基礎情報科学
～ アルゴリズムとは ～

阿萬 裕久（あまん ひろひさ）
aman@ehime-u.ac.jp
（総合情報メディアセンター）

まずは簡単な数学の問題（中学生レベル）

544 と 119 の
最大公約数
を求めなさい

（制限時間 3 分）

答え $\boxed{17}$

それぞれ素因数分解すると

- $544 = 2 \times 2 \times 2 \times 2 \times 2 \times 17$
- $119 = 7 \times 17$

求め方（解法）を確認すると

① 二つの数を a, b として，a と b それぞれの**素因数分解**を行う

$a = 544 = 2 \times 2 \times 2 \times 2 \times 2 \times 17$

$b = 119 = 7 \times 17$

② a の素因数分解と b の素因数分解の**両方に登場する素数**を**できるだけ多く**見つける

③ 上で見つかった**共通の素数の積**が最大公約数である

別の例でも計算すると

$a = 500, b = 120$ の場合

$$a = 500 = 2 \times 2 \times 5 \times 5 \times 5$$
$$b = 120 = 2 \times 2 \times 2 \times 3 \times 5$$

より

最大公約数 $= 2 \times 2 \times 5 = 20$

最大公約数を求める別の方法

①二つの数を a, b とする．ただし，$a > b$．
② a を b で割った余りを r とする．
③ $r \neq 0$ ならば④へ，さもなくば⑧へ進む．
④ b を a に代入する($a \leftarrow b$)．
⑤ r を b に代入する($b \leftarrow r$)．
⑥ a を b で割った余りを r とする．
⑦ ③へ戻る．
⑧ この時点での b が求める最大公約数である．

（例） $a = 544, \ b = 119$

①二つの数を a, b とする．ただし，$a > b$．
② a を りを r とする．
③ $r \neq$ さもなくば⑦へ進む．
④ b を a に代入する($a \leftarrow b$)．
⑤ r を b に代入する($b \leftarrow r$)．
⑥ ③へ戻る．
⑦ この時点での b が求める最大公約数である．

$a = 544$
$b = 119$

（例） $a = 544, \ b = 119$

①二つの数を a, b とする．ただし，$a > b$．
② a を b で割った余りを r とする．
③ $r \neq 0$ 進む．
④ b を a
⑤ r を b
⑥ a を b
⑦ ③へ戻る．
⑧ この時点での b が求める最大公約数である．

$a = 544$
$b = 119$
$544 \div 119 = 4 \cdots 68$
$r = 68$

計算過程

	a	b	r
1回目	544	119	68

配布した用紙の裏面にこの表があるので，
一緒に書き込んでいきましょう
（二つある表の**上の方を使用**します）

（例） $a = 544,\ b = 119$

①二つの数を a, b とする．ただし，$a > b$．
② a を b で割った余りを r とする．
③ $r \neq 0$ ならば④へ，さもなくば⑧へ進む．
④ b を a に代入する（$a \leftarrow b$）．
⑤ r を b に
⑥ a を b で
⑦ ③へ戻る
⑧ この時点での b が求める最大公約数である．

$a = 544 \ \rightarrow\ 119$
$b = 119$
$r = 68$

（例） $a = 544,\ b = 119$

①二つの数を a, b とする．ただし，$a > b$．
② a を b で割った余りを r とする．
③ $r \neq 0$ ならば④へ，さもなくば⑧へ進む．
④ b を a に代入する（$a \leftarrow b$）．
⑤ r を b に代入する（$b \leftarrow r$）．
⑥ a を b で割
⑦ ③へ戻る．
⑧ この時点で　約数である．

$a = 119$
$b = 119 \rightarrow 68$
$r = 68$

計算過程

	a	b	r
1回目	544	119	68
2回目	119	68	

（例） $a = 544,\ b = 119$

①二つの数 … b.
② a を b で
③ $r \neq 0$ な … 進む.
④ b を a に
⑤ r を b に代入する($b \leftarrow r$).
⑥ a を b で割った余りを r とする.
⑦ ③へ戻る.
⑧ この時点での b が求める最大公約数である.

$a = 119$
$b = 68$
$119 \div 68 = 1 \cdots 51$
$r = 51$

計算過程

	a	b	r
1回目	544	119	68
2回目	119	68	51

（例） $a = 544,\ b = 119$

①二つの数を a, b とする. ただし, $a > b$.
② a を b で割った余りを r とする.
③ $r \neq 0$ ならば④へ, さもなくば⑧へ進む.
④ b を a に代入する($a \leftarrow b$).
⑤ r を b に代入する($b \leftarrow r$
⑥ a を b で割った余りを r と
⑦ ③へ戻る.
⑧ この時点での b が求める最大公約数である.

$a = 119 \rightarrow 68$
$b = 68$
$r = 51$

（例） $a = 544,\ b = 119$

①二つの数を a, b とする. ただし, $a > b$.
② a を b で割った余りを r とする.
③ $r \neq 0$ ならば④へ, さもなくば⑧へ進む.
④ b を a に代入する($a \leftarrow b$).
⑤ r を b に代入する($b \leftarrow r$).
⑥ a を b で割った余りを
⑦ ③へ戻る.
⑧ この時点での b が求 … ある.

$a = 68$
$b = 68 \rightarrow 51$
$r = 51$

計算過程

	a	b	r
1回目	544	119	68
2回目	119	68	51
3回目	68	51	

（例） $a = 544,\ b = 119$

①二つの数を ... $> b$.
② a を b で割...
③ $r \neq 0$ なら... 進む.
④ b を a に...
⑤ r を b に代入する($b \leftarrow r$).
⑥ a を b で割った余りを r とする.
⑦ ③へ戻る.
⑧ この時点での b が求める最大公約数である.

$a = 68$
$b = 51$
$68 \div 51 = 1 \cdots 17$
$r = 17$

計算過程

	a	b	r
1回目	544	119	68
2回目	119	68	51
3回目	68	51	17

（例） $a = 544,\ b = 119$

①二つの数を a, b とする. ただし, $a > b$.
② a を b で割った余りを r とする.
③ $r \neq 0$ ならば④へ, さもなくば⑧へ進む.
④ b を a に代入する($a \leftarrow b$).
⑤ r を b に代入する($b \leftarrow$ ...
⑥ a を b で割った余りを ...
⑦ ③へ戻る.
⑧ この時点での b が求める最大公約数である.

$a = 68 \rightarrow\ 51$
$b = 51$
$r = 17$

（例） $a = 544,\ b = 119$

①二つの数を a, b とする．ただし，$a > b$．
② a を b で割った余りを r とする．
③ $r \neq 0$ ならば④へ，さもなくば⑧へ進む．
④ b を a に代入する（$a \leftarrow b$）．
⑤ r を b に代入する（$b \leftarrow r$）．
⑥ a を b で割った余りを r とする．
⑦ ③へ戻る．
⑧ この時点での b が求める最大公約数である．

$$a = 51$$
$$b = 51 \rightarrow 17$$
$$r = 17$$

計算過程

	a	b	r
1回目	544	119	68
2回目	119	68	51
3回目	68	51	17
4回目	51	17	

（例） $a = 544,\ b = 119$

①二つの数を a, b とする．ただし，$a > b$．
② a を b で割った余りを r とする．
③ $r \neq 0$ ならば④へ，さもなくば⑧へ進む．
④ b を a に代入する（$a \leftarrow b$）．
⑤ r を b に代入する（$b \leftarrow r$）．
⑥ a を b で割った余りを r とする．
⑦ ③へ戻る．
⑧ この時点での b が求める最大公約数である．

$$a = 51$$
$$b = 17$$
$$51 \div 17 = 3 \cdots 0$$
$$r = 0$$

計算過程

	a	b	r
1回目	544	119	68
2回目	119	68	51
3回目	68	51	17
4回目	51	17	0

（例） $a = 544,\ b = 119$

①二つの数を a, b とする．ただし，$a > b$．
② a を b で割った余りを r とする．
③ $r \neq 0$ ならば④へ，さもなくば⑧へ進む．
④ b を a に代入する($a \leftarrow$
⑤ r を b に代入する($b \leftarrow$
⑥ a を b で割った余りを r
⑦ ③へ戻る．
⑧ この時点での b が求める最大公約数である．

$a = 51$
$b = 17$
$r = 0$

（例） $a = 544,\ b = 119$

①二つの数を a, b とする．ただし，$a > b$．
② a を b で割った余りを r とする．
③ $r \neq 0$ ならば④へ，さもなくば⑧へ進む．
④ b を a に代入する($a \leftarrow$
⑤ r を b に代入する($b \leftarrow$
⑥ a を b で割った余りを r
⑦ ③へ戻る．
⑧ この時点での b が求める最大公約数である．

$a = 51$
$b = 17$
$r = 0$

計算過程

	a	b	r
1回目	544	119	68
2回目	119	68	51
3回目	68	51	17
4回目	51	17	0

17

【問題】以下の手順で 528 と 154 の最大公約数を求めよ

①二つの数を a, b とする．ただし，$a > b$．
② a を b で割った余りを r とする．
③ $r \neq 0$ ならば④へ，さもなくば⑧へ進む．
④ b を a に代入する($a \leftarrow b$)．
⑤ r を b に代入する($b \leftarrow r$)．
⑥ a を b で割った余りを r とする．
⑦ ③へ戻る．
⑧ この時点での b が求める最大公約数である．

計算結果

	a	b	r
1回目	528	154	66
2回目	154	66	22
3回目	66	22	0

22

なぜこの方法で最大公約数が求まるのか？

【基本となる性質】

a を b で割った余りを $r\ (\neq 0)$ としたとき，
「x が a と b の公約数」⇔「x が b と r の公約数」

（例） { 544 と 119 の公約数 }

（※ 544 を 119 で割った余りが 68 なので）

= { 119 と 68 の公約数 }

（※ 119 を 68 で割った余りが 51 なので）

= { 68 と 51 の公約数 }

（※ 68 を 51 で割った余りが 17 なので）

= { 51 と 17 の公約数 }（※ 51 は 17 で割り切れるので）

最大公約数は 17

ユークリッドの互除法

- この方法を**ユークリッドの互除法**という
- 英語では Euclidean algorithm という

※ユークリッドの互除法は世界最古のアルゴリズムと言われている（B.C.300年頃）

「アルゴリズム」

問題の解き方を曖昧さ無く，明確に表したもの

アルゴリズムを**コンピュータで実行できるように書いたものがコンピュータプログラム**（**ソフトウェア**）
※正確な表現ではないが，スマホのアプリもある種のアルゴリズムに従って動作するように作られている

アルゴリズムの重要性

- **コンピュータの性能は年々向上**
  - 正しくは**計算が速く**なったり，データの**読み書きが速く**なったり，一度に処理できる**データ量が多くなったり**というものである
- **よく勘違いされる**が決してコンピュータが**賢くなったわけではない**！
  - コンピュータは**プログラムに書かれたことを実行するだけ**であり，**賢いアルゴリズム**を**人間が考え出さなければ宝の持ち腐れ**になるのである

※「**AI（人工知能）がどうにかしてくれる**」というのは少々楽観的で過度な期待も含まれている．実際，AI 自体が「何をどう学習するか」は与えられたプログラムで決まる．