プログラミングの背景：数論

ユークリッドの互除法

tbasic.org [*1]

[2014 年 6 月版]

> ユークリッドの互除法は今日まで生き残っている意味のあるアルゴリズムのうち最古のもので，あらゆるアルゴリズムの祖父と呼ぶことができる。
>
> （ドナルド・クヌース
> 「The Art of Computer Programming 」）

ユークリッドの互除法は最大公約数を計算する効率的な方法です。この方法の起源は古く，しかも，現在でも重要なアルゴリズムとして使われています。クヌースが述べているように，アルゴリズムの祖父とも譬えられています。

ここではこれについて説明します。

目次

[*1] http://www.tbasic.org

1　ユークリッドの互除法の由来

ユークリッド（-330？〜-275）はユークリッド幾何学の名前で有名な古代ギリシアの数学者です。ユークリッドは非常に有名ですが，ユークリッド自身についてはあまり知られていません。確実なことは彼が「原論」と言われる著作を 残したことぐらいです。[*2]

「原論」はいわゆるユークリッド幾何学の原典です。このユークリッド「原論」は全 13 巻からなる大著で，その全貌を見るのは大変ですが，幸い日本語訳が出ていて，身近に触れることも出来ます。比較的大きな図書館には蔵書されていると思いますから，興味のある人は一度ご覧になってみると良いと思います。

この「原論」は幾何学だけでなく数論も含んだ，当時のギリシア正統的数学の集大成ともいえるものです。ユークリッドの互除法は「原論」第 7 巻命題 1 から命題 3 に書かれている方法のことです。ユークリッドの互除法という名前もこのことに由来します。数学史の研究によると，「原論」はユークリッド自身の著作と言うよりは，当時の数学をまとめた著作と言われています。そしてこの成果はもう少し前のピタゴラスの時代のものと言われています。ですから本当はピタゴラスの互除法というのが正しいかもしれません。もっとも，古代中国や古代インドでも似たようなアルゴリズムがありますので，何処が本当の起源かは不明です。

2　ユークリッドの互除法とは

ユークリッドの互除法は 2 つの自然数 a, b の最大公約数を計算する方法です。

2 つの数の最大公約数は，それらを測るときの最大の共通尺度で，数を扱うときの基本的な量と言えます。そのことから，最大公約数を求めることは，数を扱う学問の中では最も基本的な問題として扱われてきました。

a と b の最大公約数を求めるためによく行われる方法として，a と b を素因数分解してその共通項を見つけるというものがあります。この方法は小さい数の場合は計算に適していますが，a と b が少し大きくなるとこの方法での計算は難しくなります。

例えば，15 と 21 の最大公約数を求めてみます。15 と 21 の素因数分解は，それぞれ

$$15 = 3 \cdot 5 \quad \text{かつ} \quad 21 = 3 \cdot 7$$

なので，15 と 21 の最大公約数は それらの共通項 3 となります。

しかし，62873258567731 と 62908468304971 の最大公約数をこの方法で簡単に計算できるでしょうか。勿論頑張って，62873258567731 と 62908468304971 の素因数分解を見つけるという道もあります。しかし，実は

大きな数の素因数分解は難しいことがある

[*2] ユークリッドの「原論」は昔「幾何学原論」といわれたこともありました。しかし，この本は幾何学に限らず多くの内容を含みますので，現在では元々の名称「原論」と言われています。

のです[*3]。この難しいという意味は，スーパーコンピューターを使っても現実的にはほぼできないものがあるということです。この「大きな数が素因数分解が難しいことがある」と言う事実は有名なことで，暗号系の中にはこの事実を使って安全性を保証しているものもあります。

一般に素因数分解は難しいのですが，実は最大公約数の計算にはそれに比べてはるかに簡単で，効率的な良い方法があるのです。それがユークリッドの互除法です。例えば 1000 桁の 2 個の数が与えられたとき，それらの最大公約数もユークリッドの互除法を使えばパソコン上でもすぐに計算できます[*4]。

3 ユークリッドの互除法の原理

整数 $a,b \in \mathbb{Z}$ の最大公約数を $\gcd(a,b)$ と表すことにします。ここで，a,b のうち少なくとも一方は 0 ではないとします。ユークリッドの互除法は次の性質に基づいています。

ユークリッドの互除法の基本原理

$a > b \in \mathbb{N}$ とし，a を b で割った時の商を $q \in \mathbb{N}$，余りを r とする。($r = 0$ または，$r \in \mathbb{N}$)，即ち

$$a = q \cdot b + r, \quad 0 \leqq r < b$$

と表されたとする。このとき，$\gcd(a,b) = \gcd(b,r)$ となる。

証明. 少しだけ抽象的な証明をしてみましょう。

C_1 を a と b の公約数全体の成す集合とします。つまり，

$$C_1 = \{x \in \mathbb{Z} \mid x \text{ は } a \text{ の約数かつ } b \text{ の約数}\}$$

とします。同様に，C_2 を b と r の公約数全体の成す集合とします。つまり，

$$C_2 = \{x \in \mathbb{Z} \mid x \text{ は } b \text{ の約数かつ } r \text{ の約数}\}$$

とします。ここで証明することは，$C_1 = C_2$ です。

(i) $x \in C_1$ とします。このとき， x は a の約数かつ b の約数です。(記号で書くと，$x \mid a$ かつ $x \mid b$ です。) ここで，$r = a - q \cdot b$ に注意すると，整除性の基本性質より，x は r の約数となります。(記号で書くと，$x \mid r$ です。) 従って，このとき，x は b の約数かつ r の約数です。故に，$x \in C_2$ となります。つまり，$C_1 \subset C_2$ が示されました。

(ii) 逆に $x \in C_2$ とします。このとき， x は b の約数かつ r の約数です。(記号で書くと，$x \mid b$ かつ $x \mid r$ です。) ここで，$a = q \cdot b + r$ に注意すると，命題 1.1(1) より，x は a の約数となります。(記号で書くと，$x \mid a$ です。) 従って，このとき，x は a の約数かつ b の約数です。故に，$x \in C_1$ となります。つまり，$C_2 \subset C_1$ が示されました。 □

[*3] ここで大きな数とは数百桁以上の数を意味して，この例にあるような 62873258567731 のような数のことではありません。実際，この数程度なら筆算では難しいでしょうが，適当なソフトウエアを使えば，パソコン上ですぐに素因数分解が可能です。

[*4] 勿論，1000 桁の数の計算には，対応した適切なソフトウエアが必要ですが，そのようなものは比較的簡単に利用できます。

4　ユークリッドの互除法

上に述べた基本原理の内容を説明しましょう。これは $a = q \cdot b + r$ としたとき， $\gcd(a,b)$ は $\gcd(b,r)$ に等しいと言っています。ですから，$\gcd(a,b)$ を求めるには， $\gcd(b,r)$ を求めれば良いわけです。ここで $a > b > r$ の関係があることに注意しましょう。a,b に比べて b,r の方が小さいので計算が簡単なはずです。もし $\gcd(b,r)$ が分からなかったら，今度は b を r で割って同様なことを行えばもっと簡単になります。上の操作は割り算が出来る間続けられますから，

$$\gcd(x,0),\quad x > 0$$

の形になるまで，続けられます。明らかにこの場合 $\gcd(x,0) = x$ ですから，これで求められました。

具体例で確かめましょう。

例 4.1 (62979284285501 と 62873258567731 の最大公約数)**.**
$a = 62979284285501, b = 62873258567731$ から始めて，順次，除法の定理を適用すると次が得られます。

$$\begin{aligned}
62979284285501 &= 1 \times 62873258567731 + 106025717770 &(1)\\
62873258567731 &= 593 \times 106025717770 + 7930121 &(2)\\
106025717770 &= 13370 \times 7930121 + 0 &(3)
\end{aligned}$$

上のことから，それぞれ

$$\begin{aligned}
\gcd(62979284285501, 62873258567731) &= \gcd(62873258567731, 106025717770) &(1)\\
\gcd(62873258567731, 106025717770) &= \gcd(106025717770, 7930121) &(2)\\
\gcd(106025717770, 7930121) &= \gcd(7930121, 0) = 7930121 &(3)
\end{aligned}$$

が得られます。従って，

$$\gcd(62979284285501, 62873258567731) = 7930121$$

となります。このようにユークリッドの互除法を使うと驚くほど簡単に最大公約数が得られました[*5]。

このように，62979284285501 と 62873258567731 の最大公約数を，因数分解を使わないで，互除法の原理を 3 回使うだけで，簡単に求めることが出来ました。

この方法を一般的に表すと次のようになります。

[*5] 因数分解が難しい場合でも，このように最大公約数が簡単に求められました。今の場合，この結果を使って，因数分解を思いつく人もいるでしょう。実際，公約数はそれぞれの数の因数になりますから，公約数でそれぞれを割って，

$$62979284285501 = 7930121 \cdot 7941781,\quad 62873258567731 = 7930121 \cdot 7928411$$

が得られます。実は今の場合，素因数分解になっています。この素因数分解を，結果を知らずに筆算あるいは電卓を用いて得るのは，かなり困難なことと予想されるでしょう。

ユークリッドの互除法

自然数 a, b $(a > b)$ に対して，a を b で割った時の余りを r とする。以下同様な操作を行い，n 回の除法の定理を適用して，次のようになったとする。$a = r_0$，$b = r_1$，$r = r_2$ として表す。

$$
\begin{array}{lcllll}
r_0 & = & q_1 & \cdot\ r_1 & +\ r_2 & (0 < r_2 < r_1) \\
r_1 & = & q_2 & \cdot\ r_2 & +\ r_3 & (0 < r_3 < r_2) \\
r_2 & = & q_3 & \cdot\ r_3 & +\ r_4 & (0 < r_4 < r_3) \\
 & \cdots & & & & \\
r_{i-2} & = & q_{i-1} & \cdot\ r_{i-1} & +\ r_i & (0 < r_i < r_{i-1}) \\
 & \cdots & & & & \\
r_{n-2} & = & q_{n-1} & \cdot\ r_{n-1} & +\ r_n & (0 < r_n < r_{n-1}) \\
r_{n-1} & = & q_n & \cdot\ r_n & &
\end{array}
$$

このとき，

$$\gcd(a, b) = \gcd(b, r) = \gcd(r_0, r_1) = \cdots = \gcd(r_{n-1}, r_n) = r_n$$

となる。即ち，r_n が a と b の最大公約数になる。

上のような操作を行ったとき，何回目かで，必ず，$r_{n-1} = q_n \cdot r_n$ の形になることに注意してください。実際，r_{i-2} が r_{i-1} で割り切れなければ，$r_i > 0$ が得られ，

$$a > b = r_1 > r_2 > \cdots > r_{i-2} > r_{i-1} > r_i > 0$$

となります。これらはすべて自然数ですから，このような条件を満たす r_i は b 個以上存在しません。従って，多くとも b 回以下でこれらの操作は終了することになります。

$\gcd(62979284285501, 62873258567731)$ の例では，$n = 3$ 回で終了しました。この回数は，この場合の $b = 62873258567731$ に比べて極めて少ないものとなっています。ユークリッド互除法が効率的であるといわれる理由は，この回数が b に比べて極めて少なくなることが一般に成立することによります。

今の場合は，回数が特に少なくなる例ですが，実はどのような場合でもあまり回数は多くなりません。

この回数の評価についてはラメの定理と言われる定理が有名です。以下ではこの定理を説明します。

5　ユークリッド互除法の回数とフィボナッチ数

ユークリッドの互除法での除法の定理を使う回数が多くなるのはどのような場合かを調べてみると，フィボナッチ数に出会います。フィボナッチ数は，色々なところで出会う不思議な数ですが，次で定義される数列です。

フィボナッチ数

$f_0 = 0,\ f_1 = 1$ とし，$i \geqq 2$ に対して，

$$f_i \ = \ f_{i-2} \ + \ f_{i-1}$$

で定義される数列をフィボナッチ数列と言う。f_i を i 番目のフィボナッチ数と言う。[*6]

フィボナッチ数の最初の方を計算してみると，

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ 144,\ 233,\ 377,\ 610,\ 987,\ 1597,\ 2584,\ \cdots$$

となります。最初の方はそれ程ではありませんが，次第に急激に大きくなります。例えば，

$$f_{10} = 55,\ \ f_{20} = 6765,\ \ f_{30} = 832040,\ \ f_{40} = 102334155,\ \ f_{50} = 12586269025$$

となります。

ユークリッド互除法とフィボナッチ数の関係を説明しましょう。ユークリッド互除法の過程

$$r_{i-2} = q_{i-1} \cdot r_{i-1} + r_i$$

を見ると，番号付けは逆ですが，フィボナッチの数列と似た式になっていいることに気が付きます。ここで，$q_i \geqq 1$ ですから，

$$r_{i-2} = q_{i-1} \cdot r_{i-1} + r_i \geqq r_{i-1} + r_i$$

が成立します。この右辺はフィボナッチ数の形です。このことに注意すると次の命題が成立することが分かります。

命題 5.1. 仮定と記号を前節ユークリッド互除法の通りとする。即ち，$a, b\ (a > b)$ に対して，ユークリッドの互除法を適用して

$$r_{n-1} = q_n \cdot r_n$$

となり，最大公約数 r_n が得られたとする。このとき，n 番目のフィボナッチ数 f_n に対して，

$$b \ \geqq \ f_{n+1}$$

が成立する。

[*6] 文献によっては，フィボナッチ数を，$F_0 = 1,\ F_1 = 1,\ \ldots$ と定義することもあります。ここでの定義と，番号付けがずれるだけですが，この場合，色々な結果もそれに応じて修正する必要があります。このように，フィボナッチの数の性質を使う場合は，その定義を確認する必要があります。

証明. まず，$r_{n-1} > r_n > 0$ より，

$$\begin{array}{rcl} r_n & \geqq & f_2 = 1 \\ r_{n-1} & \geqq & f_3 = 2 \end{array}$$

が分かります。更に，

$$\begin{array}{rcccccccc} r_{n-2} & = & q_{n-1} \cdot r_{n-1} + r_n & \geqq & r_{n-1} + r_n & \geqq & f_3 + f_2 & = & f_4 \\ r_{n-3} & = & q_{n-2} \cdot r_{n-2} + r_{n-1} & \geqq & r_{n-2} + r_{n-1} & \geqq & f_4 + f_3 & = & f_5 \\ r_{n-4} & = & q_{n-3} \cdot r_{n-3} + r_{n-2} & \geqq & r_{n-3} + r_{n-2} & \geqq & f_5 + f_4 & = & f_6 \end{array}$$
$$\cdots$$

となりますから，一般に，$0 \leqq i \leqq n$ に対して，

$$r_{n-i} = q_{n-i+1} \cdot r_{n-i+1} + r_{n-i+2} \geqq r_{n-i+1} + r_{n-i+2} \geqq f_{i+1} + f_i = f_{i+2}$$

が成立します。特に，$i = n - 1$ のとき，

$$b = r_1 = q_2 \cdot r_2 + r_3 \geqq r_2 + r_3 \geqq f_n + f_{n-1} = f_{n+1}$$

が得られます。 □

この命題を使って，ユークリッドの互除法の回数 n の評価ができます。

例 5.1 ($b = 12345$ の場合)**.**
$b = 12345$ とします。n をユークリッド互除法での除法の定理の適用回数とします。f_i を具体的に計算してみると，$f_{21} = 10946, f_{22} = 17711$ が得られます。上の命題によれば，

$$b = 12345 \geqq f_{n+1}$$

ですから，$n \geqq 21$ ではありません。即ち，$a > b$ に対して，$\gcd(a, b)$ はユークリッドの互除法により高々 20 回の除法の定理の適用で計算可能であることが分かります。

一般的な評価を得るために，フィボナッチ数の具体的な大きさについての評価が必要になります。

6 ラメの定理

フィボナッチ数の一般項は，ビネの公式によって具体的な形が与えられていますが，その形からは大きさの評価は余り明確ではありません。

ここでは，ビネの公式を使わないで，より直接的な次の評価式を使います。

命題 6.1. $n > 2$ に対して，$\alpha = \dfrac{1 + \sqrt{5}}{2}$ とすると，

$$f_n > \alpha^{n-2} \qquad (*)$$

が成立する。

証明. 数学的帰納法で証明しましょう。

(1) 命題の主張は $n > 2$ の場合ですが，$n = 2$ のときも似た性質，この場合は等号が成立します。即ち，

$$f_2 = 1, \quad \alpha^{2-2} = \alpha^0 = 1$$

より，$f_2 = \alpha^0$ となります。

(2) $n = 3$ のときは，f_3 と α の値を具体的に比較します。即ち，

$$f_3 = 2, \quad \alpha^{3-2} = \alpha^1 = \frac{1+\sqrt{5}}{2} = 1.61\ldots$$

より，$f_3 > \alpha^1$ が成立します。

(3) そこで次に，$n \geqq 3$ として，n 以下について主張が成立すると仮定します[*7]。このとき，$\alpha^2 = \alpha + 1$ に注意すると，

$$f_{n+1} = f_n + f_{n-1} > \alpha^{n-2} + \alpha^{n-3} = \alpha^{n-3}(\alpha+1) = \alpha^{n-3}\cdot\alpha^2 = \alpha^{n-1} = \alpha^{(n+1)-2}$$

となります。これで，$(*)$ が $n+1$ のとき成立することが示されました。

□

これらの命題から，ラメの定理が示されます。

ラメの定理

仮定と記号を前節ユークリッド互除法の通りとする。即ち，a, b $(a > b)$ に対して，ユークリッドの互除法を適用して

$$r_{n-1} = q_n \cdot r_n$$

となり，最大公約数 r_n が得られたとする。b を 10 進法で表示したときの桁数を m とする。このとき，

$$5m \geqq n$$

である。

証明. まず，命題 5.1 と命題 6.1 より，

$$b \geqq f_{n+1} > \alpha^{n-1}$$

が得られます。ここで，$\log_{10}\alpha = 0.208\ldots > 0.2 = \frac{1}{5}$ に注意すると，

$$\log_{10} b > (n-1)\log_{10}\alpha > \frac{n-1}{5}$$

となります。m の定義から

$$10^m > b \geqq 10^{m-1} \text{ 故に, } m > \log_{10} b \geqq m-1$$

ですから，

$$m > \frac{n-1}{5} \text{ 即ち, } 5m > n-1$$

となります。ここで，m, n は自然数ですから

$$5m \geqq n$$

が得られます。 □

[*7] 数学的帰納法 2 の形のものです。

命題 5.1 の証明を見てみると，互除法での除法の定理の適用回数が多くなるのは，2 数にフィボナッチ数と同様な関係があるときであることに気が付きます。そのことに注意して，フィボナッチ数列を見てみると次の例が見つかります。

例 6.1 ($n = 5m$ となる例)**.**

$a = 1597 = f_{17}$, $b = 987 = f_{16}$ として，ユークリッドの互除法を適用してみると，$m = 3$ で，

$$
\begin{aligned}
1597 &= 1 \cdot 987 + 610 && (1)\\
987 &= 1 \cdot 610 + 377 && (2)\\
610 &= 1 \cdot 377 + 233 && (3)\\
377 &= 1 \cdot 233 + 144 && (4)\\
233 &= 1 \cdot 144 + 89 && (5)\\
144 &= 1 \cdot 89 + 55 && (6)\\
89 &= 1 \cdot 55 + 34 && (7)\\
55 &= 1 \cdot 34 + 21 && (8)\\
34 &= 1 \cdot 21 + 13 && (9)\\
21 &= 1 \cdot 13 + 8 && (10)\\
13 &= 1 \cdot 8 + 5 && (11)\\
8 &= 1 \cdot 5 + 3 && (12)\\
5 &= 1 \cdot 3 + 2 && (13)\\
3 &= 1 \cdot 2 + 1 && (14)\\
2 &= 2 \cdot 1 && (15)
\end{aligned}
$$

より，$n = 15 = 5m$ になる。

上の例は，除法の定理の適用回数が多い例でしたが，そこでは，b は比較的小さい数でした。ラメの定理は b がどんなに大きな数でも成立します。

例えば $a > b$ で，b が 100 桁の数でも最大公約数 $\gcd(a, b)$ は高々 500 回の計算で求まるということです。100 桁の数は例えば

```
1000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000
```

です！