Expressing $d = \gcd(a, b)$ as $d = as + bt$

An important theorem in Number Theory states the following:

Given two non-zero integers a and b,

the integer $d = \gcd(a, b)$ is **a <u>linear combination</u> of a and b**,

that is to say, there exist integers s and t such that $\mathbf{d = as + bt}$.

The following is a description of a process by which two such integers s and t can be determined.

There are three steps:

I. Apply the Euclidean Algorithm to determine the value of $d = \gcd(a, b)$.

II. For each application of the Division Algorithm which divides, say, N by D and giving quotient q and remainder r, express the remainder r as a linear combination of N and D as follows:

From:
$$\begin{array}{r|l} & q \\ \hline D & N \\ & -Dq \\ \hline & r \end{array}$$
Write $r = (N)(1) - (D)(q)$, which comes from $N = Dq + r$.

This will result in a list of expressions of remainders as linear combinations of previous remainders or of a and b.

III. Working backward from the last linear combination, which expresses $d = \gcd(a, b)$ as a linear combination of previous remainders, continually express d as a linear combination of ever earlier remainders by substituting remainder factors by the linear combinations which express those factors as linear combinations of even earlier remainders.

After each substitution, simplify the expression, always having d expressed as a linear combination of remainders or of a and b. This might mean that a previous remainder, say 225, may have to be written with a multiplier of 1, that is, as (225) (1).

This process eventually leads to an expression of $d = \gcd(a, b)$ as a linear combination of a and b. At this point BE SURE TO DO THE FOLLOWING:

(1) Express this linear combination as a s SUM with perhaps a negative factor multiplied by a or by b.

(2) Check your equation with a calculator to make sure you didn't make an algebraic error along the way.

Note that using this process is a major step in finding Modular Inverses.

On the following pages are two examples illustrating this process.

EXAMPLE 1: Let $a = 330$ and $b = 156$.

EXPRESS $\gcd(330, 156) = 6$ as a LINEAR COMBINATION OF $a = 330$ and $b = 156$.

I. $156 \overline{)330}$ (2), -312, 18

$18 \overline{)156}$ (8), -144, 12

$12 \overline{)18}$ (1), -12, 6

$6 \overline{)12}$ (2), -12, 0

GCD = 6

II. $18 = (330)(1) - (156)(2)$

$12 = (156)(1) - (18)(8)$

$6 = (18)(1) - (12)(1)$

III. $6 = (18)(1) - [(156)(1) - (18)(8)](1)$

$6 = (18)(9) - (156)(1)$

$6 = [(330)(1) - (156)(2)](9) - (156)(1)$

$6 = (330)(9) - (156)(19)$ $[2 \times 9 + 1 = 19]$

$\therefore 6 = (330)(9) + (156)(-19)$

EXAMPLE 2: Let $a = 78$ and $b = 23$.

EXPRESS $\gcd(78, 23) = 1$ as a LINEAR COMBINATION OF $a = 78$ and $b = 23$.

I.
$$23\overline{)78}\ 3,\ -69,\ 9 \qquad 9\overline{)23}\ 2,\ -18,\ 5 \qquad 5\overline{)9}\ 1,\ -5,\ 4 \qquad 4\overline{)5}\ 1,\ -4,\ 1 \qquad 1\overline{)4}\ 4,\ -4,\ 0$$
↑ GCD = 1

II. $9 = (78)(1) - (23)(3)$

$5 = (23)(1) - (9)(2)$

$4 = (9)(1) - (5)(1)$

$1 = (5)(1) - (4)(1)$

III. $1 = (5)(1) - [(9)(1) - (5)(1)](1)$

$1 = (5)(2) - (9)(1)$

$1 = [(23)(1) - (9)(2)](2) - (9)(1)$

$1 = (23)(2) - (9)(5)$ $[2 \times 2 + 1 = 5]$

$1 = (23)(2) - [(78)(1) - (23)(3)](5)$

$1 = (23)(17) - (78)(5)$ $[2 + 3 \times 5 = 17]$

$\therefore\ 1 = (23)(17) + (78)(-5)$