# A Top-down Approach for Solving Linear Diophantine Equation

Yiu-Kwong Man

***Abstract*—A simple approach for solving the linear Diophantine equation via the Euclidean Algorithm (EA) is presented. Unlike the common approach for applying the Extended Euclidean Algorithm (EEA), we present a top-down approach for finding the unknowns by the sequence of quotients obtained by successive divisions. Some illustrative examples are provided.**

***IndexTerms*—Diophantine equation, Euclidean Algorithm, Extended Euclidean Algorithm, top-down approach.**

## I. Introduction

THE Euclidean Algorithm (EA) and the Extended Euclidean Algorithm (EEA) have important applications in areas such as matrix Pade approximations, privacy and secure communications, and knot theory [1, 2, 5, 7], etc. In this paper, we present a simple top-down approach for solving linear Diophantine equation via EA. Unlike the common bottom-up approach employed by the EEA to compute the particular solution of a given linear Diophantine equation, the new approach can be applied to compute the solution by the sequence of quotients obtained by the Euclidean algorithm [3, 4, 6]. This approach is highly suitable for either hand calculation or machine computation.

The whole paper is organized like this. The mathematical background is described in section 2. Then, the new approach is introduced in section 3, followed by some examples in section 4. Finally, some concluding remarks are provided in section 5.

## II. Mathematical Background

Given two positive integers $a$ and $b$ such that $a > b$, we can compute their greatest common divisor GCD ($a$, $b$) by the Euclidean Algorithm below.

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\vdots \\ r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1} \\ r_{n-2} &= r_{n-1}q_n \end{aligned}$$

where $q_i$, $r_i$ are the successive quotients and remainders obtained by the divisions involved in the Euclidean Algorithm. Then, GCD ($a$, $b$) is given by $r_{n-1}$. Moreover, if we are required to solve the Diophantine equation $ax + by = c$, where $c$ is divisible by GCD ($a$, $b$), then we can apply a bottom-up approach to compute a particular solution, which is often called the Extended Euclidean Algorithm. The following example illustrates how it works.

The author is an Associate Professor of the Department of Mathematics and Information Technology, EdUHK and a member of *IAENG*. (E-mail: ykman@ eduhk.hk).

Example 1. Solve the linear Diophantine equation $126x + 35y = 14$ by the Extended Euclidean Algorithm.

Solution. By the Euclidean Algorithm, we have:

$$\begin{aligned} 126 &= 3 \times 35 + 21 \\ 35 &= 1 \times 21 + 14 \\ 21 &= 1 \times 14 + 7 \\ 14 &= 2 \times 7 \end{aligned}$$

Hence, GCD(126, 35) = 7. Now, working in a reverse order (bottom-up) for the above equations. We have

$$\begin{aligned} 7 &= 21 - 1 \times 14 \\ &= 21 - (35 - 21) \\ &= 2 \times 21 - 35 \\ &= 2 \times (126 - 3 \times 35) - 35 \\ &= 2 \times 126 - 7 \times 35 \end{aligned}$$

So, $x = 2$, $y = -7$ is a particular solution of $126x + 35y = 7$. Hence, $x = 4$, $y = -14$ is a particular solution of $126x + 35y = 14$ and the general solution is given by $x = 4 - 35t$, $y = -14 + 126t$, where $t$ is an arbitrary integer constant.

From this example, we can see that finding a particular solution is a crucial step in solving the given Diophantine equation. However, the drawback in applying the bottom-up approach is that we have to remove the brackets quite often in order to express the GCD as a linear combination of the integer coefficients of the given Diophantine equation. Can we work in a top-down approach instead? The answer is affirmative and we will introduce such an approach in the next section.

## III. A Top-down Approach

By using the same notations as above, we have

$$\begin{aligned} r_1 &= a - bq_1 \\ r_2 &= b - r_1q_2 = b - (a - bq_1)q_2 = -a\,q_2 + (1 + q_1q_2)b \\ r_3 &= r_1 - r_2q_3 = (a - bq_1) - q_3[-a\,q_2 + (1 + q_1q_2)b] \\ &= a\,(1 + q_1q_2) - [q_1 + q_3\,(1 + q_1q_2)]\,b \\ r_4 &= r_2 - r_3q_4 \\ &= -aq_2 + (1 + q_1q_2)b - q_4[a\,(1 + q_2q_3) - (q_1 + q_3\,(1 + q_1q_2))\,b] \\ &= -a\,[q_2 + q_4\,(1 + q_2q_3)] + [q_1\,q_4 + (1 + q_1q_2)\,(1 + q_3q_4)]\,b \end{aligned}$$

ISBN: 978-988-14048-6-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

and so on. We can see that the coefficients of $a$ and $b$ can be computed effectively by the following steps.

(i) For finding the coefficient of $b$, we can proceed like this:

| | $q_1$ | $q_2$ | $q_3$ | $q_4$ | … |
|---|---|---|---|---|---|
| 1 | $q_1$ | $1 + q_1 q_2$ | $q_1 + q_3 (1 + q_1 q_2)$ | $(1 + q_1 q_2) + q_4 [q_1 + q_3 (1 + q_1 q_2)]$ | … |
| + | – | + | – | + | … |

First, write the quotients $q_1, q_2, \ldots, q_{n-1}$ obtained in the first row. Then, multiply $q_1$ by 1 and write the product next to it. Then, multiply $q_2$ by $q_1$ and add the product to the previous number, namely 1, to obtain $1 + q_1 q_2$. Similarly, multiply $q_3$ by $1 + q_1 q_2$ and add the product to the previous number, namely $q_1$, to obtain $q_1 + q_3 (1 + q_1 q_2)$. Repeat the process for each quotient appeared in the first row. Then, the coefficient of $b$ is given by the last answer in the second row and its sign (+ or –) is indicated by the sign appeared in the third row below.

(ii) For finding the coefficient of $a$, we can proceed similarly as follows:

| | $q_2$ | $q_3$ | $q_4$ | … |
|---|---|---|---|---|
| 1 | $q_2$ | $1 + q_2 q_3$ | $q_2 + q_4 (1 + q_2 q_3)$ | … |
| + | – | + | – | |

The calculation procedure is similar to that described above, so we do not repeat the details here.

The advantage for adopting such a top-down approach is that we can avoid the tedious task for removing the brackets required in the traditional bottom-up approach. Also, the whole computational procedure do not require the knowledge of the remainders obtained by the divisions, but only the quotients. Hence, it is highly suitable for either hand calculation or implementation in common computer languages.

## IV. EXAMPLES

Example 2. Find a particular solution of the Diophantine equation $126x + 35y = 7$ by applying the top-down approach.

Solution. Referring to Example 1, the quotients (except the last one) obtained by successive divisions are 3, 1 and 1, respectively. Following the procedure described in the last section, we have:

| | 3 | 1 | 1 |
|---|---|---|---|
| 1 | 3 | 4 | 7 |
| + | – | + | – |

Thus, $y = -7$. Similarly,

| | 1 | 1 |
|---|---|---|
| 1 | 1 | 2 |
| + | – | + |

So, $x = 2$. In other words, (2, -7) is a particular solution of the given Diophantine equation, which is the same as that obtained by the traditional EEA, but no removal of brackets is needed.

Example 3. Solve the Diophantine equation $2406x + 654y = 6$ by applying top-down approach.

Solution. Using the common presentation of the Euclidean algorithm by long divisions, we have

| | | | |
|---|---|---|---|
| 3 | 2406 | 654 | 1 |
| | 1962 | 444 | |
| 2 | 444 | 210 | 8 |
| | 420 | 192 | |
| 1 | 24 | 18 | 3 |
| | 18 | 18 | |
| | 6 | | |

So, the successive quotients (except the last one) obtained are 3, 1, 2, 8 and 1, respectively. Following the procedure described in the third section, we have:

| | 3 | 1 | 2 | 8 | 1 |
|---|---|---|---|---|---|
| 1 | 3 | 4 | 11 | 92 | 103 |
| + | – | + | – | + | – |

Thus, $y = -103$. Similarly,

| | 1 | 2 | 8 | 1 |
|---|---|---|---|---|
| 1 | 1 | 3 | 25 | 28 |
| + | – | + | – | + |

So, $x = 28$. In other words, (28, -103) is a particular solution of $2406x + 654y = 6$. Hence, the general solution is given by $x = 28 - 654t$, $y = -103 + 2406t$, where $t$ is an arbitrary integer constant.

## V. FINAL REMARKS

In this paper, we have introduced a simple top-down approach for solving linear Diophantine equation, which is more elegant than the traditional bottom-up approach as described in [3, 6]. Since the EA and EEA algorithms have wide applications in various disciplines, we anticipate that this approach can be found useful for reference by researchers working in related areas or instructors involved in teaching number theory, discrete mathematics and computer programming, etc.

## REFERENCES

[1] P. Achuthan and S. Sundar, "A new application of the Extended Euclidean algorithm for matrix Pade approximants", *Comput. Math. Appl*, vol. 16, pp, 287-296, 1988.
[2] B. Anjanadevi, P. S. Sitharama Raju, V. Jyothi and V. Kumari, "A Novel approach for privacy preserving in video using Extended

Euclidean algorithm based on Chinese Remainder Theorem", *Int. J. Communication & Network Security*, vol. 1, pp. 45-49, 2011.
[3] D. M. Burton, *Elementary Number Theory*, Boston: Allyn and Bacon, 1980.
[4] J. Gathen and J. Gerhard, *Modern Computer Algebra*, Cambridge: Cambridge University Press, 1999.
[5] J. A. M. Naranjo, J. A. Lopez-Ramos and L. G. Casado, "Applications of the Extended Euclidean Algorithm to privacy and secure communications", *Proceedings of the 10th International Conference on Computational and Mathematical Methods in Science and Engineering*, CMMSE 2010, pp. 27-30, 2010.
[6] O. Ore, *Number Theory and Its History*, NY: Dover, 1988.
[7] M. Syafiq Johar, "Minimal number of steps in the Euclidean algorithm and its application to rational tangles", *Rose-Hulman Undergraduate Mathematics Journal*, vol. 16, article 3, 2015.

ISBN: 978-988-14048-6-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)