Diophantine equations

February 20, 2009

Euclidean Algorithm

Euclidean Algorithm is an efficient method of finding the greatest common divisor (gcd) for a pair of given integers.

Here is how the Euclidean Algorithm works:

Basic observation: A common divisor of two numbers also divides their difference. Moreover, the greatest common divisor of a pair of two numbers equals to the greatest common divisor of their difference and the smaller number.

The algorithm: Let $a \geq b > 0$ be two positive integers.

- STEP 1: Let $a_0 = a$ and $b_0 = b$. Apply the division algorithm to the pair (a_0, b_0) to get
$$a_0 = q_1 b_0 + r_1, \qquad 0 \leq r_1 < b_0.$$
- STEP 2: There are two possibilities:
  - If $r_1 = 0$, then $b|a$, and $gcd(a, b) = b$.
  - If $r_1 \neq 0$, let $a_1 = b_0$ and $b_1 = r_1$. Apply the division algorithm to the pair (a_1, b_1) to get
$$a_1 = q_2 b_1 + r_2, \qquad 0 \leq r_2 < b_{1.}$$
- STEP 3: Now keep repeating the previous step up until the moment when the remainder in the division algorithm turns out to be 0. Since all $a_k \geq b_k$ are positive, and $a_{k+1} = b_k < a_k$ (i.e., the numbers to which we apply the Euclidean algorithm decrease at each iteration while remaining positive), such a moment will come.
  Suppose that $r_{k+1} = 0$. Then $b_k | a_k$ and, therefore, $b_k = gcd(a, b)$.

Problem 1. Apply the Euclidean algorithm to find the greatest common divisor of the numbers

1. $a = 78$ and $b = 90$.
2. $a = 12378$ and $b = 3054$.

Problem 2. Use the Euclidean algorithm to find the integers x and y such that

1. $gcd(78, 90) = 78x + 90y$.
2. $gcd(12378, 3054) = 12378x + 3054y$.
3. Explain why you can always use the Euclidean algorithm to represent the greatest common divisor of two given numbers in such a way.

Diophantine equation

Consider equation of the form

$$ax + by = c, \tag{1}$$

where a, b, c are given integers, and x and y are integer unknowns.

Problem 3. Consier several equations. For each of them, either find at least one solution or give a simple reason why no solutions exist:

1. $3x + 6y = 8$.
2. $3x + 6y = 18$.

Problem 4. We will deduce the conditions when a Diophantine equation of the form $ax + by = c$ has a solution, how many solutions it has, and how to find them, in a series of steps:

1. Let $d = \gcd(a, b)$. Show that if $d \nmid c$, then equation (1) has no solutions.
2. Show that if $d \mid c$, i.e., $c = dc'$ for some c', then there is a solution. (*Hint:* apply Euclid's lemma and multiply by c' throughout).
3. Show that if $c = dc'$ and (x_0, y_0) is a solution, then

$$\left(x_0 + \frac{b}{d}t,\ y_0 - \frac{a}{d}t\right) \tag{2}$$

is also a solution.

4. Prove the converse of the previous statement. That is, if (x, y) is another solution of (1), then any other solution is of the form (2).

In the previous problem we have proved the following

Theorem. *A Diophantine equation of the form $ax + by = c$ has a solution if and only if $d \mid c$, where $d = gcd(a, b)$. When this condition is satisfied, the solutions are of the following form:*

$$x = x_0 + \frac{b}{d}t, \qquad y = y_0 = \frac{a}{d}t,$$

where (x_0, y_0) is a solution.

Linear congruences

A linear congruence is an equation of the form

$$ax \equiv b(\text{mod } n) \tag{3}$$

Compare this to a Diophantine equation

$$\begin{aligned} ax &= ny + b \\ ax - ny &= b. \end{aligned}$$

Two solutions x_1 and x_2 of (3) are considered equivalent if they are equal mod n. The number of solutions of a linear congruence refers to the number of non-equivalent solutions.

Given the relation with Diophantine equations, we