5.7. Linear Diophantine equations and linear congruences

5.7.1. Linear Diophantine equations

Definition 5.7.1 *Algebraic equations with integer coefficients, for which only integral solutions are considered, are called* ***Diophantine equations****.*

In particular, an equation of the type

$$ax + by = c, \tag{5.1}$$

where a, b, c are integers such that neither a nor b are 0, and for which only integral solutions are considered, is called a ***linear Diophantine equation of two unknowns****.*

Theorem 5.7.2 *A necessary and sufficient condition for the equation (5.1) to have an integral solution for x and y is that $\gcd(a, b) \mid c$.*

Proof: The condition is necessary because $\gcd(a, b) \mid ax + by$ for any integers x and y. Now, suppose $\gcd(a, b) \mid c$. Recall (Theorem 5.2.5) that there are integers u and v such that $\gcd(a, b) = ua + vb$. We will show that the pair

$$x_0 = \frac{uc}{\gcd(a, b)}, \; y_0 = \frac{vc}{\gcd(a, b)}$$

is a solution of the Definition 5.7.1 equation for any u, v such that $\gcd(a, b) = ua + vb$. Indeed, x_0 and y_0 are integers and

$$a\frac{uc}{\gcd(a, b)} + b\frac{vc}{\gcd\,(a, b)} = \left(\frac{au}{\gcd(a, b)} + \frac{bv}{\gcd(a, b)}\right)c = \frac{au + bv}{\gcd(a, b)}c = c.$$

Example 5.7.3

1. The equation $21x - 12y = 5$ has no integral solutions because $\gcd(21, 12) = 3$ and $3 \nmid 5$.
2. The equation $21x - 12y = 6$ has integral solutions since $3 \mid 6$. Since $3 = (-1) \times 21 + (-2) \times (-12)$, one solution is

$$x_0 = \frac{(-1) \times 6}{3} = -2, \; y_0 = \frac{(-2) \times 6}{3} = -4.$$

Theorem 5.7.4 *If $(x_0,\; y_0)$ is a solution of the equation in Definition 5.7.1 then all other integral solution of that equation can be obtained as*

$$x = x_0 + \frac{b}{\gcd(a, b)}t, \; y = y_0 - \frac{a}{\gcd(a, b)}t,$$

where t is an arbitrary integer parameter.

Proof: If $ax_0 + by_0 = c$ and $ax + by = c$, then $(ax + by) - (ax_0 + by_0) = 0$, i.e. $a(x - x_0) + b(y - y_0) = 0$, so $a(x - x_0) = b(y_0 - y)$ and hence $\frac{a}{\gcd(a, b)}(x - x_0) = \frac{b}{\gcd(a, b)}(y_0 - y)$. Then $\frac{a}{\gcd(a, b)} \mid \frac{b}{\gcd(a, b)}(y_0 -$

y), but $\gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1$ and hence $\frac{a}{\gcd(a,b)} \mid y_0 - y$. Let $y_0 - y = \frac{a}{\gcd(a,b)} t$ for some integer t. Then $y = y_0 - \frac{a}{\gcd(a,b)} t$. Likewise $x = x_0 + \frac{b}{\gcd(a,b)} t$.

Conversely, if $x = x_0 + \frac{b}{\gcd(a,b)} t,\ y = y_0 - \frac{a}{\gcd(a,b)} t$. Then:

$$ax + by = a\left(x_0 + \frac{b}{\gcd(a,b)} t\right) + b\left(y_0 - \frac{a}{\gcd(a,b)} t\right) = ax_0 + \frac{ab}{\gcd(a,b)} t + by_0 - \frac{ab}{\gcd(a,b)} t = ax_0 + by_0 = c.$$

Example 5.7.5

The general solution of the equation $21x - 12y = 6$ is given by

$$x = -2 + \frac{-12}{3} t = -2 - 4t,$$
$$y = -4 - \frac{21}{3} t = -4 - 7t.$$

For instance, when $t = 1$ we obtain the solution $(-6, -11)$; when $t = -1$ we obtain $(2, 3)$, etc.

5.7.2. *Linear congruences*

Definition 5.7.6 *A **linear congruence** is a congruence of the type*

$$ax \equiv c \pmod{n},$$

where a, c, n are integers and $n > 0$.

We are interested in the question of whether this congruence has solutions for x and how to find them.

First, let us observe that if the congruence $ax \equiv c \pmod{n}$ has *one* solution x_0, then it has *infinitely many* solutions: $x_0 + kn$, for any integer k. Moreover, note the following theorem.

Theorem 5.7.7 *Consider the congruence*

$$ax \equiv c \pmod{n}. \tag{5.2}$$

1. *This equation has a solution if and only if $\gcd(a, n) \mid c$. Then, one solution is $x_0 = \frac{uc}{\gcd(a,n)}$, where u is such that $\gcd(a, n) = ua + vn$ for some integer v.*
2. *If x_0 is a solution of that equation then an integer x is a solution if and only if it satisfies the congruence*
   $$ax \equiv ax_0 \pmod{n},$$
   and hence, by Theorem 5.5.7, the congruence
   $$x \equiv x_0 \left(\operatorname{mod} \frac{n}{(a,n)}\right).$$
3. *All solutions of the equation are given by the formula*
   $$x = x_0 + \frac{n}{(a,n)} k,$$
   where x_0 is any solution and k is an integer.

Proof:

1. Note that $ax \equiv c \pmod{n}$ if and only if $n \mid ax - c$ iff $ax - c = ny$ for some integer y, if and only if the equation $ax - ny = c$ has an integer solution iff $\gcd(a, n) \mid c$, by Theorem 5.7.2.
2. Exercise.
3. Follows from Theorem 5.7.4.

For instance, the congruence $6x \equiv 2 \pmod{8}$ has a solution $x = 3$ and hence all solutions are the numbers $3 + 4k$, for $k \in \mathbb{Z}$.

Often a congruence can be simplified by cancelling according to Theorem 5.5.7.

Example 5.7.8

Solve the congruence

$$9965x \equiv 19955 \pmod{4950}.$$

Solution

First we reduce the congruence by dividing by 5, using Theorem 5.5.7, to

$$1993x \equiv 3991 \pmod{990}.$$

Let us compute $\gcd(1993, 990)$:

$1993 = 2 \times 990 + 13.$

$990 = 76 \times 13 + 2.$

$13 = 6 \times 2 + 1.$

Thus, $\gcd(1993, 990) = 1$, so the congruence has solutions.

Now we look for integers u and v such that $1 = 1993u + 990v$:

$1 = 1 \times 13 - 6 \times 2 = 1 \times 13 - 6 \times (990 - 76 \times 13) = 457 \times 13 - 6 \times 990 = 457(1993 - 2 \times 990) - 6 \times 990 = 457 \times 1993 - 920 \times 990.$

Therefore, one solution is $x_0 = 457.3991 = 1\ 823\ 887$.

We can obtain a smaller solution by taking the remainder of the division of x_0 by 990: $1\ 823\ 887 = 1842 \times 990 + 307$.

Then, the general solution is $x = 307 + 990k$.

5.7.3. Exercises

❶ Solve the Diophantine equations:

(a) $81x - 24y = 18$

(b) $28x + 91y = 146$

(c) $429x + 154y = 121$

❷ Solve the congruences:

(a) $27x \equiv 12 \pmod{15}$

(b) $25x \equiv 5 \pmod{16}$

(c) $166x \equiv 18 \pmod{38}$

(d) $84x \equiv 24 \pmod{35}$

(e) $28x \equiv 42 \pmod{49}$

(f) $1001x \equiv 91 \pmod{104}$

(g) $3700x \equiv 11 \pmod{111}$

❸* Every two of n arithmetic progressions have a common term. Show that all progressions have a common term.

❹* Show that for every natural number n, in every arithmetic progression of natural numbers there are n consecutive terms that are composite numbers.

❺* Prove that for every positive integer k there exists a prime p such that each of the numbers $p - 1$, $p + 1$ and $p + 2$ has at least k different prime divisors.

[6] Translation taken from http://mathworld.wolfram.com/DiophantussRiddle.html.