Mathematics 124 (Winter 2009)
Bézout's identity

Recall the following theorem which we discussed in class.

Theorem: If a and b are positive integers, then there exist integers s and t such that $as + bt = d$ where $d = \gcd(a, b)$ is the greatest common divisor of a and b.

This theorem is sometimes called *Bézout's identity* after the French mathematician Étienne Bézout (1730–1783), and gives an example of a *linear Diophantine equation*. (In a Diophantine equation, only integer solutions are allowed.)

For a given a, b, the extended Euclidean algorithm produces *one* pair of integers s, t for which $as + bt = \gcd(a, b)$.

However, there are infinitely many integral solutions! In fact, let $s' = s - kb$ and let $t' = t + ka$ where k is an integer. Then,

$$as' + bt' = a(s - kb) + b(t + ka) = as - akb + bt + bka = as + bt = d.$$

For example, the greatest common divisor of $a = 12$ and $b = 42$ is $\gcd(12, 42) = 6$. Therefore, by Bézout's identity, there exist s and t such that

$$12s + 42t = 6.$$

Using the extended Euclidean algorithm (it only takes one step), we find

$$-3 \cdot 12 + 1 \cdot 42 = 6.$$

That is, $s = -3$ and $t = 1$. However, one can check that $s' = -3 - 42k$, $t' = 1 + 12k$ for integers k also work:

$k =$	$s' =$	$t' =$	$12s' + 42t'$
-2	81	-23	$972 - 966$
-1	39	-11	$468 - 462$
0	-3	1	$-36 + 42$
1	-45	13	$-540 + 546$
2	-87	25	$-1044 + 1050$

In fact, other solutions can be found, which in turn generate another infinite family of solutions. For instance,

$$4 \cdot 12 - 1 \cdot 42 = 6$$

so the generated solutions are

$k =$	$s' =$	$t' =$	$12s' + 42t'$
-2	88	-25	$1056 - 1050$
-1	46	-13	$552 - 546$
0	4	-1	$48 - 42$
1	-38	11	$-456 + 462$
2	-80	23	$-960 + 966$