Euclidean Algorithm

Lemma 1: Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a,b) = \gcd(b,r)$

ex: Find the gcd of 414 and 662 using the Euclidean algorithm.

Solution:

$662 = 414q + r$

$662 = 414 \cdot 1 + 248$

$414 = 248 \cdot 1 + 166$

$248 = 166 \cdot 1 + 82$

$166 = 82 \cdot 2 + 2$ ← The last nonzero remainder is your gcd

$82 = 2 \cdot 41 + 0$

stop when you have no remainder

$\boxed{\gcd(414, 662) = 2}$

ex: using the Euclidean algorithm, find the gcd of 413 and 415

set the larger number as a, and the smaller number as b.

Solution:

$415 = 413 \cdot 1 + 2$

$413 = 2 \cdot 206 + 1$ ← gcd

$2 = 1 \cdot 2 + 0$

Theorem 6: Bezout's Theorem:

If a and b are positive integers, then there exists integers s and t such that

$\gcd(a,b) = s \cdot a + t \cdot b$

- a and b are called Bezout's coefficients.

(17)

ex: Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198.

Solution:

Step 1: use Euclidean Algorithm.

Step 2: TWO methods you can use:

A. Do a backward pass

or

B. Extended Euclidean Algorithm

use these methods to get in format: $\gcd(a,b) = s \cdot a + t \cdot b$ ← this is what is meant by "linear combination"

Euclidean Algorithm:

$252 = 198 \cdot 1 + 54$ q_1

$198 = 54 \cdot 3 + 36$ q_2

$54 = 36 \cdot 1 + 18$ q_3

$36 = 18 \cdot 2$

} 4 equations

Backward Pass

- Have remainder be on left side of equation, and the rest on right side.
- Then do substitution from the bottom-up to get in the $gcd(a,b) = sa + tb$ format.

$18 = 54 - 36$

$36 = 198 - 54 \cdot 3$

$54 = 252 - 198$

$18 = 54 - 36 = 54 - (198 - 54 \cdot 3)$

$= 54 - 198 + 54 \cdot 3 = 54 \cdot 4 - 198$

$= (252 - 198) \cdot 4 - 198 = 252 \cdot 4 - 4 \cdot 198 - 198$

$18 = \boxed{4 \cdot 252 - 5 \cdot 198}$

Extended Euclidean Algorithm

$s_j = s_{j-2} - q_{j-1} \cdot s_{j-1}$ $\quad s_0 = 1$

$t_j = t_{j-2} - q_{j-1} t_{j-1}$ $\quad s_1 = 0$

$t_0 = 0$

$t_1 = 1$

- You have four equations, so need to find s_4 and t_4.

- Need the quotients (found via Euclidean Algorithm)

$q_1 = 1$

$q_2 = 3$

$q_3 = 1$

start with s_2 and t_2.

$s_2 = s_0 - q_1 s_1 = 1 - 1 \cdot 0 = 1$

$t_2 = t_0 - q_1 t_1 = 0 - 1 \cdot 1 = -1$

$s_3 = s_1 - q_2 s_2 = 0 - 3 \cdot 1 = -3$

$t_3 = t_1 - q_2 t_2 = 1 - 3 \cdot (-1) = 3$

$s_4 = s_2 - q_3 s_3 = 1 - 1(-3) = 1 + 3 = 4$

$t_4 = t_2 - q_3 t_3 = -1 - 1(4) = -1 - 4 = -5$

$18 = 4 \cdot 252 - 5 \cdot 198$