The Very Useful Linear Indefinite Equations in Applied Sciences

Lijiang Zeng
(Research Centre of Zunyi Normal College,
Zunyi 563099, GuiZhou, P. R. China)

Abstract—The number theory is an important branch of mathematics. The paper introduced some methods of solving linear indefinite equation in convergent and the so-called extended Euclid's algorithm, and got two results about linear indefinite equation. And it is very important for our understanding and using linear indefinite equation in many applied sciences.

Key words—*great common divisor; indefinite equation; convergents; integer lattice-points; xy-plane*

I. INTRODUCTION

One of an important branch of mathematics is number theory[1-6], in the number theory, linear indefinite equation[7-10] plays a foundation, and its important role. Linear indefinite equation is an irreplaceable tool in many applied sciences, for example, the linear programming in operational research[11-15], have a special part is integer programming, however, the important role of integer programming is linear indeterminate equation.

II. SOME NOTES ON LINEAR INDEFINITE EQUATION

In the number theory, the algebraic equation with two variables

$$ax + by = c \tag{1}$$

is called a linear indefinite equation, and it is also called linear Diophantine equation[16-17] sometimes, for which we wish to find integer solutions in x and y.

A linear indefinite equation is a type of algebraic equation with two linear variables. For this reason, it is sometimes also called a bilinear Diophantine equation. In this type of equation $ax+by=c$, we are only interested in the integer solutions in x and y.

In this paper we always note the fact "can not exactly divide" in symbol "$\nmid$", and the fact "can exactly divide" in symbol "$|$". For example, a can not exactly divide b, we note as $a \nmid b$. a can exactly divide b, we note as $a|b$, and we always note the great common divisor of a and b in symbol "$\gcd(a, b)$", other letters is similar meaning. We first explained it here, because we will use these symbols repeatedly.

III. TWO PROPOSITIONS

Proposition 1. Let a, b, c be integers with not both a and b equal to 0, and let $d=\gcd(a, b)$. If d can not exactly divide c, then the linear indefinite equation

$$ax + by = c$$

has no integer solution. The equation has an integer solution in x and y if and only if $d \nmid c$. Moreover, if (x_0, y_0) is a solution of the equation, then the general solution of the

Author introduction: Lijiang Zeng (1962 -), male, born in Guizhou Province of China, 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: ISTP 2 articles, ISSHP 5 articles, Email: ZLJ4383@sina.com .

equation is

$$(x, y) = \left(x_0 + \frac{b}{d} \bullet t,\ y_0 - \frac{a}{d} \bullet t \right) \quad t \in Z \quad (2)$$

Proof. Assume that x and y are integers such that $ax + by = c$. Since $d|a$ and $d|b$, $d|c$. Hence, if $d \nmid c$, there is no integer solutions of the equation.

Now suppose $d|c$. There is an integer k such that $c=kd$. Since d is a sum of multiples of a and b, we may write $am + bn = d$.
Multiplying this equation by k, we get $a(mk)+b(nc)=dk=c$, so, that $x=mk$ and $y = nk$ is a solution.

For the "only if" part, suppose x_0 and y_0 is a solution of the equation. Then $a x_0 + b y_0 = c$. Since $d|a$ and $d|b$, then $d|c$. □

Observe that the proof of **Proposition 1**, together with Euclid's algorithm[16], provides us with a practical method to obtain one solution of the equation. In what follows, however, we shall show how to find z and y by using the continued fraction method.

Suppose that a and b are two integers whose gcd is d and we wish to solve indefinite equations

$$ax-by=d. \quad (3)$$

We expand $\frac{a}{b}$ as a finite continued fraction with convergents

$$\left[\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, \cdots, \frac{P_{n-1}}{Q_{n-1}}, \frac{P_n}{Q_n} \right] = \frac{a}{b} \quad (4)$$

Since d=gcd(a, b), we must have $a=da'$, $b= db'$ and gcd(a', b')=1. Then $\frac{P_n}{Q_n} = \frac{a'}{b'}$ and both fractions are in their lowest terms, giving $P_n = a'$, $Q_n = b'$. So equation (3) gives

.

$$P_n Q_{n-1} - Q_n P_{n-1} = a' Q_{n-1} - b' P_{n-1} = (-1)^{n-1} \quad (5)$$

Hence

$$aQ_{n-1} - bP_{n-1} = da' Q_{n-1} - db' P_{n-1} = (-1)^{n-1} d \quad (6)$$

or

$$(-1)^{n-1} aQ_{n-1} - (-1)^{n-1} bP_{n-1} = d \quad (7)$$

A solution to the equation $ax-by = d$ is therefore given by

$$\begin{cases} x = (-1)^{n-1} Q_{n-1} \\ y = (-1)^{n-1} P_{n-1} \end{cases} \quad (8)$$

To conclude the above analysis, we have the following **Proposition** for solving the linear indefinite equation $ax-by = d$:

Proposition 2. Let the convergents of the finite continued fraction of $\frac{a}{b}$ be as follows:

$$\left[\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, \cdots, \frac{P_{n-1}}{Q_{n-1}}, \frac{P_n}{Q_n} \right] = \frac{a}{b} \quad (9)$$

Then the integer solution[18-19] in x and y of the equation $ax-by = d$ is

$$\left. \begin{array}{l} x = (-1)^{n-1} Q_{n-1} \\ y = (-1)^{n-1} P_{n-1} \end{array} \right\} \quad (10).$$

To imitate the proof of the above process, the proof of this Proposition **2** can be obtained, and also you can refer to [16]. □

IV. REMARK AND EXAMPLE

Remark 1. We have already known a way of solving equations like (3) by applying Euclid's algorithm to a and b and working backwards through the resulting equations (the so-called extended Euclid's algorithm). Our new method here turns out to be equivalent to this since the continued fraction for $\frac{a}{b}$ is derived from Euclid's algorithm However, it is quicker to generate the convergents $\frac{P_i}{Q_i}$ using the

recurrence relations than to work backwards through the equations in Euclid's algorithm

$$\left[1,\ 2, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{85}{53}, \frac{93}{58}, \frac{364}{227}\right]$$

We have $x = (-1)^{n-1} q_{n-1} = (-1)^{7-1} 58 = 58$

and $y = (-1)^{n-1} p_{n-1} = (-1)^{7-1} 93 = 93$. That is 364·58-227·93=1

Example 1. Use the continued fraction method to solve the following linear indefinite equation: **20719*x*+13871*y*=1.** Note first that

$$\begin{aligned} &20719x + 13871y = 1 \Leftrightarrow \\ &20719x - (-13871y) = 1 \end{aligned}.$$

Now since $\frac{20719}{13871}$ can be expanded as a finite continued fraction with convergents

$$\left[\begin{array}{l} 1, \frac{3}{2}, \frac{118}{79}, \frac{829}{555}, \frac{947}{634}, \frac{1776}{1189} \\ \frac{2723}{1823}, \frac{4499}{3012}, \frac{20719}{13871} \end{array}\right]$$

We have $x = (-1)^{n-1} q_{n-1} = (-1)^{8-1} 3012 = -3012$,

and $y = (-1)^{n-1} p_{n-1} = (-1)^{8-1} 4499 = -4499$

That is, $20719 \bullet (-3012) - 13871 \bullet (-4499) = 1$

The linear indefinite equation $ax + by = d$ can also be interpreted geometrically. If we allow (x, y) to be any real values, then the graph of this equation is a straight line L in the xy-plane. The points (x, y) in the plane with integer coordinates (x, y) are the integer lattice-points. Pairs of integers (x, y) satisfying the equation correspond to integer lattice-points(x, y) on L. Thus, **Proposition 1** tells us that L passes through such a lattice-point if and only if $\gcd(a, b)|d$, in which case it passes through infinitely many of them.

Remark 2. In some areas of number theory (see [16]), it may be necessary to solve the following more general form of linear **indefinite** equation:

$$axy + bx + cy = d. \tag{11}$$

Note first that this type of equation can be reduced to a factorization: multiplying (11) by a, adding be to both sides and factoring results in above

$$(ax+c)(ay+b) = ad+bc. \tag{12}$$

If mn is a factorization of $ad+bc$ and a divides n-c and m-b, an integer solution of (11) is

$$\begin{cases} x = \dfrac{n-c}{a} \\ y = \dfrac{m-b}{a} \end{cases} \tag{13}$$

Reference

[1] Wolfgang M. Schmidt. Simultaneous approximation to algebraic numbers by rationals[J]. Acta Mathematica. 1970 (1).21-26

[2] Fan Y, Liu H, Lluis Puig. Generalized Hamming weights and equivalences of codes[J]. Science in China, Ser. A. 2003(05).32-36

[3] LAN Tianzhu,XU Yancong,WANG Liangbin. NewExact Solutions of the Generalized Davey-Stewartson and Mikhailov-Shabat Equations[J]. Journal of hangzhou normal university (natural science edition). 2014(06). 23-26

[4] HU. M. Global Solution for Quasilinear Wave Equations with Viscosity and Nonlinear Perturbation[J]. Northeastern Mathematical Journal. 2001(03)

[5] Roland GLOWINSKI, Annalisa QUAINI. On the Numerical Solution to a Nonlinear Wave Equation Associated with the First Painlev着 Equation:an Operator-Splitting Approach[J]. Chinese Annals of Mathematics(Series B). 2013(02).89-96

[6] G.M. Coclite,H. Holden,K.H. Karlsen. Well-posedness of higher-order Camassa–Holm equations[J]. Journal of Differential Equations . 2008 (3). 78-86

[7] Wu W. ON THE CONSTRUCTION OF GROEBNER BASIS OF A POLYNOMIAL IDEAL BASED ON RIQUIER-JANET THEORY[J]. Systems Science and Mathematical Sciences. 1991(03). 43-51

[8] Oskar Perron. Grundlagen für eine Theorie des Jacobischen Kettenbruchal gorithmus[J]. Mathematische Annalen. 1907 (1).85-89

[9] Zeng L. Equivalence on finitely generated $R[G]$ module[C]. Proceedings of 2011 Asia-Pacific Youth Conference on Communication （2011APYCC）, April,4-6,2011(Hangzhou). 434-436

[10] Zeng L. On the algebraic integers in cyclotomic fields[C], Proceedings of International Conference on Engineering and Business Management(EBM2011), March, 22-24,2011(Wuhan). 2293-2296.32-37

[11] Muneo Chō,Takeaki Yamazaki. An Operator Transform from Class A to the Class of Hyponormal Operators and its Application[J]. Integral Equations and Operator Theory . 2005 (4) . 142-150

[12] Pietro Aiena,Carlos Carpintero,Ennis Rosas. Some characterizations of operators satisfying a-Browder's theorem[J]. Journal of Mathematical Analysis and Applications . 2005 (2). 87-95

[13] Xuefeng Wang. On concentration of positive bound states of nonlinear Schrödinger equations[J]. Communications in Mathematical Physics . 1993 (2) .57-65

[14] Paul H. Rabinowitz. On a class of nonlinear Schrödinger equations[J]. ZAMP Zeitschrift fürangewandte Mathematik und Physik . 1992 (2). 90-95

[15] Y. Xiao,H.Y. Zhang. A note on convergence of semi-implicit Euler methods for stochastic pantograph equations[J]. Computers and Mathematics with Applications . 2010 (4). 120-126

[16] Davenport H. The Higher Arithmetic, 5th edition[M]. Cambridge University Press, London, New York, 1982, 74-76.

[17] Sun Z H. Consecutive Numbers with the Same Legendre Symbol[C]. Proc.Amer. Math. Soc. 2002, 130: 2503-2507.

[18] Mallat S.A theory for multiresolution signal decomposition[C]. IEEE Transactions on Pattern Analysis and Machine Intelligence . 1989, 143-149

[19] Zeng Y, Li Y, Chen D. A HIERARCHY OF INTEGRABLE HAMILTONIAN SYSTEMS WITH NEUMANN TYPE CONSTRAINT[J]. Chinese Annals of Mathematics. 1992(03).64-69