高校生のための現代数学講座　　東京大学
「素数」　　玉原国際セミナーハウス
講義 (2)　辻　雄　　2012 年 7 月 14 日

「ユークリッドの互除法」

1　２つの自然数の最大公約数

- ２つの自然数 m, n に対し、m, n の両方を割り切る自然数 a を、m と n の公約数という。
- ２つの自然数 m, n の公約数のなかで、最大のものを m と n の最大公約数といい、$\mathrm{GCD}(m,n)$ あるいは、単に (m,n) と書く。英語 greatest common divisor の頭文字である。
- $m > n$ のとき、m を n で割ると q 余り r となるとする。すなわち、

$$m = n \times q + r \qquad (0 \leqq r < n)$$

とする。このとき、もし自然数 a が m と n の公約数ならば、a は r の約数であり、よって a は n と r の公約数である。逆に、もし自然数 a が n と r の公約数ならば、a は m の約数であり、よって a は m と n の公約数である。従って

$$\mathrm{GCD}(m,n) = \mathrm{GCD}(n,r).$$

2　ユークリッドの互除法

- 上に述べた割り算の余りと公約数の関係を用いると、割り算を繰り返すことにより最大公約数を求めることができる。例えば、2012 と 721 については次のように計算され、最大公約数は 1 つまり互いに素であることが分かる。この最大公約数を求める方法はユークリッドの互除法とよばれている。

$$\begin{array}{rcl} & & \mathrm{GCD}(2012,721) \\ 2012 \div 721 = 2 \text{ 余り } 570 & \Longrightarrow\ 2012 = 721 \times 2 + 570 & \Longrightarrow\ = \mathrm{GCD}(721,570) \\ 721 \div 570 = 1 \text{ 余り } 151 & 721 = 570 \times 1 + 151 & = \mathrm{GCD}(570,151) \\ 570 \div 151 = 3 \text{ 余り } 117 & 570 = 151 \times 3 + 117 & = \mathrm{GCD}(151,117) \\ 151 \div 117 = 1 \text{ 余り } 34 & 151 = 117 \times 1 + 34 & = \mathrm{GCD}(117,34) \\ 117 \div 34 = 3 \text{ 余り } 15 & 117 = 34 \times 3 + 15 & = \mathrm{GCD}(34,15) \\ 34 \div 15 = 2 \text{ 余り } 4 & 34 = 15 \times 2 + 4 & = \mathrm{GCD}(15,4) \\ 15 \div 4 = 3 \text{ 余り } 3 & 15 = 4 \times 3 + 3 & = \mathrm{GCD}(4,3) \\ 4 \div 3 = 1 \text{ 余り } 1 & 4 = 3 \times 1 + 1 & = \mathrm{GCD}(3,1) \\ 3 \div 1 = 3 & 3 = 1 \times 3 & = 1 \end{array}$$

- 筆算を次のように書くと見直しやすい。筆算の書き方はいろいろと工夫できる。

2	2012	721	
	1442		
	570		

$\Rightarrow$

2	2012	721	**1**
	1442	**570**	
	570	**151**	

$\Rightarrow$

2	2012	721	1
	1442	570	
3	570	151	
	453		
	117		

$\Rightarrow \cdots \Rightarrow$

2	2012	721	1
	1442	570	
3	570	151	1
	453	117	
3	117	34	2
	102	30	
3	15	4	1
	12	3	
3	3	1	
	3		
	0		

- この手順は、計算機にプログラムとして組めるものであり、アルゴリズムと呼ばれる。

(1) 自然数 m, n に対して、$n_0 = m$, $n_1 = n$ とおく。

(2) 自然数 k に対し、n_{k-1}, n_k が与えられ、$n_k \neq 0$ の時、$n_{k-1} = n_k \times r_k + n_{k+1}$ $(0 \leqq n_{k+1} < n_k)$ となる n_{k+1} を割り算で計算する。

(3) 最初に $n_{k+1} = 0$ になったとき、すなわち、n_{k-1} が n_k で割り切れるとき、n_k が m, n の最大公約数である。

- ここで大切なのは、$n_1 > n_2 > n_3 > \ldots$ と減少していくので、ある k で、必ず $n_{k+1} = 0$ となることである。

- 十進 BASIC のプログラムで書くと次のようになる。

```
! ユークリッドの互除法により GCD(a,b) を求める                    コメント
INPUT PROMPT  "a > b > 0 となる整数":a,b    2 つの整数の入力を求める
PRINT                                                          改行
10 LET  q=INT(a/b)                          分数 a/b の整数部分を q とする
   LET  r=MOD(a,b)                              a ÷ b の余りを r とする
   IF r =0 THEN GOTO 30 ELSE GOTO 20
                        r = 0 ならば、行番号 30 へ、そうでなければ行番号 20 へ
20 PRINT a;"=";b;"×";q;"+";r                        a=b × q+r と書く
   LET a=b                                          a の値を b に取り換える
   LET b=r                                          b の値を r に取り換える
   GOTO 10                                                  行番号 10 へ
```

```
30 PRINT a;"＝";b;"×";q                    a=b ×q と書く
END                                        プログラム終了
```

- 十進 BASIC はフリーのソフトウェアで、BASIC のプログラムをＰＣ上で実行するものです。http://hp.vector.co.jp/authors/VA008683/からダウンロードできます。

3　2 つの自然数の和や差で書ける整数

- ユークリッドの互除法で最大公約数を求めることができることから、最大公約数 $\mathrm{GCD}(m,n)$ に対して、整数 a, b で、$\mathrm{GCD}(m,n) = am + bn$ と書くものが存在することが分かる。

- 例えば、$\mathrm{GCD}(2012, 721) = 1$ の場合にユークリッドの互除法に現れるかずを順に $2012x+721y$ と表した時の係数 (x, y) は、互除法を行う時に同時に求める事ができる。

$$
\begin{array}{rrr}
 & & (x,y) \\
 & 2012 = 2012 \times 1 \quad + 721 \times 0 & (1,0) \\
 & 721 = 2012 \times 0 \quad + 721 \times 1 & (0,1) \\
(2012 - 721 \times 2 =) & 570 = 2012 \times 1 \quad + 721 \times (-2) & (1,-2) \\
(721 - 570 \times 1 =) & 151 = 2012 \times (-1) \quad + 721 \times 3 & (-1,3) \\
 & 117 = 2012 \times 4 \quad + 721 \times (-11) & (4,-11) \\
 & 34 = 2012 \times (-5) \quad + 721 \times 14 & (-5,14) \\
 & 15 = 2012 \times 19 \quad + 721 \times (-53) & (19,-53) \\
 & 4 = 2012 \times (-43) \quad + 721 \times 120 & (-43,120) \\
 & 3 = 2012 \times 148 \quad + 721 \times (-413) & (148,-413) \\
 & 1 = 2012 \times (-191) + 721 \times 533 & (-191,533)
\end{array}
$$

筆算でユークリッドの互除法をするときに同時に (x, y) を書き込んでいくと

2	2012	(1,0)	721	(0,1)	1
	1442	(0,2)	570	(1,-2)	
3	570	(1,-2)	151	(-1,3)	1
	453	(-3,9)	117	(4,-11)	
3	117	(4,-11)	34	(-5,14)	2
	102	(-15,42)	30	(38,-106)	
3	15	(19,-53)	4	(-43,120)	1
	12	(-129,360)	3	(148,-413)	
3	3	(148,-413)	1	(-191,533)	
	3				
	0				

- a, b を整数として、$am + bn$ の形に書かれる整数は、$\mathrm{GCD}(m,n)$ の倍数全体に一致する。

4　割り算による素数の判定

- ある自然数 n が素数であることを調べるためには、n が n 未満の自然数で割り切れないことを確かめればよい。

- もしも n が m で割り切れて、2 つの自然数の積 $n = \ell \times m$ と書かれれば、ℓ または m の一方は、n の平方根以下である。従って、素数であることを調べるためには、n が $\sqrt{n}$ 以下の自然数で割り切れないことを確かめればよい。

- ２進数で書かれている n, m に対し、n を m で割る計算は、次のプロセスで行われる。m は d 桁であるとする。
(1)「n の上 d 桁」$\leqq m$ ならば、商に 1 を立てて、n を引く。
(2)「n の上 d 桁」$< m$ ならば、n の上 $d+1$ 桁に対して、商に 1 を立てて、m を引く。

- これは、２進数の d 桁の比較および計算を、ほぼ（n の桁数 $-m$ の桁数）の回数繰り返していることになる。

- 例えば、$595 = 2^9 + 2^6 + 2^4 + 2^1 + 1$ で２進数の表記は 1001010011 である。$112 = 2^6 + 2^5 + 2^4$ で２進法の表記は 1110000 である。$595 \div 112 = 5$ 余り 35 の計算は次のようになる。

$$
\begin{array}{r}
101 \\
1110000\overline{)1001010011} \\
\underline{1110000} \\
10010011 \\
\underline{1110000} \\
100011
\end{array}
$$

- ２進数の表記は、10^3 と $1024 = 2^{10}$ がほぼ等しいから、１０進数の表記の $10/3$ 倍の桁数になる。

- 自然数 a の２進法による桁数を d とすると、$2^{d-1} \leqq a \leqq 2^d - 1$ だから、$d - 1 \leqq \log_2 a < d$ を満たしている。

- 自然数 n が素数であるかの判定のためには、およそ $\displaystyle\sum_{m=2}^{[\sqrt{n}]} \log_2 m \times (\log_2 n - \log_2 m)$ に比例した計算の量が必要である。ここで、$[\sqrt{n}]$ は $\sqrt{n}$ 以下の最大の整数を表す。

- 仮に n が２進法で 2ℓ 桁とすると、$\sqrt{n}$ は２進法で ℓ 桁である。k 桁の２進数は 2^{k-1} 個ある。この場合、和は $\displaystyle\sum_{k=1}^{\ell} 2^{k-1} \times k \times (2\ell - k)$ に比例した計算の量となる。これは $\ell \displaystyle\sum_{k=1}^{\ell} 2^{k-1} \times k$ 以上 $2\ell \displaystyle\sum_{k=1}^{\ell} 2^{k-1} \times k$ 以下である。$\ell \displaystyle\sum_{k=1}^{\ell} 2^{k-1} \times k = \ell(1 + (\ell - 1)2^{\ell})$ で、計算量は２進数の桁数 2ℓ に対し、$\ell(\ell - 1)2^{\ell}$ 以上である。

- ここで、$\displaystyle\sum_{k=0}^{\ell} x^k = \frac{1-x^{\ell+1}}{1-x}$ だから、$\displaystyle\sum_{k=1}^{\ell} kx^{k-1} = \frac{1}{(1-x)^2}(1-x^{\ell+1}) - \frac{\ell+1}{1-x}x^{\ell}$ であり、$x=2$ として、$\displaystyle\sum_{k=1}^{\ell} k2^{k-1} = 1-2^{\ell+1}+(\ell+1)2^{\ell} = 1+(\ell-1)2^{\ell}$ となることを用いた。

- 結局、$2^{2\ell-1}$ 以上 $2^{2\ell}$ 未満の自然数が素数かどうか調べるために、ほぼ $\ell(\ell-1)2^{\ell}$ 回の定数倍の計算が必要になる。従ってそれだけ時間がかかる。

- 2 進法で 10 桁 (10 進法で 3 桁) の自然数に対する時間が T ならば、2 進法で 20 桁 (10 進法で 6 桁) の自然数に対する計算にはほぼ、$2^{12}T$ かかる。2 進法で 40 桁 (10 進法で 12 桁) に対しては、$2^{34}T$, 2 進法で 80 桁 (10 進法で 24 桁) に対しては、$2^{76}T$, 2 進法で 160 桁 (10 進法で 48 桁) に対しては、$2^{158}T$ となる。つまり、10 進法 6 桁で 4000 倍、12 桁で 10^8 倍、24 桁で 10^{22} 倍、48 桁で 10^{49} 倍かかることになる。

- この計算は、素数であるかどうかを調べるだけではなく、$\sqrt{m}$ までの**約数をすべて求めるもの**である。

- 素数であることだけを判定するならば、桁数のべき乗で計算量が評価できるアルゴリズムが２１世紀の初めに見つかっている。「素数の判定」というキーワードで検索すると情報が見つかる。

5　ユークリッドの互除法の計算量

- ２つの自然数の最大公約数を見つけるユークリッドの互除法は、桁数に対し、その何倍かの計算量で実行できる。

- このことは、次のように説明できる。

(1) ２進法で書かれた m, n の桁数を ℓ_m, ℓ_n とすると、m を n で割る割り算には、およそ $(\ell_m-\ell_n)\ell_n$ 回の計算が必要である。

(2) その次には、ℓ_n 桁以下のものが２つのこる。これの割り算は、${\ell_n}^2$ 回以下の計算である。

(3) ２回の割り算で得られた２つの数の小さいほうの桁数は ℓ_n-1 以下である。

(4) 従って、$2\ell_n$ 回以内に互除法は必ず終わる。

- 十進法で n の桁数が、k_n ならば、２進法では n の桁数はほぼ $\frac{10}{3}k_n$ で、互除法は、$\frac{20}{3}k_n$ 回以内で終了することになる。実際には、多くて $5k_n$ 回程度である。

- ユークリッドの互除法は桁数が大きくても、短時間でできる。合同式の計算も短時間でできることになる。