第 11 章

コンピュータとアルゴリズム

西関 隆夫

内容

1. まえがき

アルゴリズムは問題を解く手続きであり，プログラムやソフトウェアの基本である．同じ問題を解くのでも，使うアルゴリズムによって速く解けたり，計算時間がたくさんかかったりする．本講義では小学校の算数の時間に習う最大公約数を求める問題を例にして，アルゴリズム設計の“こつ”と解析の仕方を伝授する．

2. 最大公約数

60 と 36 の最大公約数はいくつだろうか．小学校で習った方法を思い出してみよう．60 を割り切る素数，即ち 60 の素因数は 2, 3 および 5 であり，特に 2^2 も 60 を割り切るので，60 の素因数分解は

$$60 = 2^2 \times 3 \times 5$$

である．同様に 36 を素因数分解すると

$$36 = 2^2 \times 3^2$$

となる．よって 60 と 36 の共通な素因数は 2 と 3 であり，特に 2 の方は 2^2 が共通なので，60 と 36 の最大公約数 (greatest common divisor) $gcd\{60,36\}$ は

$$gcd\{60,36\} = 2^2 \times 3 = 12$$

であることがわかる．

「簡単，簡単，最大公約数なんて小学校の問題でお茶の子さいさい．
なんで大学の講義で扱うのか」

と思うかもしれない．

じゃあ，$a = 11,188,907$ と $b = 2,798,251$ の最大公約数を求めてごらん．

$a = 11,188,907$ の素因数分解は求まったかな．a は奇数だから 2 では割り切れない．3 でも割り切れない．2 で割り切れないのだから 4 でも割り切れない．5 でも割り切れない．以下，同じことを根気よく 2,730 回続けると，a は 2,731 で割り切れることがやっとわかる．このようにして a の素因数を 1 個求めるのに 2,730 回も割り算を実行しないといけない．上のような単純な方法では，運が悪いと a の素因数を 1 個求めるのに約 $\sqrt{a}$ 回も割り算をしないといけない．というのも，a が 同じ位の大きさの 2 つの素因数 n と m に素因数分解できる，即ち $a = nm$ とすると，n と m は 約$\sqrt{a}$ であるからである．上の例で a を 2,731 で割ると商は 4,097 である．上と同様にして 4,097 の素因数を求めていくと，1 と 4,097 自身しかないこと，即ち 4,097 は素数であることがわかる．結局 a の素因数分解は

$$a = 2,731 \times 4,097$$

であることがわかる．

同様にして b の素因数分解を求めると

$$b = 683 \times 4,097$$

が求まる.

よって, a と b の最大公約数は

$$gcd\{a,b\} = 4,097$$

であることがわかる.

上のような小学校で習った単純な方法では, $gcd\{a,b\}$ を求めるのに運が悪いと $\sqrt{a}$ 回や $\sqrt{b}$ 回も割り算を実行しないといけない. 小学校のテストのときのように a や b が小さければよいが, a や b が 10 進 200 桁もの大きい数であると膨大な計算時間がかかってしまう. (このような素因数分解の難しさを利用して, 最近の暗号では, 解読されないようにしているんだね.)

3. Euclid の互除法

最大公約数を求める高速なアルゴリズムとして Euclid の互除法が知られている. これを説明しよう.

$a = 60$, $b = 36$ とする. 大きい a を小さい b で割ると

$$\begin{array}{r} 1 \\ 36 \overline{)\ 60} \\ \underline{36} \\ 24 \end{array} \tag{1}$$

である. 即ち, 商は 1 で余りは 24 である. 次に, この余り 24 で, 前回の割る数 36 を割ると

$$\begin{array}{r} 1 \\ 24 \overline{)\ 36} \\ \underline{24} \\ 12 \end{array} \tag{2}$$

となり, 余りが 12 である. 次にこの余り 12 で, 前回の割る数 24 を割ると

$$\begin{array}{r} 2 \\ 12 \overline{)\ 24} \\ \underline{24} \\ 0 \end{array} \tag{3}$$

となり，余り 0 になる．このように割り算を繰り返していき，余りが 0 になった時，即ち割り切れた時の割る数 12 が 60 と 36 の最大公約数である．

上の 3 回の割り算 (1), (2) および (3) をまとめて次の形に書こう．

$$\begin{array}{r} 1 \\ 36\overline{)\,60} \\ \underline{36} \\ 24 \end{array} \qquad \begin{array}{r} 1 \\ 24\overline{)\,36} \\ \underline{24} \\ 12 \end{array} \qquad \begin{array}{r} 2 \\ 12\overline{)\,24} \\ \underline{24} \\ 0 \end{array} \tag{4}$$

では，どうして上の方法で正しく最大公約数 12 が求まるのだろうか．最初の割り算 (1) では $a = 60$ を $b = 36$ で割っており，商が $q = 1$ で，余りが $r = 24$ である．これを数式で書くと

$$60 = 1 \times 36 + 24 \tag{5}$$

$$a = qb + r \tag{6}$$

となる．

式 (5), (6) からまず次の (i) がわかる．

(i) a と b のどんな公約数も b と r の公約数である．

なぜならば，c を a と b の任意の公約数とすると，c は a も b も割り切る．即ち

$$a = nc \tag{7}$$

$$b = mc \tag{8}$$

なる整数 n と m がある．式 (6), (7) および (8) により

$$\begin{aligned} r &= a - qb \\ &= nc - qmc \\ &= (n - qm)c \end{aligned} \tag{9}$$

である．n, m, q は整数なので $n - qm$ も整数である．よって，c は r の約数である．むろん c は b の約数である．したがって c は b と r の公約数である．

同様にして，(i) とは逆に次の (ii) も式 (6) から直ちにわかる．

(ii) b と r のどんな公約数も a と b の公約数である.

(i) と (ii) から a と b の公約数で最大なもの，即ち最大公約数は，b と r の最大公約数である．即ち次の (iii) がいえる.

$$\text{(iii)}\ gcd\{a,b\} = gcd\{b,r\}$$

よって $a = 60$, $b = 36$ なる上の例では

$$gcd\{60,36\} = gcd\{36,24\} \tag{10}$$

である．したがって $a = 60$ と $b = 36$ の最大公約数 $gcd\{60,36\}$ を求める代りに，b と $r = 24$ の最大公約数 $gcd\{36,24\}$ を求めればよい.

では $gcd\{36,24\}$ を求めるにはどうしたらよいか．36 と 24 の小さい方 $r = 24$ で大きい方 $b = 36$ を割ると，余りは $r' = 12$ なので,

$$gcd\{36,24\} = gcd\{24,12\} \tag{11}$$

である．よって $gcd\{36,24\}$ を求める代りに，$gcd\{24,12\}$ を求めればよい.

次に $r' = 12$ で 24 を割ると，割り切れて，余りは 0 である．即ち

$$gcd\{24,12\} = 12 \tag{12}$$

である.

式 (10), (11) および (12) から

$$gcd\{60,36\} = gcd\{36,24\} = gcd\{24,12\} = 12$$

であることがわかり，Euclid の互除法で正しく最大公約数 12 が求まることがいえた.

もう一つの例 $a = 11,188,907$, $b = 2,798,251$ について示すと

$$\begin{array}{r|l}
 & 3 \\ \hline
2,798,251 & 11,188,907 \\
 & 8,394,753 \\ \hline
 & 2,794,154
\end{array}
\qquad
\begin{array}{r|l}
 & 1 \\ \hline
2,794,154 & 2,798,251 \\
 & 2,794,154 \\ \hline
 & 4,097
\end{array}
\qquad
\begin{array}{r|l}
 & 682 \\ \hline
4,097 & 2,794,154 \\
 & 2,794,154 \\ \hline
 & 0
\end{array}$$

となり，正しく最大公約数 4,097 が求まる.

Euclid の互除法を使うと上の 2 つの例では割り算は 3 回しか必要ない．このように Euclid の互除法は素因数分解法より圧倒的に速いことがわかる.

4. アルゴリズムの計算時間

Euclid の互除法で最大公約数が求まるまでに割り算を何回位繰り返す必要があるのだろうか.

60 と 36 の最大公約数を求める計算過程の (4) をもう一度見てみよう.

$$
\begin{array}{rr}
 & 1 \\
36 & \overline{)\ 60} \\
 & \underline{36} \\
 & 24
\end{array}
\qquad
\begin{array}{rr}
 & 1 \\
24 & \overline{)\ 36} \\
 & \underline{24} \\
 & 12
\end{array}
\qquad
\begin{array}{rr}
 & 2 \\
12 & \overline{)\ 24} \\
 & \underline{24} \\
 & 0
\end{array}
\tag{4}
$$

(4) では割り算が 3 回実行されている. それら 3 回の割り算で割る数はそれぞれ 36, 24, 12 であり,

$$36 > 24 > 12$$

と段々小さくなる. なぜならば, 36 で 60 を割った余りが 24 なので, 余り 24 は割る数 36 より小さい. また 24 で 36 を割った余りが 12 なので, 余り 12 は割る数 24 より小さいからである.

割る数が段々小さくなるので, いずれ割り切る. というのも, 割る数が小さくなって 1 になれば, 必ず割り切るからである.

運悪く割る数が毎回 1 しか小さくならないとしても, 高々36 回しか割り算は必要ない. しかし, それでは小学校で習った素因数分解と同じ位計算がかかることになってしまう. でも実際は割り算は 3 回で済んでいた. もっと上手い考え方はないのだろうか.

最初の割り算 (1) の式

$$60 = 1 \times 36 + 24 \tag{5}$$

をもう一度見てみよう. 割る数 36 は余り 24 より大きく, 商は必ず 1 以上であるので,

$$60 = 1 \times 36 + 24 > 24 + 24 = 2 \times 24$$

であり,

$$24 < 60/2$$

である. つまり余りは割られる数の半分以下である.

2 番目の割り算 (2) の式

$$36 = 1 \times 24 + 12$$

においても，$24 > 12$ で，商は 1 以上であるので，

$$36 > 12 + 12 = 2 \times 12$$

であり，

$$12 < 36/2$$

である．

このように 3 番目の割り算 (3) での割る数 12 は 1 番目の割り算 (1) での割る数 36 の半分以下である．

この事実は一般に成り立っている．一番目の割り算の式

$$a = qb + r \tag{6}$$

で，$b > r$ かつ $q \geq 1$ なので

$$a > r + r = 2r$$

であり，

$$r < a/2$$

である．2 番目の割り算では，r で b を割る．そのときの商を q' とし，余りを r' とすると，

$$b = q'r + r'$$

である．$r > r'$ かつ $q' \geq 1$ なので

$$r' < b/2$$

である．このように，3 番目の割り算の割る数 r' は 1 番目の割り算の割る数 b の半分以下である．

同じようにして，5 番目は 3 番目の半分以下，7 番目は 5 番目の半分以下である．

$a > b$ なる 2 つの数 a と b の最大公約数を Euclid の互除法で求めるとき割り算が N 回実行されたとし，割る数の数列を $b_1(= b), b_2, b_3, \cdots, b_N$ としよう．$a = 60, b = 36$ の例では $N = 3$ であり，b_1, b_2, b_3 は $36, 24, 12$ である．上で示したように数列 $b_1, b_2, \cdots, b_N$ は単調に減少するばかりでなく，一つおきに半分，半分と等比級数的に減少する．即ち

$$\begin{aligned} b_3 &< b_1/2 \\ b_5 &< b_3/2 < b_1/2^2 \\ b_7 &< b_5/2 < b_1/2^3 \\ &\vdots \end{aligned}$$

である．よって $n(\leq N)$ を $n = 2m + 1$ なる奇数としたとき，n 番目の割る数 b_n は

$$b_n < b_1/2^m$$

である．

もし右辺 $b_1/2^m$ の分母 2^m が b_1 以上になってしまうと，右辺は 1 以下になり，$b_n < 1$ 即ち $b_n = 0$ となってしまい，$(n-1)$ 回目の割り算が割り切れていたことになるので，分母 2^m は $b_1(=b)$ より小さい．即ち

$$2^m < b$$

である．底が 2 の対数を両辺に対してとると

$$m = \log_2 2^m < \log_2 b$$

を得る．よって

$$n = 2m + 1 < 2\log_2 b + 1 \tag{13}$$

である．

式 (13) からわかるように，割り算の回数 N は，N が奇数ならば $N < 2\log_2 b + 1$ である．一方 N が偶数ならば，$n = N - 1$ は奇数であり，$n < 2\log_2 b + 1$ なので，$N = n + 1 < 2\log_2 b + 2$ である．いずれにしろ，割り算の回数 N は

$$N < 2\log_2 b + 2 \tag{14}$$

である．

では $\log_2 b$ はどの位の数なのだろうか．$b = 36$ は 10 進 2 桁の数であり，$b = 2,798,251$ は 10 進 7 桁の数である．b が 10 進 c 桁の数であるとすると，

$$b < 10^c$$

であるので，

$$\log_2 b < \log_2 10^c = c\log_2 10 \simeq 3.3c \tag{15}$$

である．

式 (14) と (15) により

$$\boxed{N < 6.6c+2} \tag{16}$$

である．このように割り算の回数 N は b の桁数 c の約 6 倍以下である．

Euclid の互除法の計算時間は割り算の回数 N で決まり，運が悪くいつも商が 1 で余りが (割る数) -1 であっても，N は式 (16) のように a, b の小さい方の数 b の桁数 c の 6 倍程度で抑えられる．

アルゴリズムの計算時間はこのように解析される．これを最悪計算時間解析という．実際には，いつも商が 1 で，余りが (割る数) -1 であるような運が悪いことが続くことは稀なので，割り算の回数 N は $6.6c + 2$ よりもずっと少い．

$b = 36$ のとき $c = 2$ なので

$$N < 6.6 \times 2 + 2 = 15.2$$

であり，$gcd\{60, 36\}$ を求めるのに割り算は高々15 回しか必要ないことがわかる．

一方 $b = 2,798,251$ のとき $c = 7$ なので

$$N < 6.6 \times 7 + 2 = 48.2$$

であり，$gcd\{11,188,907,\ 2,798,251\}$ を求めるのに割り算は高々48 回しか必要ないことが理論上わかる．

しかし，どちらの場合も実際には割り算はたったの 3 回しか必要ない．

5. アルゴリズム設計の “こつ”

最大公約数を求める問題を解くアルゴリズムとして，素因数分解法と Euclid 互除法の 2 つを説明し，Euclid 互除法が圧倒的に高速であることを示した．このような効率のよいアルゴリズムを設計する “こつ” はあるのだろうか．

碁や将棋に必勝法がないように，効率のよいアルゴリズムを設計する万能の方法はない．しかし碁や将棋に定石があるように効率のよいアルゴリズムの設計に役立つ，お決まりの方法がいくつか知られている．その一つとして，大きな問題をより小さい問題に帰着させる方法がある．Euclid の互除法は，大きい数 a, b の最大公約数を求める問題を，より小さい数 b, r の最大公約数を求める問題に帰着させている．

この他にも分割統治法という方法がある．これは問題を一度に解くのではなく，問題を 2 つに分割して独立に解き，それらの解をうまく統合して元の問題を解く方法である．名前の由来は大英帝国時代の植民地統治のやり方から来ている．この方法は 2 つの数の最大公約数を求める問題には適用できそうにない．しかし，多くの数，例えば n 個の数 $a_1, a_2, \cdots, a_n$ が与えられた時に，それらの最大公約数を求める問題には分割統治法が適用できるであろう．学生諸君は自分で考えてみよう．(演習問題 (3) 参照．)

アルゴリズムのもっとおもしろい話は工学部情報工学科の講義「情報数学」や「アルゴリズムとデータ構造」を聞きに来て下さい．

6. 演習問題

(1) 2,094,081 と 1,046,017 の最大公約数を求めよ．
(2) 3,069 と 2,047 の最大公約数を求めよ．
(3) 次の 8 個の数の最大公約数を求めよ．
14,196, 4,914, 2,457, 1,911, 6,825, 4,095, 5,915, 11,375

(答え)
(1) 2,047
(2) 3,069 と 2,047 は互いに素であり，それらの最大公約数は 1 である．
(3) 91