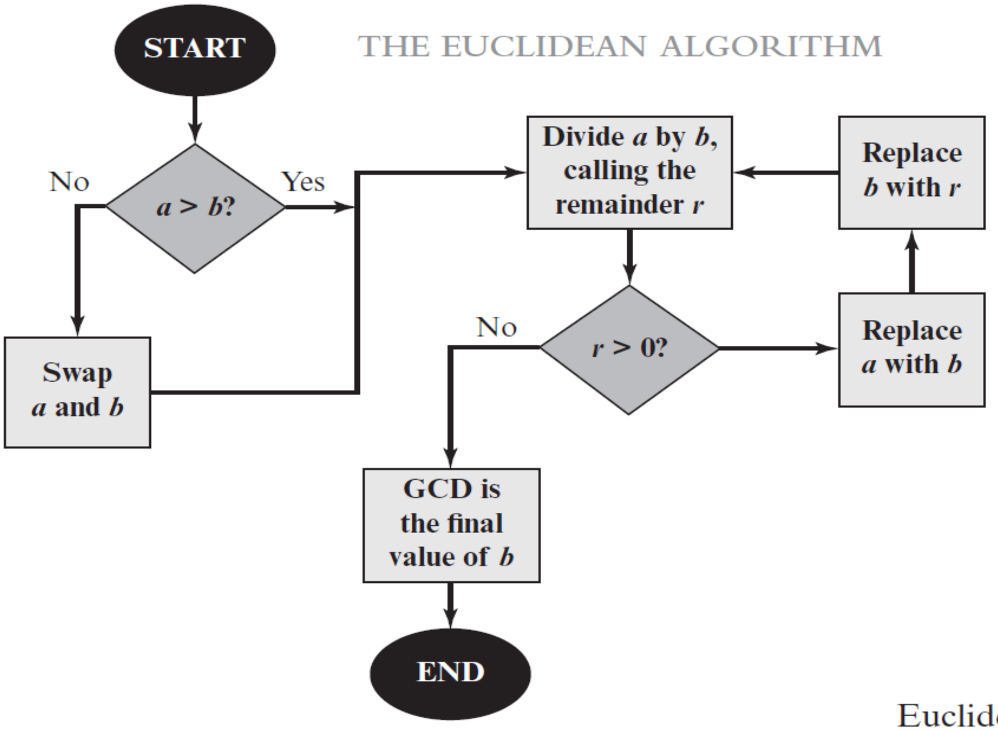
Euclidean algorithm

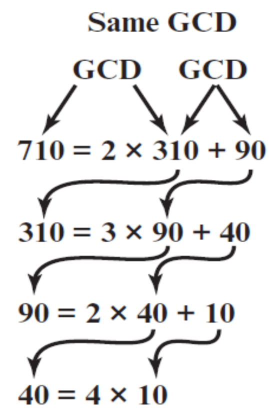
One of the basic techniques of number theory is the Euclidean algorithm, which is a simple procedure for determining the greatest common divisor of two positive integers. Let *a* and *b* be integers, not both zero. Recall that GCD (a, b) is the greatest common divisor of *a* and *b*. The best general algorithm for computing GCD (a, b) (and the only practical algorithm, unless the prime factorizations of *a* and *b* are known) is due to Euclid. This algorithm (known as Euclid"s Algorithm or the Euclidean Algorithm) involves repeated application of the Division Algorithm. In another word, given any positive integer n and any positive integer a, if we divide a by b, we get an integer *q* quotient and an integer *r* remainder that obey the following relationship:

$$a = q\,b + r \qquad 0 \le r < b$$

If have two numbers c,q that c=q*d+r, then GCD(c,q)=GCD(d,r)



Euclidean Algorithm



Euclidean Algorithm Example: gcd(710, 310)

The GCD of 710 and 310 is 10

Ex1: Find the Greatest Common Divisor (GCD) between 26 and 15 by using Euclid's Algorithm.

26= 15 * 1 + 11 → 26-15=11

15=11*1+4 → 15-11=4

11=4*2+3→11-8=3

4=3*1+1

GCD(26,15) = 1

Ex2: Find the Greatest Common Divisor (GCD) between 26 and 19 by using Euclid's Algorithm.

26 = 19 * 1 + 7 →26-19=7

19 = 7 * 2 + 5 →19- 14=5

7 = 5 * 1 + 2 →7-5=2

5 = 2 * 2 + 1 → 5-4=1

2 = 2 * 1 + 0 → 2-2=0

Ex3: Find the Greatest Common Divisor (GCD) between 132 and 55 by using Euclid's Algorithm.

132 = 55 * 2 + 22
55 = 22 * 2 + 11
22 = 11 * 2 + 0
Stopping when getting zero 0 then GCD is 11:

GCD(132,55) = GCD(55,22) = GCD(22,11) = GCD(11,0) = 11

Ex4: find the GCD (252 , 198) by using Euclid's Algorithm.

252 = 198 * 1 + 54
198 = 54 * 3 + 36
54 = 36 * 1 + 18
36 = 18 * 2 + 0

GCD(252,198) = (198,54) = (54,36) = (36,18) = (18,0) = 18.

Example: Compute the greatest common divisor (GCD) between the numbers (831, 366(.

Solution:

831	=	2 × 366	+ 99
366	=	3 × 99	+ 69
99	=	1 × 69	+ 30
69	=	2 × 30	+ 9
30	=	3 × 9	+ 3
9	=	3 × 3	+ 0

The answer is revealed as the last nonzero remainder: gcd (831, 366) = 3

Note: Because we require that the greatest common divisor be positive GCD (a, b)

= GCD (a, -b) = GCD (-a, b) = GCD(-a,-b). In general, GCD(a, b)

= GCD(/ a / , / b/).

Example: Find the greatest common divisor (GCD) of

a=321805575, b=198645

Solution:

321805575	=	1620 * ***198645***	+ 675
198645	=	294 * ***675***	+ 195
675	=	3 * ***195***	+ 90
195	=	2 * ***90***	+ 15
90	=	6 * ***15***	+ 0

The answer is revealed as the last nonzero remainder: GCD (321805575, 198645) = 15

H.W.

Now you try some: Answers		
(a) gcd(24, 54) = 6 (b) gcd(18, 42) = 6	(c) gcd(244, 354) = 2 (d) gcd(128, 423) = 1	(e) gcd(2415, 3289) = 23 (f) gcd(4278, 8602) = 46 (g) gcd(406, 555) = 1