2019 HAWAII UNIVERSITY INTERNATIONAL CONFERENCES
SCIENCE, TECHNOLOGY & ENGINEERING, ARTS, MATHEMATICS & EDUCATION JUNE 5 - 7, 2019
HAWAII PRINCE HOTEL WAIKIKI, HONOLULU, HAWAII

A "NON-EUCLIDEAN" ALGORITHM OF LINEAR DIOPHANTINE EQUATION

GARRISON, MARK
HU, XIAOYAN
DEPARTMENT OF MATHEMATICS
MIDDLE GEORGIA STATE UNIVERSITY
MACON, GEORGIA

A "NON-EUCLIDEAN" ALGORITHM OF LINEAR DIOPHANTINE EQUATIONS

MARK GARRISON , XIAOYAN HU

ABSTRACT. This paper will present an alternative algorithm for introductory students of mathematics to find solutions to linear Diophantine equations of the form $ax + by = c$, where a, b and c are integers.

INTRODUCTION

Diophantine equations have both a theoretical and practical appeal to the student of mathematics. It is well established [1] that the diophantine equation $ax+by = c$ has a solution if and only if c is a multiple of $d = \gcd(a, b)$, the greatest common divisor of a and b. If (p, q) is a solution of the equation, then the solution set is $\{(p+\frac{kb}{d}, q-\frac{ka}{d}),\ k \in \mathbb{Z}\}$. In elementary number theory, we use the Euclidean algorithm to find one pair of solutions. In this paper, we will present an alternative algorithm for finding solutions of the equation $ax+by = c$, where a and b are relatively prime. We will show it is sufficient to consider $x = 0, ..., b-1$ to find one solution (p, q) for the equation $ax + by = 1$ which leads to the general solution for $ax + by = c$ of the form $(cp + kb, cq - ka)$. Examples of this algorithm are presented at the end of the paper.

ALL SOLUTIONS FOR $ax + by = 1$

Given two nonzero integers a and b that are relatively prime *i.e.*, $\gcd(a, b) = 1$, we will present an alternative algorithm for finding integral solutions of the equation $ax + by = 1$, including proofs to demonstrate that our algorithm is valid. We will also solve a problem with both the Euclidean algorithm and the alternative algorithm.

The following is the alternative algorithm used to find solutions of the equation $ax + by = 1$. If $a < b$ we can switch the positions of the two terms on the left side of the equation. Without loss of generality, we can assume $a > b$.

Step 1: Substitute for x in the equation $ax + by = 1$ beginning at $x = 0$ and continuing in the order $0, 1, 2, \cdots, b-1$. This will produce exactly one specific solution (x_0, y_0).

Step 2: The general solution for $ax + by = 1$ then becomes

$$(x_0 + kb, y_0 - ka), \ \textit{k is any integer}$$

Example 1. Given the equation $5x+3y = 1$, find all integral solutions.

In this problem, we have $a = 5$ and $b = 3$, which are relatively prime. Substitute $x = 0, 1, 2$ to the equation to solve for y which gives us $(0, \frac{1}{3}), (1, -\frac{4}{3})$ and $(2, -3)$. Hence $(x, y) = (2, -3)$ is a pair of integral solution for the equation $5x + 3y = 1$. Then the general solution set of the equation $5x + 3y = 1$ is

$$\{(2 + 3k, -3 - 5k), \ k \text{ is any integer}\}$$

Now it will be shown that this algorithm is valid. .

Proof. First, we will show that there is at least one pair of integral solutions with x value in the set $\{0, 1, 2, \cdots, b-1\}$. □

Since a and b are relatively prime, it is well known **[reference]** that the greatest common divisor of a and b is 1 and there exist integral solutions for $ax + by = 1$. Assume (x_1, y_1) is a solution of the equation $ax+by = 1$, then $ax_1+by_1 = 1$. Now from the integer (x_1+kb, y_1-ka), where k is an integer, we have

$$\begin{aligned} a(x_1 + kb) + b(y_1 - ka) &= ax_1 + akb + by_1 - bka \\ &= ax_1 + by_1 \\ &= 1 \end{aligned}$$

Hence, $(x_1 + kb, y_1 - ka)$ is also a solution for $ax + by = 1$.

Now we will show there exists one solution with $x \in \{0, 1, \cdots, b-1\}$. By division algorithm, there exists integers q and r such that

$$x_1 = qb + r, \ \text{where } 0 \le r < b$$

Let $x_0 = x_1 - qb$ and $y_0 = y_1 + qa$, then $0 \le x_0 = r \le b-1$ and (x_0, y_0) is the solution with x value in the desire domain $\{0, 1, \cdots, b-1\}$.

Second, we will show that there is at most one solutions with $x \in \{0, ..., b-1\}$.

Suppose (x_2, y_2) is another integral solution for the equation $ax + by = 1$ with $x_2 \neq x_0$. We have

$$ax_0 + by_0 = ax_2 + by_2 = 1$$

and then

$$a(x_0 - x_2) = b\,(y_2 - y_0)$$

Since a and b are relatively prime and b divides $a(x_0 - x_2)$, we know $b|(x_0 - x_2)$ and $x_0 - x_2$ is a multiple of b. Hence (x_0, y_0) is the unique solution with the x value in $\{1, 2, \cdots, b-1\}$ $\square$

Given $a, b \in \mathbb{Z}$, the classical Euclidean algorithm **[add reference]** uses the division algorithm repeatedly to obtain a series of equations of the form

$$a = bq_1 + r_1,\ b = r_1 q_2 + r_2, ..., r_{j-2} = r_{j-1} q_j + r_j$$

The last non-zero r_j is $gcd(a, b)$. Then we do back substitution to find x, y.

Example 2. Apply both Euclidean algorithm and alternative algorithm to find one solution of the equation

$$23x + 13y = 1$$

with x value in the set $\{0, 1, \cdots, 13\}$.

Euclidean Algorithm: we first find $gcd(23, 13)$ as following

$$\begin{aligned} 23 &= 13 \cdot 1 + 10 \\ 13 &= 10 \cdot 1 + 3 \\ 10 &= 3 \cdot 3 + 1 \end{aligned}$$

Then we do the back-substitution as following

$$\begin{aligned} 1 &= 10 - 3 \cdot 3 \\ &= 10 - 3 \cdot (13 - 10) \\ &= 4 \cdot 10 - 3 \cdot 13 \\ &= 4 \cdot (23 - 13) - 3 \cdot 13 \\ &= 4 \cdot 23 - 7 \cdot 13 \end{aligned}$$

Hence $(4, -7)$ is one solution.

Alternative algorithm: Substitute values from the set $\{0, 1, \cdots, 12\}$ for x in order until we find a pair of integral solutions

x	0	1	2	3	4
y	$\frac{1}{13}$	$-\frac{22}{13}$	$-\frac{45}{13}$	$-\frac{68}{13}$	-7

We stop at $x = 4$ and $(4, -7)$ is one solution.

Both algorithms are appropriate, the users will probably find one algorithm more preferable than another in given situations.

All Solutions for $ax + by = c$

In this section we will show that the set of all integral solutions for $ax + by = c$ is $\{(cx_0 + kb, cy_0 - ka), k \text{ is any integer}\}$, where a, b, c are nonzero integers and $\gcd(a, b) = 1$. So we only need to know how to solve $ax + by = 1$ to find all solutions for $ax + by = c$.

First, using the algorithm in the previous section, we find a solution (x_0, y_0) for the equation $ax + by = 1$. Then we have

$$\begin{aligned} ax_0 + by_0 &= 1 \\ c\,(ax_0 + by_0) &= c \\ a\,(cx_0) + b\,(cy_0) &= c \end{aligned}$$

Thus, (cx_0, cy_0) is a solution for $ax + by = c$.

Next, we will find a general solution for $ax + by = c$.

By the same argument in the previous section for finding general solutions of $ax+by = 1$, we conclude that $\{(cx_0+kb, cy_0-ka), k \text{ is any integer}\}$ is the solution set of the equation $ax + by = c$. □

Application

There are many applications in the real world that require natural solutions, as illustrated in the following two examples.

Example 3. A school has budget of \$40.90 for pencils and erasers. Erasers cost 7 cents each and pencils cost 17 cents each. How many of each should be purchased to have at least one eraser per pencil, which minimizes the number of erasers left over and uses the entire budget?

Let x be the number of erasers and y be the number of pencils purchased. The problem can be interpreted by finding the maximum number of pencils and minimum number of erasers where

$$7x + 17y = 4090, \;\; x \geq y > 0, \;\; x, y \in \mathbb{N}$$

Since $\gcd(7,17) = 1$, we will first substitute $y = 0, ..., 6$ in order to find one solution for $7x + 17y = 1$.

y	0	1	2	3	4	5
x	$\frac{1}{17}$	$-\frac{16}{7}$	$-\frac{33}{7}$	$-\frac{50}{7}$	$-\frac{67}{7}$	-12

We stop at $y = 5$ and $(-12, 5)$ is a solution for $7x + 17y = 1$. Then $(-12 \cdot 4090, 5 \cdot 4090) = (-49080, 20450)$ is one solution for $7x + 17y = 4090$ and the general solutions are

$$(-49080 + 17k, 20450 - 7k), \ \ k \text{ is any integer}$$

We are trying to find largest y such that $x \geq y$ and $x, y \in \mathbb{N}$. By solving $-49080 + 17k \geq 20450 - 7k > 0$, $k \in \mathbb{Z}$, we obtain $2922 > k \geq 2898$. Since $x = -49080 + 17k$ is a decreasing function, the largest x occurs at $x = 2898$ and the solution is $(186, 164)$.

The best use of the budget \$40.90 is buying 186 erasers and 164 pencils.

Example 4. David is buying apples and oranges for the dining hall. Apples cost 31 cents each and oranges cost 47 cents each. He wants to spend exactly \$82.98. He wants each student to have one orange and two apples with no oranges left over. How many apples will be left over?

Let x be the number of apples and y be the number of oranges purchased. The problem can be interpreted by finding the largest integral solution for y satisfying

$$31x + 47y = 8298, 2y \geq x > 0, \ \ x, y \in \mathbb{Z}$$

We first find a specific solution for $31x + 47y = 1$. Since $31 < 47$, we are going to take $y = 0, .., 30$

y	0	1	2
x	$\frac{1}{31}$	$-\frac{46}{31}$	-3

We stop at $y = 2$ and obtain the special solution $(-3, 2)$. The general solution for $31x+47y = 8298$ is $(-24, 894+47k, 16, 596-31k)$. Since the condition is $2y \geq x > 0$, we have $2(16596 - 31 \cdot k) \geq -24894 + 47 \cdot k > 0$ and $535 \geq k \geq 533$. Since $y = 16596 - 31 \cdot k$ is a decreasing function, y is maximum when $k = 533$ and $(x, y) = (157, 73)$. We spend \$82.98 to buy 157 apples and 73 oranges with 11 apples left over.

In summary the introductory students of mathematics can effectively use the concept of slope of a straight line and limited inductive reasoning to solve Diophantine equations of the form $ax + by = c$.

References

[1] Introduction to the Theory of Numbers, Niven and Zuckerman