THE (EXTENDED) EUCLIDEAN ALGORITHM

Given integers a, b, this enables us to find $\gcd(a, b)$ and express it in the form $ax + by$, by successive divisions-with-remainder. The calculation may be set out as in the following example.

To find $\gcd(963, 657)$:

							1	0
963	=	1	×	657	+	306	0	1
657	=	2	×	306	+	45	**1**	1
306	=	**6**	×	45	+	36	**2**	3
45	=	1	×	36	+	9	**13**	19
36	=	4	×	9	+	0	15	22

In the last two columns, each entry (except for the first two rows) is obtained from the two entries immediately above it and the quotient in the row above it; e.g. $13 = 6 \times 2 + 1$.

The example shows that $\gcd(963, 657) = 9$ and that

$$\pm 9 = 15 \times 963 - 22 \times 657.$$

We have to check the sign: it is $-$ here.

Why it works:
Add labels

i	a		q		b		r	x	y
0					(963)		(657)	1	0
1	963	=	1	×	657	+	306	0	1
2	657	=	2	×	306	+	45	1	1
3	306	=	6	×	45	+	36	2	3
4	45	=	1	×	36	+	9	13	19
5	36	=	4	×	9	+	0	15	22

and write a_i for the entry in row i and the column headed a, etc. We have

$$\gcd(a_1, b_1) = \gcd(a_2, b_2) = \ldots = \text{final value of } b,$$

and

$$(-1)^i b_i = x_i a_1 - y_i b_1 \qquad \text{for each } i.$$

When implementing this as a computer program, we can absorb the factor $(-1)^i$ by using the rule $x_i = x_{i-2} - q_{i-1}x_{i-1}$, instead of $x_i = x_{i-2} + q_{i-1}x_{i-1}$ (and similarly for y):- this means that the x_i and y_i have alternating signs, which easily leads to errors in hand calculations. Here is a more precise specification of this version of the algorithm, in the form of a MAPLE procedure:

```
> euclid:=proc(a1,b1)
> local a,b,q,r,x0,x1,x,y0,y1,y;
> a:=abs(a1);b:=abs(b1);x0:=sign(a1);x1:=0;y0:=0;y1:=sign(b1);
> while b<>0 do
>   q:=iquo(a,b);r:=a-q*b;
>   a:=b;b:=r;
>   x:=x0-x1*q;x0:=x1;x1:=x;
>   y:=y0-y1*q;y0:=y1;y1:=y;
> od;
> RETURN([a,x0,y0]);
> end;

> euclid(963,657);

                              [9, -15, 22]
```

So $\gcd(963, 657) = 9 = -15 \times 963 + 22 \times 657$.

Notes

(1) We only to store the values for previous two lines of the table.

(2) Using `abs(a1)` and `abs(b1)` ensures that we are dealing with non-negative integers, so that `iquo` coincides with the "floor" function. We therefore initialise `x0` and `y0` to ± 1.

(3) MAPLE has built-in functions for this:

```
> igcd(963,657);
                                9

> igcdex(963,657,`x`,`y`);x;y;
                                9

                               -15

                                22
```

Nigel Byott, October 2002