Euclidean Algorithm

Algorithm used to find the gcd between two integers.

Algorithm:

Input: Two positive integers a,b

$a = bq + r \qquad 0 \le r < b$

$b = rq_1 + r_1 \qquad 0 \le r_1 < r$

$r = r_1q_2 + r_2 \qquad 0 \le r_2 < r_1$

.

.

.

(continue until remainder is zero)

$r_{i-2} = r_{i-1}q_i + r_i \qquad 0 \le r_i < r_{i-1}$

$r_{i-1} = r_iq_{i+1} + 0$

The last nonzero remainder is the gcd

$\gcd(a,b) = r_i$

Example:

Input: 34, 55

$55 = 34(1) + 21$

$34 = 21(1) + 13$

$21 = 13(1) + 8$

$13 = 8(1) + 5$

$8 = 5(1) + 3$

$5 = 3(1) + 2$

$3 = 2(1) + 1$

$2 = 2(1) + 0$

$\gcd(55,34) = 1$

Euclidean Algorithm

Algorithm:

Input: Two positive integers a,b

$$a = bq + r \qquad 0 \le r < b$$
$$b = rq_1 + r_1 \qquad 0 \le r_1 < r$$
$$r = r_1q_2 + r_2 \qquad 0 \le r_2 < r_1$$
$$\vdots$$

(continue until remainder is zero)

$$r_{i-2} = r_{i-1}q_i + r_i \quad 0 \le r_i < r_{i-1}$$
$$r_{i-1} = r_iq_{i+1} + 0$$

$$\gcd(a,b) = r_i$$

Why it works:

Thm:

If $a = bq + r$, then $\gcd(a,b) = \gcd(b,r)$

$$\gcd(a,b) = \gcd(b,r)$$
$$\gcd(b,r) = \gcd(r, r_1)$$
$$\gcd(r,r_1) = \gcd(r_1,r_2)$$
$$\vdots$$
$$= \gcd(r_{i-1},r_i) = \gcd(r_i,0) = r_i$$

Proof of Thm:

Let d be any common divisor of a and b.

$d \mid a,\ d \mid b \ \longrightarrow\ d \mid (a - bq) \ \longrightarrow\ d \mid r$

Let e be any common divisor of b and r.

$e \mid b,\ e \mid r \ \longrightarrow\ e \mid bq + r \ \longrightarrow\ e \mid a$

$\longrightarrow$ d is a common divisor of a and b iff d is a common divisor of b and r.

$\longrightarrow \gcd(a,b) = \gcd(b,r)$