

# Integer Divisibility

Victor Adamchik

Fall of 2005

## Lecture 5 (out of seven)

### ■ Plan

1. Introduction to Diophantine Equations
2. Linear Diophantine Equations
3. Positive solutions to LDE

### ■ Introduction

**Definition.** Let  $P(x, y, \dots)$  is a polynomial with integer coefficients in one or more variables. A **Diophantine equation** is an algebraic equation

$$P(x, y, z, \dots) = 0$$

for which integer solutions are sought.

For example,

$$2x + 3y = 11$$

$$7x^2 - 5y^2 + 2x + 4y - 11 = 0$$

$$y^3 + x^3 = z^3$$

The problem to be solved is to determine whether or not a given Diophantine equation has solutions in the domain of integer numbers.

In 1900 Hilbert proposed 23 most important unsolved problems of 20th century. His **10th** problem was about solvability a general Diophantine equation. Hilbert asked for a *universal method* of solving all Diophantine equations.

What is the notion of *solvable*? What is the notion of an *algorithm*?

**1930.** Godel, Kleene, Turing developed the notion of computability.

**1946.** Turing invented Universal Turing Machine and discovered basic unsolvable problems

**1970** Y. Matiyasevich proved that the Diophantine problem is unsolvable.

**Theorem** (Y. Matiyasevich) *There is no algorithm which, for a given arbitrary Diophantine equation, would tell whether the equation has a solution or not.*

By the way, Goldbach's conjecture (which was mentioned a few lectures back) is Hilbert's 8th problem.

## ■ Linear Diophantine Equations

### Definition.

A [linear Diophantine equation](#) (in two variables  $x$  and  $y$ ) is an equation

$$a x + b y = c$$

with integer coefficients  $a, b, c \in \mathbb{Z}$  to which we seek integer solutions.

It is not obvious that all such equations solvable. For example, the equation

$$2 x + 2 y = 1$$

does not have integer solutions.

Some linear Diophantine equations have finite number of solutions, for example

$$2 x = 4$$

and some have infinite number of solutions.

### Theorem.

*The linear equation  $a x + b y = c$  with  $a, b, c \in \mathbb{Z}$*

$$a x + b y = c$$

*has an integer solution in  $x$  and  $y \in \mathbb{Z} \iff \gcd(a, b) \mid c$*

*Proof.*

$\implies$ )

$$\gcd(a, b) \mid a \wedge \gcd(a, b) \mid b \implies$$

$$\gcd(a, b) \mid (x a + y b) \implies \gcd(a, b) \mid c$$

$\impliedby$ )

Given

$$\gcd(a, b) \mid c \implies \exists z \in \mathbb{Z}, c = \gcd(a, b) * z$$

On the other hand

$$\exists x_1, y_1 \in \mathbb{Z}, \gcd(a, b) = x_1 a + y_1 b.$$

Multiply this by  $z$ :

$$z * \gcd(a, b) = a * x_1 * z + b * y_1 * z$$

$$c = a * x_1 * z + b * y_1 * z$$

Then the pair  $x_1 * z$  and  $y_1 * z$  is the solution

QED.

***How do you find a particular solution?***

$$a x + b y = c$$

By extended Euclidean algorithm we find  $\gcd$  and such  $n$  and  $m$  that

$$a * n + b * m = \gcd(a, b)$$

Multiply this by  $c$

$$a * n * c + b * m * c = \gcd(a, b) * c$$

Divide it by  $\gcd$

$$a \frac{n * c}{\gcd(a, b)} + b \frac{m * c}{\gcd(a, b)} = c$$

Compare this with the original equation

$$a x + b y = c$$

It follows that a particular solution is

$$x_0 = \frac{n * c}{\gcd(a, b)}; y_0 = \frac{m * c}{\gcd(a, b)}$$

**Question.** Are  $x_0$  and  $y_0$  integer?

**Exercise.** Find a particular solution of

$$56 x + 72 y = 40$$

*Solution.* Run the EEA to find GCD,  $n$  and  $m$

$$\text{GCD}(56, 72) = 8 = 4 * 56 + (-3) * 72$$

Then one of the solutions is

$$x_0 = \frac{4 * 40}{8}; y_0 = \frac{(-3) * 40}{8}$$

$$x_0 = 20; y_0 = -15$$

**How do you find all solutions?**

$$a x + b y = c$$

By the extended Euclidean algorithm we find gcd and such  $n$  and  $m$  that

$$\gcd(a, b) = a * n + b * m$$

$$\gcd(a, b) * c = a * n * c + b * m * c$$

Next we add and subtract  $a * b * k$ , where  $\forall k \in \mathbb{Z}$

$$\gcd(a, b) * c = a * n * c + b * m * c + a * b * k - a * b * k$$

Collect terms with respect  $a$  and  $b$

$$a * (n c + b k) + b * (m c - a k) = \gcd(a, b) * c$$

Divide this by  $\gcd(a, b)$

$$a * \frac{(n c + b k)}{\gcd(a, b)} + b * \frac{(m c - a k)}{\gcd(a, b)} = c$$

It can be rewritten as

$$c = a * \left( \frac{n c}{\gcd(a, b)} + \frac{b k}{\gcd(a, b)} \right) + b * \left( \frac{m c}{\gcd(a, b)} - \frac{a k}{\gcd(a, b)} \right)$$

or

$$c = a * \left( x_0 + \frac{b * k}{\gcd(a, b)} \right) + b * \left( y_0 - \frac{a * k}{\gcd(a, b)} \right)$$

$$k = 0, \pm 1, \pm 2, \dots$$

since  $(x_0, y_0)$  is a particular solution.

Therefore, all integers solutions are in the form

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

$$k = 0, \pm 1, \pm 2, \dots$$

**Exercise.** Find all integer solutions of

$$56 x + 72 y = 40$$

*Solution.* Run the EEA to find GCD,  $n$  and  $m$

$$\text{GCD}(56, 72) = 8 = 4 * 56 + (-3) * 72$$

All solutions are in the form

$$x = \frac{n c}{\gcd(a, b)} + \frac{b k}{\gcd(a, b)}$$

$$y = \frac{m c}{\gcd(a, b)} - \frac{a k}{\gcd(a, b)}$$

Hence

$$x = \frac{4 * 40}{8} + \frac{72 k}{8} = 20 + 9 * k$$

$$y = \frac{-3 * 40}{8} - \frac{56 k}{8} = -15 - 7 * k$$

### ■ Positive solutions of LDE

In some applications it might required to find all positive solutions  $x, y \in \mathbb{Z}^+$ .

We take a general solution

$$x = \frac{n c}{\gcd(a, b)} + \frac{b k}{\gcd(a, b)}$$

$$y = \frac{m c}{\gcd(a, b)} - \frac{a k}{\gcd(a, b)}$$

from which we get two inequalities

$$n c + b k > 0$$

$$m c - a k > 0$$

To find out how many positive solutions a given equation has let us consider two cases

$$1. \quad a x + b y = c, \quad \gcd(a, b) = 1, \quad a, b > 0$$

$$2. \quad a x - b y = c, \quad \gcd(a, b) = 1, \quad a, b > 0$$

It follows that in the first case, the equation has a finite number of solutions

$$-\frac{n c}{|b|} < k < \frac{m c}{|a|}$$

In the second case, there is an infinite number of solutions

$$n c - |b| k > 0$$

$$m c - |a| k > 0$$

**Exercise.** Determine the number of solutions in positive integers

$$4 x + 7 y = 117$$

*Solution.*

$$\text{GCD}(4, 7) = 1 = 2 * 4 + (-1) * 7$$

The number of solutions in positive integers can be determined from the system

$$n c + b k > 0$$

$$m c - a k > 0$$

which for our equation transforms to

$$2 * 117 + 7 * k > 0$$

$$(-1) * 117 - 4 * k > 0$$

This gives

$$-\frac{2 * 117}{7} < k < \frac{-117}{4}$$

There 4 such  $k$ , namely  $k = -33, -32, -31, -30$ .

## ■ LDEs with three variables

Consider

$$3 x + 6 y + 5 z = 7$$

$$\text{GCD}(3, 6)(x + 2 y) + 5 z = 7$$

Let

$$w = x + 2 y$$

The equation becomes

$$3 w + 5 z = 7$$

Its general solution is

$$w = 2 * 7 + 5 k$$

$$z = (-1) * 7 - 3 k$$

since

$$\text{GCD}(3, 5) = 1 = 2 * 3 + (-1) * 5$$

Next we find  $x$  and  $y$

$$x + 2 y = 14 + 5 k$$

Since  $\text{GCD}(1, 2) \mid (14 + 5 k)$ , the equation is solvable and the solution is

$$x = 1 * (14 + 5 k) + 2 * l$$

$$y = 0 * (14 + 5 k) - 1 * l$$

where  $l \in \mathbb{Z}$  is another parameter. Here are all triple-solutions

$$x = 5 k + 2 l + 14$$

$$y = -l$$

$$z = -7 - 3 k$$

where

$$k, l = 0, \pm 1, \pm 2, \dots$$