The extended Euclidean algorithm

Given a, $b \in \mathbf{N}$, this computes $g = \gcd(a, b)$ and also finds integers r and s such that $g = ra + sb$. The key is the observation that $\gcd(a, b) = \gcd(b, a - qb)$ for any integer q. If $b \mid a$ then $\gcd(a, b) = b$ but if $b \nmid a$ we choose the integer q with $0 < a - qb < b$.

In detail we produce three sequences of numbers $a_1, a_2, \ldots$, $r_1, r_2, \ldots$ and $s_1, s_2, \ldots$, and an auxiliary sequence $q_2, q_3 \ldots$. The crucial property of these sequences will be that

$$a_j = r_j a + s_j b \tag{$\dagger$}$$

for each j, or in matrix/vector terms

$$\begin{pmatrix} 1 & -a & -b \end{pmatrix} \begin{pmatrix} a_j \\ r_j \\ s_j \end{pmatrix} = (0). \tag{$\ddagger$}$$

We start by taking $a_1 = a$, $a_2 = b$, $r_1 = 1$, $r_2 = 0$, $s_1 = 0$ and $s_2 = 1$. Then ($\dagger$) holds for $j = 1$ and $j = 2$. We repeat the following procedure for $j = 2, 3, \ldots$. If $a_j \mid a_{j-1}$ we STOP: and return the values $g = a_j$, $r = r_j$ and $s = s_j$. Otherwise we let q_j be the integer part of the fraction a_{j-1}/a_j and calculate

$$a_{j+1} = a_{j-1} - q_j a_j, \quad r_{j+1} = r_{j-1} - q_j r_j, \quad s_{j+1} = s_{j-1} - q_j s_j$$

or in vector terms

$$\begin{pmatrix} a_{j+1} \\ r_{j+1} \\ s_{j+1} \end{pmatrix} = \begin{pmatrix} a_{j-1} \\ r_{j-1} \\ s_{j-1} \end{pmatrix} - q_j \begin{pmatrix} a_j \\ r_j \\ s_j \end{pmatrix}.$$

Then $0 < a_{j+1} < a_j$ and it's easy to see that as long as ($\dagger$)/($\ddagger$) is true for $j - 1$ and for j then it's also true for $j + 1$.

It's handy to set out these sequences in a table. Let's take $a = 963$, $b = 657$.

j	q_j	a_j	r_j	s_j
1		963	1	0
2	1	657	0	1
3	2	306	1	−1
4	6	45	−2	3
5	1	36	13	−19
6		9	−15	22

We stop there, as $9 \mid 36$, and conclude that $g = 9$, $r = -15$ and $s = 22$. We check that $g = ra + sb$; indeed $ra = -14445$ and $sb = 14454$ and $9 = -14445 + 14454$.

We remark that in this table the first column (j) is completely superfluous and may be omitted. The second column (q_j) is not essential, but is useful for checking.

`MAPLE` has built-in functions for the Euclidean algorithm and extended Euclidean algorithm: `igcd(a,b)` returns the gcd of a and b. Applying the extended Euclidean algorithm is slightly awkward: `igcdex(a,b,‘r‘,‘s‘)` returns the the gcd of a and b and assigns to the variables `r` and `s` numbers r and s with $\gcd(a, b) = ra + sb$.

In our example we get:

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

> igcdex(963,657,‘r‘,‘s‘);
                                    9

> r;
                                   -15

> s;
                                    22
```

RJC 3/2/2005