The Euclidean algorithm cont'd.

(a) Finding gcd's.

To find gcd(a, b):

1) Divide the smaller number into the larger.
2) Divide the previous remainder into the previous divisor.
3) Do step 2 repeatedly until the remainder becomes zero.
4) The previous remainder is gcd(a, b).

Example 1. Find gcd(714, 138).

Solution

$$714 = 138 \cdot 5 + 24$$
$$138 = 24 \cdot 5 + 18$$
$$24 = 18 \cdot 1 + 6$$
$$18 = 6 \cdot 3 + 0$$

So $\gcd(714, 138) = 6$.

(b) Expressing gcd(a, b) in the form ax−by.

To find x and y:

1) Use the next-to-last "remainder equation" from part (a) to rewrite gcd(a, b).
E.g. from the above, we have

$$6 = 24 - 18 \cdot 1.$$

2) Solve the <u>previous</u> remainder equation for the remainder there. Plug this result into the formula just found for $\gcd(a,b)$. Then simplify by collecting like terms.
E.g. from our second remainder equation above,

$$18 = 138 - 24\cdot 5,$$

so by Step 1,

$$\begin{aligned} 6 &= 24 - (138 - 24\cdot 5)\cdot 1 \\ &= 24 - 138 + 24\cdot 5 \\ &= 24\cdot 6 - 138. \end{aligned}$$

3) Repeat Step 2 until you're done.
E.g. we have, from our first remainder equation,
$24 = 714 - 138\cdot 5$, so by Step 2,

$$\begin{aligned} 6 &= (714 - 138\cdot 5)\cdot 6 - 138 \\ &= 714\cdot 6 - 138\cdot 30 - 138 \\ &= 714\cdot 6 - 138\cdot 31. \end{aligned}$$

<u>Example 2</u>.
Find $\gcd(35, 1174)$ and find $x, y \in \mathbb{Z}$ with $35x - 1174y = 1$.

<u>Solution</u>. (a)

$$\begin{aligned} 1174 &= 35\cdot 33 + 19 \\ 35 &= 19\cdot 1 + 16 \\ 19 &= 16\cdot 1 + 3 \\ 16 &= 3\cdot 5 + 1 \leftarrow \gcd(35, 1174) = 1. \\ 3 &= 3\cdot 1 + 0 \end{aligned}$$

(b) By part (a),

$$
\begin{aligned}
1 &= 16 - 3\cdot 5 && \text{(by fourth eq'n above)}\\
&= 16-(19-16\cdot 1)\cdot 5 && \text{(by third eq'n above)}\\
&= 16-19\cdot 5+16\cdot 5 && \text{(simplify)}\\
&= 16\cdot 6-19\cdot 5 && \text{(simplify)}\\
&= (35-19\cdot 1)\cdot 6-19\cdot 5 && \text{(by second eq'n above)}\\
&= 35\cdot 6-19\cdot 6-19\cdot 5 && \text{(simplify)}\\
&= 35\cdot 6-19\cdot 11 && \text{(simplify)}\\
&= 35\cdot 6-(1174-35\cdot 33)\cdot 11 && \text{(by first eq'n above)}\\
&= 35\cdot 6-1174\cdot 11+35\cdot 33\cdot 11 && \text{(simplify)}\\
&= 35\cdot(6+33\cdot 11)-1174\cdot 11 && \text{(simplify)}\\
&= 35\cdot 369-1174\cdot 11. && \text{(simplify)}
\end{aligned}
$$