THE EUCLIDEAN ALGORITHM

INTRODUCTION

The Euclid's Algorithm is an efficient method to calculate the Greatest Common Divisor(GCD) of two numbers, the largest number that divides them without leaving a reaminder.

HISTORY

- It is named after the ancient Greek Mathematician, Euclid who described it in Euclid's Elements(c. 300BC).
- It is one of the oldest algorithms in common use.
- It can be used to reduce fractions to their simplest form and is useful in many number theoretic and cryptographic calculations.

PRINCIPLE

- It is based on the principle that (assuming a<b):
  gcd(a,b) = gcd(b-a, a) = gcd(b%a,a),
  where b%a is b modulo a i.e. the remainder when b is divided by a.
- By reversing the steps, the gcd can be expressed as a sum of the two original numbers, each multiplied by a positive or negetive integer.

ALGORITHM

Given integers b and c > 0, we make a repeated application of the division algorithm, to obtain a series of equations:

$b = c*q_1 + r_1$ $0<r_1<c$
$c = r_1*q_2 + r_2$ $0<r_2<r_1$
$r_1=r_2*q_3 + r_3$ $0<r_3<r_2$

$r_{j-2} = r_{j-}1*q_j + r_j$ $0<r_j<r_{j-1}$
$r_{j-1} = rj*q_j+1$

The greatest commo divisor (b,c) of b and c is r_j, the last non-zero remainder i the division process.

REVERSAL

Values of x_0 and y_0 in $(b,c) = bx_0 + cy_0$ can be by writing each r_i as a linear combination of b and c.

PROOF

The chain of equtions is obtained by applying division algorithm repeatedly. The process stops when the division is exact and the remainder is zero. Thus the remainder inequalities are strict, $0<r_k<r_{k-1}$. If it were $0<=r_k<r_{k-1}$, the division would be exact and the algorithm should have stopped there.
We now prove that r_j is the greatest common divisor of b and c:
We know that (a,b) = (a, b+ax)
Thus $(b,c) = (b-cq_1,c) =(r_1,c)=(r_1,c) =(r_1,c-r_1q_2) =(r_1,r_2)$

REVERSAL PROOF

To see that r_j is a linear combination of b and c, we argue by induction that each r_i is a linear combination of b and c. Clearly, r_1 is a linear combination, and likewise r_2. In general, r_i is a linear combination of r_{i-1} and r_{i-2}. By the inductive hypothesis, we may suppose that these latter two numbers are linear combinations of b and c, and it follows that r_i is a linear combination of b and c.

EXAMPLES

1.GCD OF 42823 AND 6409

42823 = 6.6409 + 4369 (42823,6409)
6409 = 1.4369 + 2040 =(6409,4369)
4369 = 2.2040 + 289 =(4369,2040)
2040 = 7.289 +17 =(2040,289)
289 = 17.17 =(289,17) =17

2.FINDING x AND y TO SATISFY 42823x + 6409y = 17

i	q_{i+1}	r_i	x_i	y_i
-1		42823	1	0
0	6	6409	0	1
1	1	4369	1	-6
2	2	2040	-1	7
3	7	289	3	-20
4	17	17	-22	147
5		0		

NUMBER OF ITERATIONS

To get a rough bound on the number of iterations, j :

- $r_i <= r_{i-1}/2$, or
- $q_{i+1}=1$, $r_{i+1}=r_{i-1} - r_i$; $r_{i+1} < r_{i-1}/2$

From this, we deduce that the number of operations is of the order O(n) = log n.

APPLICATIONS

Euclid's algorithm had numerous cryptographic applications, most commonly in public key encryption.