

課題 最大公約数

正整数 a, b の最大公約数をユークリッド互除法で求めよ。

$a = bq + r$ ($0 < r < b$) のとき、 a と b の最大公約数 $\text{gcd}(a, b)$ と b と r の最大公約数 $\text{gcd}(b, r)$ が一致することに基づく。すなわち、 $\text{gcd}(a, b) = \text{gcd}(b, r)$ 。

$a=155, b=40$ の場合、

$$\begin{array}{ll} 155 = 40 * 3 + 35 & \text{gcd}(155, 40) = \text{gcd}(40, 35) \\ 40 = 35 * 1 + 5 & \text{gcd}(40, 35) = \text{gcd}(35, 5) \\ 35 = 5 * 7 & \text{gcd}(35, 5) = 5 \end{array}$$

となる。

●再帰的定義

$$\begin{aligned} \text{gcd}(a, b) &= \text{gcd}(b, r) & (a=bq+r, r>0) \\ &= b & (a=bq+r, r=0) \end{aligned}$$

関数 $\text{gcd}(a, b)$ は、定義通りに書ける。

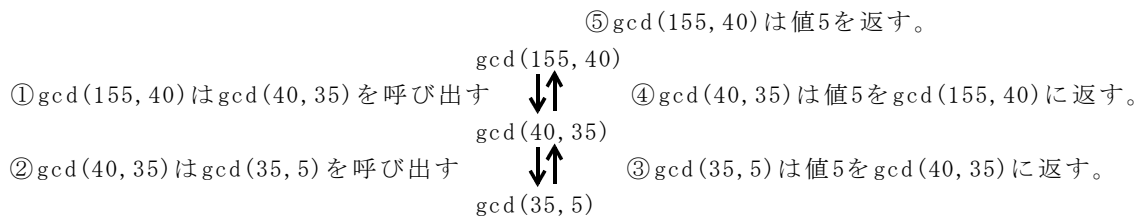
●プログラム (KA811. bas)

```
1  ' << K811. bas >>
2  ' 最大公約数
3  '
4  Do
5  ' 正整数A, Bの読み込み。
6  Read A, B
7  If (A <= 0) Or (B <= 0) Then Exit Do
8  RST=Fcd(A, B)
9  Print"Fcd(";A;", ";B;) =" ;RST
10 Loop
11 End
12 '
13 ' 最大公約数。Gcdは予約語と重なるためFcdとする。
14 Function Fcd(A, B)
15   R = A Mod B
16   If R =  Then
17     Z=
18   Else
19     Z=
20   End If
21   Fcd=Z
22 End Function
23 '
24 ' データ。
25 Data 1234, 567, 120, 64, 0, 0
```

実行結果

```
Fcd( 1234, 567) = 1
Fcd( 120, 64) = 8
OK
```

● a=155, b=40の場合、プログラムKA811. basの動作は①から⑤のようになる。



(考察) $\text{gcd}(a, b) = \text{gcd}(b, r)$ の証明。

$a = bq + r$ ($0 < r < b$) のとき、 a, b の公約数の集合を $G(a, b)$ とおくと、

$$G(a, b) = G(b, r)$$

が成り立つ。これは、 a, b の最大公約数と b, r の最大公約数が一致することを意味する。

$G(a, b) \subset G(b, r)$ を示す。

$a = a'k, b = b'k$ とすると、 $a'k = b'kq + r$ となり、変形して、 $r = (a' - b'q)k$ となる。これは、 b, r が約数 k を持つことを意味する。すなわち、 $G(a, b) \subset G(b, r)$ が示された。

$G(a, b) \supset G(b, r)$ を示す。

$b = b'm, r = r'm$ とすると、 $a = b'mq + r'm$ となり、変形して、 $a = (b'q + r')m$ となる。これは、 a, b が約数 m を持つことを意味する。すなわち、 $G(a, b) \supset G(b, r)$ が示された。

以上より、 $G(a, b) = G(b, r)$ が証明された。