Number Theory Section Summary: 2.4

Diophantine Equations

1. Definitions

Diophantine equation: A **Diophantine equation** is basically one whose solution is over the integers.

2. Theorems

Theorem 2.9: The linear Diophantine equation $ax + by = c$ has a solution iff $d|c$, where $d =$ gcd(a,b). If (x_0, y_0) is any particular solution of this equation, then all other solutions are given by

$$x = x_0 + \left(\frac{b}{d}\right)t \qquad y = y_0 - \left(\frac{a}{d}\right)t$$

for integral values of t.

Corollary: If 1 = gcd(a,b), and (x_0, y_0) is any particular solution of the equation $ax + by = c$, then all other solutions are given by

$$x = x_0 + bt \qquad y = y_0 - at$$

for integral values of t.

3. Properties/Tricks/Hints/Etc.

In doing these problems, which are often are of the form of amusing story problems, it is important to include restraints imposed by the nature of the variables. For example, if you are counting roosters, what does a negative number of roosters mean?

4. Summary

Theorem 2.9 is really an obvious conclusion of the corollary of Theorem 2.3: the set $T = \{ax + by | x, y \text{ are integers } \}$ is precisely the set of multiples of d = gcd(a,b), and we're testing whether a value c is an element of T.

Hence, the question "Does $ax + by = c$ have a solution?" is answered by checking to see if $d|c$ (that is, if c is a multiple of d).

A solution (x_0, y_0) is not unique, however, as one can obviously see: for example, if $x = b$ and $y = -a$, then $ab + b(-a) = 0$. So for any solution (x_0, y_0) of

$$ax_0 + by_0 = c$$

simply add zero (in the form $t(ab + b(-a))$):

$$ax_0 + by_0 + t(ab + b(-a)) = c$$

or

$$a(x_0 + tb) + b(y_0 - ta) = c$$

also holds true. So $(x_0 + tb, y_0 - ta)$ is a solution, for any integral value of t.

For those of you who love linear algebra (all of you, I'm sure!), you can think of it this way: if we have a solution

$$\langle a, b\rangle \cdot \langle x_0, y_0\rangle = c$$

then we can find the solutions of the homogeneous equation

$$\langle a, b\rangle \cdot \langle u, v\rangle = 0$$

and then tack them on to $\langle x_0, y_0\rangle$ to create the general solution

$$\langle x, y\rangle = \langle x_0, y_0\rangle + k\langle b, -a\rangle$$

This represents all the solutions, if we're willing to allow k to be real. But we're only interested in solutions over the integers, so we have to be careful! We can factor out a d = gcd(a,b) from the homogeneous equation, to produce

$$\langle x, y\rangle = \langle x_0, y_0\rangle + kd\langle (b/d), -(a/d)\rangle$$

The safe bet is to make sure that $t \equiv kd \in \mathbb{Z}$: hence the general solution is

$$\langle x, y\rangle = \langle x_0, y_0\rangle + t\langle (b/d), -(a/d)\rangle$$