BEGINNERS' CORNER

Edited by DMITRI THORO
San Jose State College, San Jose, California

THE EUCLIDEAN ALGORITHM I

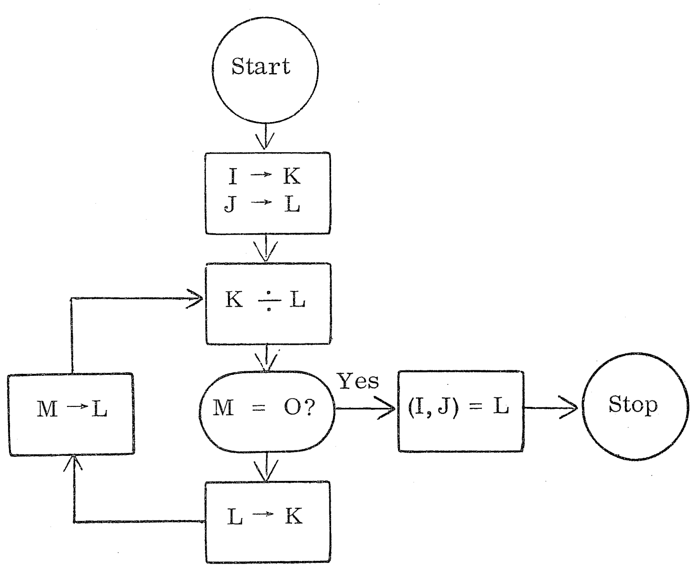
1. INTRODUCTION

Consider the problem of finding the greatest common divisor of 34 and 144. The factorizations $34 = 2 \cdot 17$, $144 = 2^4 \cdot 3^2$ make this a trivial problem. However, this approach is discouraging when one deals with, say, "long" Fibonacci numbers. Fortunately in Prop. 2 of Book VII, Euclid gave an elegant algorithm. As usual, we shall designate the g. c. d. of s and t by (s, t).

2. THE ALGORITHM

The algorithm may be defined by the following flow chart. $A \rightarrow B$ means A replaces B, i. e., set B = the current value of A.

M represents the remainder in the division of K by L.



Flow Chart for Computing the G. C. D of Positive Integers I and J

For I = 13 and J = 8, the successive values of K, L, and M are:

K	L	M
13	8	5
8	5	3
5	3	2
3	2	1
2	1	0

The last value of L is the desired g.c.d. In the following computation, (10946, 2584) = the last non-zero remainder.

```
          4
 2584|10946
      10336    4
        610|2584
            2440   4
             144|610
                 576  4
                  34|144
                     136 4
                       8|34
                         32 4
                          2|8
                            8
                            0
```

In this discussion we shall emphasize computational considerations. There are, however, numerous "theoretical" applications of the Euclidean Algorithm. As LeVeque [1] expresses it, "...it is the cornerstone of multiplicative number theory." For a related theorem see Glenn Michael [2], this issue.

3. A FORTRAN PROGRAM

With an occasional glance at our flow chart, it is easy to decipher the following Fortran program. (Fortran is a problem-oriented language commonly used in conversing with electronic digital computers.)

(i) A = B means A is replaced by B.

(ii) The READ and PUNCH statements refer to card input/output.

(iii) In this context, N = K/L is an instruction to set N equal to [K/L], i.e., the greatest integer not exceeding K/L (sometimes called an integer or fixed point quotient). Thus if K = 13 and L = 3, N will equal 4.

(iv) The symbol for multiplication is an asterisk.

(v) A "conditional transfer" is achieved by using an IF statement: if $M \leq 0$, go to statement 3 for the next instruction; otherwise go to statement 4.

(vi) The FORMAT and END statements are technical requirements (which may be ignored).

```
READ 10, I, J
10 FORMAT (3I5)
K = I
L = J
2 N = K/L
M = K - L * N
IF (M) 3, 3, 4
4 K = L
L = M
GO TO 2
3 PUNCH 10, I, J, L
END
```

4. Length of the Algorithm

A natural question arises: What is the "length" of this algorithm? I.e., if s and t are given, how many divisions are required to compute (s, t) via the Euclidean Algorithm?

Let us designate this number by $N(s, t)$. For convenience we may assume $s \geq t$. Thus for $n > 1$, $N(n + 1, n) = 2$; the first division yields the remainder 1, whereas the second results in a zero remainder — signifying termination of the algorithm. (As a byproduct we see that any two consecutive integers are relatively prime.)

In Part II we shall see how Fibonacci numbers ($F_1 = F_2 = 1$, $F_{i+1} = F_i + F_{i-1}$) were used by Lamé to establish a remarkable result. Additional properties of $N(s, t)$ are suggested in the following exercises.

5. EXERCISES

E1. Note that the Euclidean Algorithm applied to the positive integers s and t may be described by the equations

$$\begin{aligned}
s &= tq_1 + r_1, & 0 &\le r_1 < s \\
t &= r_1q_2 + r_2, & 0 &\le r_2 < r_1 \\
r_1 &= r_2q_3 + r_3, & 0 &\le r_3 < r_2 \\
&\;\;\vdots & &\;\;\vdots \\
r_{n-2} &= r_{n-1}q_n + r_n, & 0 &\le r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1} + 0 & .
\end{aligned}$$

Explain why we must reach a remainder (r_{n+1}) which is zero in a finite number of steps. Hint: Look at the inequalities.

E2. In E1, show that $(s,t) = r_n$ (the last non-zero remainder). Hint: Use repeated applications of Problem 1.3 [3].

E3. (a) Verify that $M = K - L * N$ is the remainder in the division represented by statement 2 $(N = K/L)$ of the Fortran program.

(b) Can the Fortran program be used to compute (I, J) when $I \le J$?

E4. Prove that if $n \ge 3$, then $N(n, 3) = 1, 2,$ or 3.

E5. Suppose that $n > 5$ is chosen at random. Find the probability that $N(n, 5) > 2$.

E6. Prove that for $n > 3$, $N(n + 3, n) = 2, 3,$ or 4.

E7. For what values of n is $3 \le N(2n - 5, n) \le 6$?

E8. Express (F_{n+1}, F_n) as a function of n.

E9. Investigate the following conjecture: If $a \le F_K$, then $N(n, a) \le K - 1$. Can n be any positive integer?

E10. Investigate the following conjecture: Let $F \ge 2$ be any Fibonacci number. Then $\max_n N(n, F) = 1 + \max_n (n, F - 1)$.

REFERENCES

1. William J. LeVeque, Topics in Number Theory, Addison-Wesley, Reading, Mass., 1956, Vol. I, Chap. 2.
2. Glenn Michael, "A New Proof for an Old Property," Fibonacci Quarterly, Vol. 2, No. 1, Feb. 1964, p. 57.
3. D. E. Thoro, "Divisibility I," Fibonacci Quarterly, Vol. 1, No. 1, Feb. 1963, p. 51.