The Greatest Common Divisor As a Linear Combination

E. L. Lady

Proposition. Let a and b be integers. If t is a linear combination of a and b (i.e. $ax + by = t$ for some x and y) then $a \bmod t$ and $b \bmod t$ are also linear combinations of a and b.

PROOF: Let q be the quotient and r the remainder when a is divided by t. Then

$$\begin{aligned} a \bmod t = r = a - qt &= a - q(ax + by) \\ &= a(1 - qx) + b(-qy) \end{aligned}$$

showing that $a \bmod t$ is a linear combination of a and b.

Likewise for $b \bmod t$. $\boxed{\checkmark}$

Corollary. If a linear combination of a and b is not also a common divisor of a and b, then there exists a smaller strictly positive linear combination.

PROOF: Suppose that $ax + by = t$ and t does not divide a, for instance. Then $t \bmod a \neq 0$ and $t \bmod a < t$. But by the Proposition, $t \bmod a$ is a linear combination of a and b. $\boxed{\checkmark}$

Theorem. The smallest strictly positive linear combination of a and b is the same as the greatest common divisor of a and b.

PROOF: Let $t = ax + by$ and $g = \gcd(a, b)$. Since g divides both a and b, it is clear that g divides $ax + by = t$. Thus $g \leq t$. On the other hand, by the above Corollary, if t is the **smallest** linear combination of a and b, then t must also be a common divisor of a and b, so $t \leq \gcd(a, b) = g$. Thus in this case $t = g$. $\boxed{\checkmark}$

The proof of the Proposition above actually provides an algorithm for finding the smallest strictly positive linear combination of a and b, which by the Theorem is the same as $\gcd(a, b)$.

We start with any x and y such that $ax + by \neq 0$ and let $t = ax + by$. Now if t does not divide both a and b then either we let q be the quotient when a is divided by t and replace x, y, and t by $1 - qx$, $-qy$ and $a \bmod t$, or, in case t divides a, let q be the quotient when b is divided by t and replace x, y, and t by $-qx$, $1 - qy$, and $b \bmod t$. Repeat until t divides both a and b. At this point, t will equal $\gcd(a, b)$ and $t = ax + by$.

The algorithm below accomplishes this.

```
procedure smallest-linear-combination(a, b, x, y)
t:= ax + by
while (a mod t ≠ 0 and b mod t ≠ 0)
if a mod t ≠ 0 then
    begin
    q:= ⌊a/t⌋
    x:= 1 − qx
    y:= −qy
    t:= a mod t
    end
else if b mod t ≠ 0
    begin
    q:= ⌊b/t⌋
    x:= −qx
    y:= 1 − qy
    t:= b mod t
    end
```

This algorithm works fairly quickly. For hand calculation, the most annoying part, if a and b are large numbers, is the continual need to divide a or b by t.

If we start with the initial values $x = 1$, $y = 0$, and $t = a$, then the following algorithm implements the same idea but with the advantage that the required long divisions involve increasingly small numbers.

After the algorithm, we give a pair of short numerical examples.

procedure `linear-combination(a, b: strictly positive integers)`

{ *We will find a sequences of values for* `x`, `y`, and `g` *such that in each case* `ax + by = g`, *and the final value for* `g` *equals* `gcd(a,b)`. }

g_0 := a
x_0 := 1
y_0 := 0
g_1 := b
x_1 := 0
y_1 := 1

{ *Note that* $ax_i + by_i = g_i$ *in each case.* }

while $g_0 \bmod g_1 \neq 0$

begin

q:= $\lfloor g_0 / g_1 \rfloor$
temp:= g_1
$g_1 := g_0 - qg_1$ { $g_1 := g_0 \bmod g_1$ }
g_0 := temp

{ *These four steps do not change* $\gcd(g_0, g_1)$ *since*
$\gcd(g_0 - qg_1, g_1) = \gcd(g_1, g_0)$,
so we still have $\gcd(g_1, g_0) = \gcd(a,b)$. }

temp:= x_1
$x_1 := x_0 - qx_1$
x_0 := temp
temp:= y_1
$y_1 := y_0 - qy_1$
y_0 := temp

{ *Now* $ax_1 + by_1 = g_1$. }

end

{ *Now* g_1 *divides* g_0, *and* x_1 *and* y_1 *are integers such that*
$ax_1 + by_1 = g_1 = \gcd(g_1, g_0) = \gcd(a,b)$. }

292x + 126y = g

q	x	y	g
	1	0	292
	0	1	126
2	1	-2	40
3	-3	7	6
6	19	-44	4

39x + 87y = g

q	x	y	g
	1	0	39
	0	1	87
0	1	0	39
2	-2	1	9
4	9	-4	3