Elementary Number Theory **Mathematics Dept.,**
Course I - High Diploma Students **Edu. College for Pure Sciences**
Asst. Prof. Dr. Ruma Kareem K. Ajeena **University of Babylon**
ruma.usm@gmail.com

Lecture 4: The Diophantine Equation $ax + by = c$

3.1 The Diophantine Equation

The simplest type of Diophantine equation that we shall consider is the linear Diophantine equation in two unknowns:

$$ax+by=c$$

where a, b, c given integers and a, b are not both zero. A solution of this equation is a pair of integers x_0, y_0 that, when substituted into the equation, satisfy it; that is, we ask that $ax_0+by_0=c$.

A given linear Diophantine equation can have a number of solutions, as is the case with $3x+6y=18$, where

$$3\cdot 4+6\cdot 1=18$$
$$3(-6)+6\cdot 6=18$$
$$3\cdot 10+6(-2)=18$$

By contrast, there is no solution to the equation $2x+10y=17$. The left-hand side is an even integer whatever the choice of x and y, whereas the right-hand side is not.

The condition for solvability is easy to state: the linear Diophantine equation $ax+by=c$ admits a solution if and only if $d|c$, where $d=\gcd(a,b)$. We know that there are integers r and s for which $a=dr$ and $b=ds$. If a solution of $ax+by=c$ exists, so that $ax_0+by_0=c$ for suitable x_0 and y_0, then

$$c=ax_0+by_0=drx_0+dsy_0=d(rx_0+sy_0)$$

which simply says that $d|c$. Conversely, assume that $d|c$, say $c=dt$. Using Theorem (), integers x_0 and y_0 can be found satisfying $d=ax_0+by_0$. When

Dr. Ruma Kareem K. Ajeena

this relation is multiplied by t, we get $c = dt = (ax_0 + by_0)t = a(tx_0) + b(ty_0)$ Hence, the Diophantine equation $ax+by = c$ has $x = tx_0$ and $y = ty_0$ as a particular solution. This proves in the next theorem.

Theorem 3.1.1. The linear Diophantine equation $ax+by=c$ has a solution if and only if $d|c$, where $d = \gcd(a,b)$. If x_0, y_0 is any particular solution of this equation, then all other solutions are given by

$$x = x_0 + (b/d)t \quad \text{and} \quad y = x_0 - (a/d)t$$

where t is an arbitrary integer.

Proof. To establish the second assertion of the theorem, let us suppose that a solution x_0, y_0 of the given equation is known.
If x', y' is any other solution, then $ax_0 + by_0 = c = ax' + by'$ which is equivalent to

$$a(x' - x_0) = b(y_0 - y').$$

By the corollary [If a|c and b|c, with gcd(a,b)=1, then ab|c.], there exist relatively prime integers r and s such that $a = dr$, $b = ds$.

Substituting these values into the last-written equation and canceling the common factor d, we find that

$$r(x' - x_0) = s(y_0 - y'). \quad (*)$$

The situation is now this: $r|s(y_0 - y')$, with $\gcd(r,s)=1$.

Using Euclid's lemma, it must be the case that $r|(y_0 - y')$; or, in other words,

$$y0 - y' = rt \quad (**)$$

for some integer t.
Substituting Eq. (**) in Eq. (*), we obtain $x' - x0 = st$.

This leads us to the formulas

$$x' = x0 + st = x0 + (b/d)t \quad \text{and} \quad y' = y0 - rt = y0 - (a/d)t.$$

It is easy to see that these values satisfy the Diophantine equation, regardless of the choice of the integer t; for

$$\begin{aligned} ax'+by' &= a(x0 + (b/d)t) + b(y0 - (a/d)t \\ &= (ax0 + by0) + (ab/d - ab/d)t \\ &= c + 0 \cdot t = c. \end{aligned}$$

Dr. Ruma Kareem K. Ajeena

Thus, there are an infinite number of solutions of the given equation, one for each value of t.

Example 3.1.1. Consider the linear Diophantine equation

$$172x + 20y = 1000.$$

Applying the Euclidean's Algorithm to the evaluation of gcd(172, 20), we find that

$$\begin{aligned} 172 &= 8 \cdot 20 + 12 \\ 20 &= 1 \cdot 12 + 8 \\ 12 &= 1 \cdot 8 + 4 \\ 8 &= 2 \cdot 4 + 0 \end{aligned}$$

Whence gcd(172,20)=4. Because 4|1000, a solution to this equation exists. To obtain the integer 4 as a linear combination of 172 and 20, we work backward through the previous calculations, as follows:

$$\begin{aligned} 4 &= 12 - 8 \\ &= 12 - (20 - 12) \\ &= 2 \cdot 12 - 20 \\ &= 2(172 - 8 \cdot 20) - 20 \\ &= 2 \cdot 172 + (-17)20. \end{aligned}$$

Upon multiplying this relation by 250, we arrive at
$1000 = 250 \cdot 4 = 250[2 \cdot 172 + (-17)20] = 500 \cdot 172 + (-4250)20$,
so that $x = 500$ and $y = -4250$ provide one solution to the Diophantine equation in question.

All other solutions are expressed by

$$x = 500 + (20/4)t = 500 + 5t \text{ and } y = -4250 - (172/4)t = -4250 - 43t$$

for some integer t.
A little further effort produces the solutions in the positive integers, if any happen to exist. For this, t must be chosen to satisfy simultaneously the inequalities

$$5t + 500 > 0 \quad -43t - 4250 > 0$$

or, what amounts to the same thing, $-98(36/43) > t > -100$. Because t must be an integer, we are forced to conclude that $t = -99$.

Dr. Ruma Kareem K. Ajeena

Thus, our Diophantine equation has a unique positive solution x =5, y =7 corresponding to the value t =−99.
It might be helpful to record the form that Theorem (3.1.1) takes when the coefficients are relatively prime integers.

Corollary. If gcd(a,b)=1 and if x0, y0 is a particular solution of the linear Diophantine equation ax+by =c, then all solutions are given by

$$x = x0 + bt \quad \text{and} \quad y = y0 - at$$

for integral values of t.

Here is an example. The equation 5x +22y =18 has x0 =8, y0 =−1 as one solution; from the corollary, a complete solution is given by x =8+22t, y =− 1−5t for arbitrary t.

Dr. Ruma Kareem K. Ajeena