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 $t(ab + b(-a))$):

$$\overline{ax_0 + by_0 + t(ab + b(-a)) = c}$$

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.

This is not all the solutions, however, unless the gcd of a and b is one: in order to have a solution, $d|c$, so $\exists r$ such that $c = dr$. Hence

$$ax_0 + by_0 = c \iff (a/d)x_0 + (b/d)y_0 = r$$

and the same trick implies that

$$(\underline{x_0 + t(b/d)}, \underline{y_0 - t(a/d)})$$

is the general solution, with t an integer.

1a, p 38

$6x + 51y = 22$

$\gcd(6,51) = 3 \nmid 22$, so can't solve in integers.

2b. $24x + 138y = 18$

$\gcd(24, 138) = 6$

$x_0 = -5$ $\quad$ $24\cdot(-5) + 138\cdot 1 = 18$

$y_0 = 1$

(by guess + check - could get from EA otherwise)

$x = -5 + 23t$

$y = 1 - 4t$

$\begin{pmatrix} a=24 \\ b=138 \end{pmatrix}$

3c, p 38 Find positive integer solns of

$123x + 360y = 99$

$\gcd(123, 360) = 3$

Do it the hard way:

$360 = 2\cdot 123 + 114$ $\qquad$ $114 = a - 2b$

$123 = 1\cdot 114 + 9$ $\qquad$ $9 = 123 - 114$

$114 = 12\cdot 9 + 6$ $\qquad$ $6 = 114 - 12\cdot 9$

$9 = 1\cdot 6 + \boxed{3}$ $\qquad$ $3 = 9 - 6$

$6 = 2\cdot 3 + 0$

$9 = b - (a - 2b)$

$= -a + 3b$

$6 = a - 2b - 12(-a + 3b)$

$= 13a - 38b$

$a = 360$

$b = 123$

$3 = (-a + 3b) - (13a - 38b)$

$= -14a + 41b$

$$\boxed{3 = -14\cdot 360 + 41\cdot 123}$$

Multiply by 33 to get the particular solution

Particular soln: $x_0 = 33\cdot -14 = -462$

$y_0 = 33\cdot 41 = 1353$

$x = -462 + 41t > 0$ $\qquad$ $t > 11.$ change

$y = 1353 - 120t > 0$ $\qquad$ $t < 11.$ change

No solution – inconsistent!

#4d p25 $\qquad$ $21 \mid 4^{n+1} + 5^{2n-1}$ $\qquad$ for $n \geq 1$

Anchor: $n = 1$

$$4^{1+1} + 5^{2-1} = 16 + 5 = 21$$

$$21 \mid 21 \checkmark$$

Inductive step:

Assume it's true for k; show it for $k+1$:

Consider $4^{(k+1)+1} + 5^{2(k+1)-1}$

$$= 4 \cdot 4^{k+1} + \underbrace{25}_{4+21} \cdot 5^{2k-1}$$

$$= 4\underbrace{\left(4^{k+1} + 5^{2k-1}\right)}_{21 \mid \text{this}} + \underbrace{21}_{21 \mid 21!} \cdot 5^{2k-1}$$

So $21 \mid$ the linear combinations.

$$= 4 \cdot (4^{k+1} + 5^{2k-1} - 5^{2k-1}) + 25 \cdot 5^{2k-1}$$

$$= 4(4^{k+1} + 5^{2k-1}) + 21 \cdot 5^{2k-1}$$

✓

Q.E.D.

\#7d, p39 $\quad m, w, c$

$m + w + c = 20 \qquad m + w + c = 20$

$3m + 2w + \frac{1}{2}c = 20 \iff 6m + 4w + c = 40$

$a = 5$

$b = 3$

$\boxed{5m + 3w = 20}$

$\gcd(5,3) = 1 \implies$ there's a solution for any RHS (integral)

Particular solution: $m_0 = 1, \; w_0 = 5$

$5 \cdot 1 + 3 \cdot 5 = 20$ ✓

$m = m_0 + 3t$

$w = 5 - 5t$

Constraint: $m \geq 0$

$w \geq 0$

$1 + 3t \geq 0$

$5 - 5t \geq 0$

(m, w, c)

$t = 0$ is a legitimate solution : $(1, 5, 14)$

$t = 1$ " " " " : $(4, 0, 16)$