が target と diviser の約数となる。そしてそのときの diviser を最大公約数と呼ぶ (定義)

2.3 倍数の判定

3 桁の数 N は 100a + 10b + c とあらわせる。

$N = 2(50a + 5b) + c$ とあらわせるので、N が 2 の倍数になるかどうかは最後の桁が 2 の倍数かどうかによる。

$N = 100a + 10b + c = 99a + a + 9b + b + c = 3(33a + 3b) + a + b + c$ なので、各桁の数の合計が 3 の倍数になるかで N が 3 の倍数かどうか判定できる

3 統計

3.1 条件つき確率

2 つの事象 A,B に対し、A が起こった状況のもとで B が起こる条件つき確率といい、以下のように表す

$$P(B|A) = \frac{P(A \cap B)}{P(A)}$$

考え方としては、$P(B|A)$ を given として与えられている事象 A の個数と事象 A かつ B の個数と捉えて以下のように導く

$$\begin{aligned} P(B|A) &= \frac{n(A \cap B)}{n(A)} \\ &= \frac{\frac{n(A \cap B)}{n(U)}}{\frac{n(A)}{n(U)}} \qquad \text{(分子, 分母を n(U) で割る)} \\ &= \frac{P(A \cap B)}{P(A)} \end{aligned}$$

条件付き確率を以下の形にしたものを乗法定理という。

$$P(A \cap B) = P(B|A) \cdot P(A)$$

3.2 ベイズの定理

$$
\begin{aligned}
P(X \cap Y) &= \frac{n(X \cap Y)}{n(U)} \\
&= \frac{n(X \cap Y)}{1} \cdot \frac{1}{n(U)} \\
&= \frac{n(X \cap Y)}{n(X)} \cdot \frac{n(X)}{n(U)} \\
&= P(Y|X) \cdot P(X)
\end{aligned}
$$

同様に

$$
\begin{aligned}
P(X \cap Y) &= \frac{n(X \cap Y)}{n(U)} \\
&= \frac{n(X \cap Y)}{1} \cdot \frac{1}{n(U)} \\
&= \frac{n(X \cap Y)}{n(Y)} \cdot \frac{n(Y)}{n(U)} \\
&= P(X|Y) \cdot P(Y)
\end{aligned}
$$

従って

$$P(Y|X)P(X) = P(X|Y)P(Y)$$

$$P(X|Y) = P(X) \cdot \frac{P(Y|X)}{P(Y)}$$

事後確率　事前確率　修正項

4 Burn Mathclass

4.1 分数

$\frac{1}{n}$ は n をかけると 1 になる数として定義する。これでうっかり騙されて割り算というものを使わされることを防げる。だから、$\frac{15}{72}$ は $(15)(\frac{1}{72})$ の略号でしかない。

$\frac{ac}{bc} = \frac{a}{b}$ という分母と分子の共通の因子を約分できるというのは以下の操作から導ける.

$$\frac{ac}{bc} = (a)(c)(\frac{1}{b})(\frac{1}{c}) = (a)(c)(\frac{1}{c})(\frac{1}{b}) = (a)(\frac{1}{b}) = \frac{a}{b}$$

$\frac{a+b}{c} = \frac{a}{c} + \frac{b}{c}$ は以下のように説明する。

$$\frac{a+b}{c} = (a+b)(\frac{1}{c}) = (a)(\frac{1}{c}) + (b)(\frac{1}{c}) = \frac{a}{c} + \frac{b}{c}$$

4.2 面積を発明する

長方形の”面積”がなんであろうと、それは長方形の横と縦の長さに左右される (無関係な”面積”を定義したければしてもよいが)。 この内容を略号を使って表すと

$$A(l,w) = ?$$

今、ある長方形の縦の長さをかえないで、横の長さを 2 倍すると、元の長方形が 2 つできるので面積は 2 倍になるはずと考える。また、横をそのままに縦を 2 倍しても面積は 2 倍になるはずなので、略号を使って表すと

$$A(l,2w) = 2A(l,w)$$
$$A(2l,w) = 2A(l,w)$$

そして、この文の 2 には特別な意味はなかったので、一般化すると

$$A(l,\#w) = \#A(l,w)$$
$$A(\#l,w) = \#A(l,w)$$

どんな数であろうとその数を装置の外にだせることがわかる。ここで、 $l = l \cdot 1$ とあらわせるので

$$A(l,w) = lA(1,w) = lwA(1,1)$$

この文は、は、長方形の面積は、縦かける横かける単位であることを表現している。

$$\frac{A(l,w)}{A(1,1)} = lw$$

こう書き直すと、縦かける横の値は、$A(l,w)$ の中に $A(1,1)$ がいくついれられるかを表す比の表現とみることもできる。

4.3 傾きを定義してみよう

山を登る険しさ (傾き) は、垂直方向の移動距離だけ、あるいは水平方向の移動距離だけでは決まらない。これを傾き (S), 水平 (h, horizontal), 垂直 (v, vertical) で表すと

$$S(h,v) = ?$$

直線では、どの 2 点間をとっても傾きは同じであってほしい。これを表すと

$$S(h,v) = S(2h,2v)$$

そして、抽象化すると

$$S(h,v) = S(\#h,\#v)$$

傾きが何を意味するにしても、水平な線の傾きはゼロであったほうが直感に合致するので $S(h,v) = \frac{h}{v}$ は除外される。今のところの候補は

$$S(h,v) = \frac{v}{h}$$

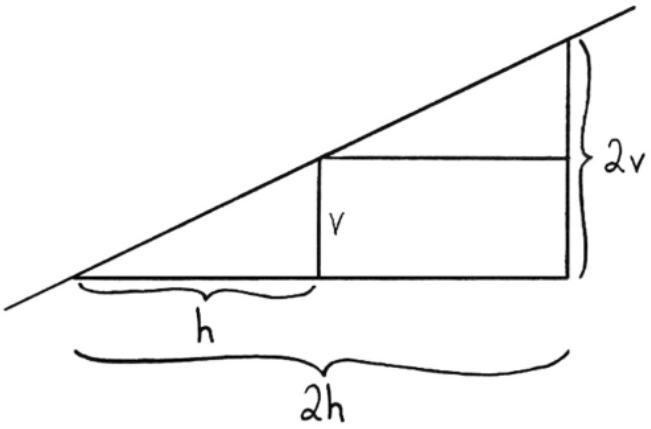


図 1　caption だよ

次に、水平距離を一定にして、垂直距離を#倍にしたとき傾きも#倍になってほしいので、以下の性質が必要

$$S(h, \#v) = \#S(h, v)$$

仮に、垂直距離を 2 倍にしたときは (ここでは $S = (\frac{h}{v})^{\#}$) の可能性を考慮にいれている)

$$S(h, 2v) = (\frac{2v}{h})^{\#} = 2^{\#}(\frac{v}{h})^{\#} = 2^{\#}S(h, v)$$

日常の理解を成り立たせるにはこの結果が 2 になってほしいので#は 1 になる。ここでも $\frac{v}{h}$ が生き残る

4.4　直線を表現してみよう

直線がある装置 $M(x)$ で表されているとする。どんな数 $x, \tilde{x}$ に対しても、以下がなりたつはず

$$\frac{(1\text{ 点の垂直位置}) - (\text{もう }1\text{ 点の垂直位置})}{(1\text{ 点の水平位置}) - (\text{もう }1\text{ 点の水平位置})} \equiv \frac{\text{垂直距離}}{\text{水平距離}} \equiv \frac{M(x) - M(\tilde{x})}{x - \tilde{x}} = \#$$

つまりどの 2 点間をえらんでも、傾きは一定 (#) となる。 そして、(たまたま) $\tilde{x}$ が 0 の場合

$$\frac{M(x) - M(0)}{x} = \#$$
$$M(x) = \#x + M(0)$$

M(0) は一部で y 切片とよばれ、#と M(0) を別の略号に書き直すと

$$M(x) = ax + b$$

となり、おなじみの直線の文になった。

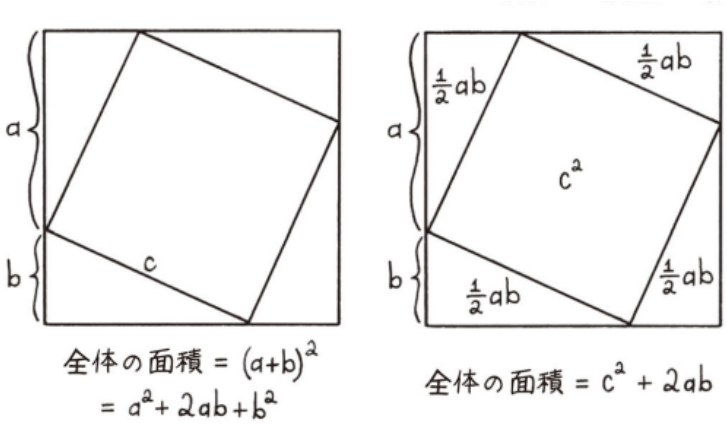


図 1.11　全体の面積を 2 通りのやり方で表すことによって、近道の道のりの公式——教科書が「ピタゴラスの定理」と呼ぶもの——を発明することができる。

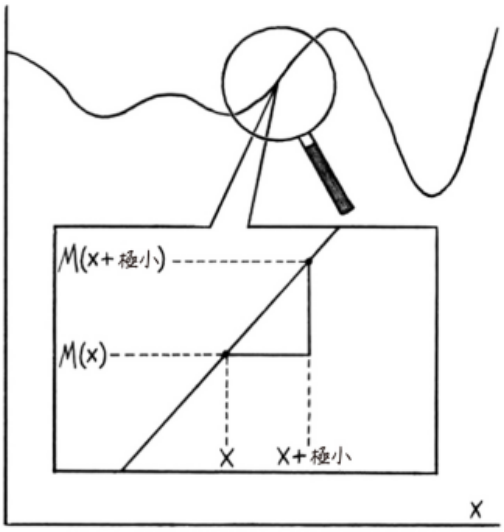
4.5　近道の公式

$$c^2 + 2ab = a^2 + 2ab + b^2$$
$$c^2 = a^2 + b^2$$

5　微分

まがったグラフの傾きをどのように表現するか。まがっているものは扱えないので、ある 1 点を無限に拡大してそこに直線をみいだすというアプローチを採用する。そうすると点 x での傾きは

$$x \text{ における } M \text{ の傾向} \equiv \frac{\text{極小垂直変位}}{\text{極小水平変位}} \equiv \frac{\text{垂直距離}}{\text{水平距離}} \equiv \frac{M(x + \text{極小}) - M(x)}{(x + \text{極小}) - x}$$



曲がったものの上の適当な点を選んで、無限に拡大する。いったん拡大してしまえば、直線のように扱うことができる。たとえば、互いに無限に近い2点の「水平距離分の垂直距離」を見さえすれば、（拡大した点における）険しさを定義することができる。