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