Vol.6.Issue.2.2018 (April-June)

http://www.bomsr.com
Email:editorbomsr@gmail.com

RESEARCH ARTICLE

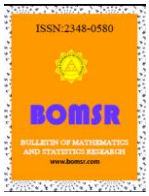
BULLETIN OF MATHEMATICS AND STATISTICS RESEARCH

A Peer Reviewed International Research Journal

INTERNATIONAL STANDARD SERIAL NUMBER 2348-0580

SOME NOTES ON LINEAR DIOPHANTINE EQUATIONS AND THE EUCLIDEAN ALGORITHM

LIJIANG ZENG
Research Centre of Zunyi Normal College, Zunyi 563000, GuiZhou, China
E-mail: ZLJ4383@sina.com



ABSTRACT

Linear Diophantine equation both in mathematics and other natural sciences, has extremely important position, Euclidean algorithm is a powerful mathematical tool in number theory and mathematical, based on the greatest common divisor of the bridge link the linear Diophantine equation and Euclidean algorithm, we obtained the new math concepts -- vector Euclidean algorithm, the vector Euclidean algorithm is quick and easy role to solve concrete problems.

Key words: linear Diophantine equation; Euclidean algorithm; linear programming; greatest common divisor

MSC2010: 11D04; 11A05

1. Introduction

Linear Diophantine equation[1-7] and Euclidean algorithm[8-11] in number theory, linear programming[12-14], integer programming[15-16], and other applied subjects plays an extremely important role, and their close relationship exists between the links, relationship between them is the greatest common divisor[17] of two integers, the greatest common divisor is not only in solving linear Diophantine equation, not only discriminating solvability and other links play an important role, but also in Euclidean algorithm also plays a very important role, in this paper by using the greatest common divisor this tool, in-depth study of linear Diophantine equation and Euclidean algorithm, obtained the significant vector Euclidean algorithm concept and its natures.

2. Some facts on linear Diophantine equations

The simplest nontrivial Diophantine equations are linear equations in two variables.

$ax + bv = c$, where $a, b, c \in Z$

Such an equation may have infinitely many solutions or none. For example.

The equation

$6x + 15y = 0$

has the infinitely many solutions *x*=15*t*. *y*=-6*t* as *t* runs through the integers. On the other hand, the equation

$$6x + 15y = 0$$

has no integer solutions. This is so because 3 divides 6x + 15y when *x* and *y* are integers (since 3 divides both 6 and 15) but 3 does not divide l. This example shows that common divisors are involved in linear Diophantine equations, and exposes the key to their solution: the linear representation of the gcd(i.e., the greatest common divisor).

3.Criterion for solvability of linear Diophantine equations.

Proposition 1. When a, b, c are integers, the equation $ax + by = c$ has an integer solution if and only if gcd (a, b) divides c.

Proof. Since $gcd(a, b)$ divides *a* and *b*, it divides *ax+by* for any integers *x* and *y*. Therefore, if *ax+by=c*, then gcd(*a*, *b*) divides *c*.

Conversely, we know there exist some integers *m* and *n* such that gcd(*a*, *b*)=*am+bn*. Hence if g gcd(*a*, *b*) divides *c* we have

$$c = gcd(a, b)d \ = \ (am \ + \ bn)d \ = \ amd + bnd \text{ for some } d \mid Z .$$

But then $x = md$， $y = nd$ is a solution of $ax + by \ = \ c$.

This proof also shows how to find a solution $ax + by \ = \ c$ if one exists. Namely, express $gcd(a, b)$ in the form $am + bn$, using the symbolic Euclidean algorithm to find m and n, then multiply m and n by the integer d such that $c = gcd(a, b)d$.

If there is one solution $x = x_0$ and $y = y_0$, then there are infinitely many, because we can add to the pair (x_0, y_0) any of the infinitely many solutions of *ax+by*=0.

4. General solution of $ax + by = c$.

Proposition 2. The solution of $ax + by = c$ in *Z* is $x = x_0 + \frac{b}{\gcd(a, b)}t$, $y = y_0 - \frac{a}{\gcd(a, b)}t$

where $x = x_0$, $y = y_0$ is any particular solution and *t* runs through *Z*.

Proof. Since $x = \frac{b}{\gcd(a, b)}t$, $y = -\frac{a}{\gcd(a, b)}t$ is clearly an integer solution of *ax+by =0*, adding it to any solution $x = x_0$, $y = y_0$ of $ax + by = c$ gives another solution of $ax + by = c$.

Conversely, if *x*, *y* is any solution of *ax+by=c*, then $x' = x - x_0$, $y' = y - y_0$ satisfies $ax' + by' = 0$. But any integer solution of a $ax' + by' = 0$ is a solution of the equation

$$a'x' = -b'y'$$

whose coefficients are the relatively prime integers $a' = \frac{a}{\gcd(a, b)}$, $b' = -\frac{b}{\gcd(a, b)}$

Since a' and b' have no common prime divisor, it follows from the unique prime factorization of both sides of the equation $a'x' = -b'y'$ that

b' divides x'. That is $x' = b't$ for some integer *t*, and hence $y' = -a't$, Substituting the values of x', y', a', b' back in the equations above yields

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

as claimed.

5. The vector Euclidean algorithm

We used an extension of the Euclidean algorithm to compute the gcd of integers *a* and *b* in the form

$\gcd(a, b)$ =*ma+nb* for some $m, n \in Z$

The extension runs the ordinary algorithm ("subtracting the smaller number from the larger") and uses it to guide a symbolic imitation that performs e same operations on linear combinations of the letters a and *b*.

We now wish to analyze the symbolic part of the algorithm more closely in the case where a and *b* are relatively prime. To do so we replace each linear combination $m_i a + n_i b$ by the ordered pair (m_i, n_i) enable the ordinary algorithm to run as simply as possible we take *a*>0 and *b*<0 and keep the positive number in the first place and the negative in the second.

Then each step of the ordinary Euclidean algorithm is actually an addition: the number with the larger absolute value being replaced by its sum with the other number. The corresponding steps in the symbolic a1gorithm are vector additions so we ca11 the resulting process the vector Euclidean algorithm.

Example 1.

Table 2.1 shows the steps of the vector Euclidean algorithm on (12, -5), with number pairs in the first column, symbolic pairs in the second column, and vector pairs in the third. The actual additions are shown only in the symbolic column.

Table 2.1: Outputs of Euclidean algorithm

Number	Symbolic pairs	Vector pairs
$(12, -5)$	(a, b)	$((1, 0), (0, 1))$
$(7, -5)$	$(a + b, b)$	$((1, 1), (0, 1))$
$(2, -5)$	$((a + b) + b, b) = (a + 2b, b)$	$((1, 2), (0, 1))$
$(2, -3)$	$(a + 2b, b + (a + 2b)) = (a + 2b, a + 3b)$	$((1, 2), (1, 3))$
$(2, -1)$	$(a + 2b, a + 3b + (a + 2b) = (a + 2b, 2a + 5b)$	$((1, 2), (2, 5))$
$(1, -1)$	$(a + 2b + (2a + 5b), 2a + 5b) = (3a + 7b, 2a + 5b)$	$((3, 7), (2, 5))$

From the bottom line of Euclidean algorithm that

$$1 = 3a + 7b = 3\times 12 - 7\times 5$$

so $(m, n) = (3, 7)$, $\Rightarrow$(3, 7) is a natural number vector such that $12m - 5n = 1$.

It is also interesting to run the algorithm one step further (adding the number **1** to the number **-1** in the first column to get **0**)because **12** and **5**then reappear in the vector column.

Table 2.2:Result of the extra step

$(1, 0)$	$(3a + 7b, 2a + 5b) + (3a + 7b) = (3a + 7b, 5a + 12b)$	$((3, 7), (5, 12))$

This is not surprising because 0 = 5×12-12×5 though conceivably we could have obtained a larger multiple of the vector (5, 12). What is interesting is how easily we arrive at the vector (5, 12): namely we started with the vector ***i***= (1, 0) and ***j***=(0, 1) and took a series of steps in which a vector pair (v_1, v_2) was replaced by either $(v_1 + v_2, v_2)$ or $(v_1, v_1 + v_2)$

We now generalize this example to show:

6. Relative primality in the vector Euclidean algorithm.

Proposition 3. In running the vector Euclidean algorithm:

1. Every vector produced from (1, 0) and (0, 1) is a relatively prime pair of natural numbers. (We call such a vector primitive.)

2. Every relatively prime pair (*a*, *b*) of natural numbers can be produced (by starting the ordinary Euclidean algorithm on *b* and -*a*).

Proof. 1. It is clear that any vector produce is a pair of natural numbers, because the first new pair is (1, 1) and further vector additions cannot decrease the members of the pair. To see why each pair produced is relatively prime we prove a stronger property: if $((m_1, n_1), (m_2, n_2))$ is the vector pair at any step, then

$m_1 n_2 - n_1 m_2 = 1$

This is true at the first, when $(m_1, n_1) = (1, 0)$ and $(m_2, n_2) = (0, 1)$. And if it is true for the vector pair $((m_1, n_1), (m_2, n_2))$ then it is also true for the next pair $((m_1 + m_2, n_1 + n_2), (m_2, n_2))$ or $((m_1 + m_2), (m_1 + m_2, n_1 + n_2))$.

This is so because

$(m_1 + m_2)\ n_2 - (n_1 + n_2)m_2 = m_2 n_1 - n_1 m_2 = 1$

and

$m_1\ (n_1 + n_2) - n_1(m_1 + m_2) = m_1 n_2 - n_1 m_2 = 1$

It follows that each vector (m_1, n_1) produced is a relatively prime pair because any common divisor of m_1 and n_1 also divides $m_1 n_2 - n_1 m_2 = 1$. Similarly for each vector (m_2, n_2).

3. If *a* and *b* are relatively prime natural numbers then the vector Euclidean algorithm guided by the ordinary Euclidean algorithm on *b* and *–a* produces a vector (m, n) such that *mb-na*=0 and *m* and *n* are relatively prime by part 1.

Since prime factorization is unique, *mb=na* for relatively prime *a*, *b* and relatively prime *m*, *n* implies *m=a* and *n=b*. Hence any relatively prime pair (a, b) can be produced by the vector Euclidean algorithm

7. Conclusions

From the above, we have seen that Euclidean algorithm is a powerful mathematical tool in number theory and mathematical, based on the greatest common divisor of the bridge link the linear Diophantine equation and Euclidean algorithm, we obtained the new math concepts - vector Euclidean algorithm, the vector Euclidean algorithm is quick and easy role to solve concrete mathematical problems.

Reference

[1]. Jiagui Luo, Alain Togbé, Pingzhi Yuan. On Some Equations Related to Ma's Conjecture[J]. Integers . 2011 (5), 45-52

[2]. J. Luo, P. Yuan. ON THE DIOPHANTINE EQUATION axn+2l + c/abt(2)xn + c = by(2) [J]. Acta Mathematica Hungarica . 2011 (2), 55-62

[3]. S. P. Mohanty, A. M. S. Ramasamy. The simultaneous Diophantine equations 5y 2 ? 20 = x 2 and 2y 2 + 1 = z 2[J]. Journal of Number Theory . 1984 (1), 51-56

[4]. Walker D T. On the Diophantine equation mx2-nY2=±1[J]. The American Mathematical Monthly . 1967 (4), 41-46

[5]. Le M-H. A conjecture concerning the exponential diophantine equation a~x+b~y=c~z[J]. Acta Arithmetica . 2003(2), 35-39

[6]. Le M-H. A note on then exponential diophantine equation a~x+b~y=c~z [C]. Proceedings of the Japan Academy. 2004, 90-96

[7]. Le M-H. A conjecture concerning the pure exponential diophantine equation a~x+b~y=c~z[J]. Acta Math. Sinica,English Series . 2005(4), 40-45

[8]. Le M-H. An open problem concerning the diophantine equation a~x+b~y=c~z. Publications Mathematicae Debrecen [C]. 2006, 100-105

[9]. D. M. Mandelbaum. On Iterative array for the Euclidean algorithm over finite fields. IEEE Trans. On Computers [C]. 1989, 92-96

[10]. MISHRA P.K.. Optimal parallel algorithm for shortest-paths problem on interval graphs[J]. Journal of Zhejiang University Science. 2004(09) , 25-30

[11]. Win, M. Z. Pinto, P. C. Shepp, L.A. A Mathematical Theory of Network Interference and Its Applications. Proceedings of Tricomm[C] . 2009, 110-116

[12]. P. Baginski, S. T. Chapman, K. McDonald, L. Pudwell. On cross numbers of minimal zero sequences in certain cyclic groups[J]. Ars Combinatoria . 2004(3), 40-45

[13]. Askari-Nasab, H. Pourrahimian, Y. Ben-Awuah, E. Kalantari, S. Mixed integer linear programming formulations for open pit production scheduling[J]. Journal of Mining Science . 2011(2), 34-40

[14]. Dimitrakopoulos, R., Ramazan, S. Stochastic integer programming for optimising long term production schedules of open pit mines: Methods, application and value of stochastic solutions[C]. Transactions of the Institutions of Mining and Metallurgy, Section A: Mining Technology . 2008, 56-61

[15]. Hanho Lee VLSI designs of Reed-Solomon decoder architectures[C]. Proceedings of the 2000 IEEE International Symposium on Circuits and Systems. 2000, 156-161

[16]. Hanho Lee. Modified Euclidean Algorithm Block for High-Speed Reed-Solomon Decoder[C]. IEE Electronics Letters. 2001, 230-236

[17]. Pablo Huijse, Pablo A. Estévez, Pavlos Protopapas, Pablo Zegers, José C. An information theoretic algorithm for finding periodicities in stellar light curves[C]. Principe. IEEE Transactions on Signal Processing . 2012, 85-90

About The Author

Lijiang Zeng (1962 -), male, born in Chishui of Guizhou Province, Professor of Zunyi Normal College, major research field: mathematics and applied mathematics, research direction: algebra and its application, number theory and its application. Have existed search results: CPCI-S(ISTP), CPCI-SSH(ISSHP), and EI 20 articles published, Email: ZLJ4383@sina.com .