Algorithms in Ancient India

Amba Kulkarni

Fellow IIAS, Shimla

16th January 2017

Algorithm

Algorithm: Step-by-step procedure to accomplish a certain task
Origin of the word, attributed to

Muḥammad ibn Mūsā al-Khwārizmī (9th century Persian Mathematician)

Al Khwarizmi wrote 'On the Calculation with Hindu Numerals' around 825 AD
About the Hindu–Arabic numeral system
spread throughout the Middle East and Europe.

It was translated into Latin as “Algoritmi de numero Indorum”.
Al-Khwārizmī, rendered as (Latin) Algoritmi, led to the term “algorithm”.

Characterisation of an algorithm

Knuth (1968, 1973) has given a list of five properties as requirements for an algorithm:

- Finiteness: An algorithm must always terminate after a finite number of steps
- Definiteness: Each step of an algorithm must be precisely defined; the actions to be carried out must be rigorously and unambiguously specified for each case
- Input: quantities which are given to it initially before the algorithm begins. These inputs are taken from specified sets of objects
- Output: quantities which have a specified relation to the inputs
- Effectiveness: all of the operations to be performed in the algorithm must be sufficiently basic that they can in principle be done exactly and in a finite length of time by a man using paper and pencil

Euclid's algorithm

One of the oldest Algorithms: Euclid's Algorithm for computing GCD
Euclid's Elements (circa 400 BC)

$r_{k-2} = r_{k-1} + r_k$

$a = b + r_0$
$b = r_0 + r_1$
$r_0 = r_1 + r_2$
.
.
.
$r_{n-2} = r_{n-1} + r_n$
When $r_n = 0$, r_{n-1} is the GCD of a and b

Euclid's algorithm: An Example

Find GCD of 21 and 35

$35 = 21 + 14$

$21 = 14 + 7$

$14 = 7 + 7$

$7 = 7 + 0$

GCD $= 7$

Euclid's algorithm

Better algorithm

$r_{k-2} = q_k r_{k-1} + r_k$

$a = q_0 b + r_0$
$b = q_1 r_0 + r_1$
$r_0 = q_2 r_1 + r_2$
.
.
.
$r_{n-2} = q_n r_{n-1} + r_n$
When $r_n = 0$, r_{n-1} is the GCD of a and b

Euclid's algorithm: An Example

Find GCD of 21 and 35

$35 = 1^* \ 21 + 14$

$21 = 1^* \ 14 + 7$

$14 = 2^* \ 7 + 0$

GCD $= 7$

Euclid's algorithm: An Example

- Finiteness: Algorithm terminates in finite steps
- Definiteness: Each step is precisely defined.
- Input: Two non-negative numbers
- Output: A non-negative number which is GCD of the given input
- Effectiveness: Each step can be effectively done with paper and pencil

Recursive version (An OCaml code)
Subtraction

```
let rec gcd a b =
  if a > b then gcd (a-b) b
  else if b > a then gcd a (b-a)
  else a
  ;;
```

Recursive version (An OCaml code)
Modulo division

```
let rec gcd a b =
    if b = 0 then a
    else gcd b (a mod b)
;;
```