Diophantine Equation

Amba Kulkarni

University of Hyderabad

13th March 2018

Diophantine Equation

A Diophantine Equation is a polynomimal equation in 2 or more unknowns such that all the unknown variables have integer solution.

There are fewer equations than unknown variables.

Diophantine refers to a Greek Mathematician of 3rd century Diophantus of Alexandria who studied such equations. He is the first who introduced symbols such as '$=$', '$<$', and letter-based symbols etc. in Algebra.

Examples of Diophantine Equation

ax+by=1	Linear Diophantine Equation
$w^3 + x^3 = y^3 + z^3$	smallest solution: $12^3 + 1^3 = 9^3 + 10^3 = 1729$ Hardy Ramanujan Number
$x^n + y^n = z^n$	Fermat's Last Theorem (No solutions for n $>$ 2)
$x^2 - ny^2 = \pm 1$	Pell's Equation
$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$	Erdoš-Straus Conjecture For every positive integer $n > 1$ there exists a solution in x,y,z > 1
$x^4 + y^4 + z^4 = w^4$	Elkies showed that there are many nontrivial solutions.

Diophantine: adjective for nature of solutions to be Integer

Diophantine Equation

Diophantus: Investigated **a rational** solution

Indians: Investigated **all Integer** solutions of 1st and 2nd dgeree

Diophantine: linear equations

Aryabhaṭṭa (5th AD) gave algorithm to solve linear equation. This is briefly described in Āryabhaṭīya. This description is very incomprehensible.

Later Bhaskara -I (7th century) gave a detailed algorithm with several examples in āryabhaṭīyabhāṣya and gave the name *kuṭṭaka*.

Diophantine: quadratic equations

No general method is known to solve quadratic or higher order equations.
Pell's equation: $x^2 - Dy^2 = 1$

Indians evolved an algorithm to solve these (during 7th to 11th century).

Systematic study of Diophantine equations in Europe began only in 17th century.

Prayojana

What motivated Indian to solve linear Diophantine equations?
Śulbasutras
Altar construction: Five layers of bricks with each layer having 21 bricks.
Total area: 1 square unit.

To have stability in structure, the cleavages between two adjacent bricks of two successive layers should not coincide.

Suppose a layer has x bricks of m^2 area and y bricks of n^2 area.
The problem reduces to solving simultaneous Diophantine equations
$x + y = 21$
$\frac{x}{m^2} + \frac{y}{n^2} = 1$

Baudhāyana's solutions

Suppose a layer has x bricks of m^2 area and y bricks of n^2 area.
$x + y = 21$
$\frac{x}{m^2} + \frac{y}{n^2} = 1$

There are two solutions for (x, y, m, n) viz. $(16, 5, 6, 3)$ and $(9, 12, 6, 4)$.

Baudhāyana's Sulvasutra:

Three types of square bricks of length $\frac{1}{6}$, $\frac{1}{4}$, and $\frac{1}{3}$.
1st, 3rd and 5th layer: 9 bricks of length $\frac{1}{6}$ and 12 bricks of length $\frac{1}{4}$
2nd and 4th layer: 16 bricks of length $\frac{1}{6}$ and 5 bricks of length $\frac{1}{3}$

Baudhāyana and āpastambha

Construction of śyena citi (Falcon shaped Altar)
$x + y + z + u = 200$ and $\frac{x}{m} + \frac{y}{n} + \frac{z}{p} + \frac{u}{q} = 7\frac{1}{2}$.

$x + y + z + u + v = 200$ and $\frac{x}{m} + \frac{y}{n} + \frac{z}{p} + \frac{u}{q} + \frac{v}{r} = 7\frac{1}{2}$.

Aryabhaṭa’s description

adhikāgrabhāgahāraṃ chindyādūnāgrabhāgahāreṇa
śeṣa parasparabhaktaṃ matiguṇamagrāntare kṣiptam
adhauparigunịtamantyayugūnāgracchedabhājite śeṣa
mādhikāgracchedaguṇam dvicchedāgramadhikāgrayutam

Aryabhaṭa's description: English Translation

Divide the divisor corresponding to the greater remainder by the divisor corresponding to the smalleer remainder. The residue (and the divisor corresponding to the smaller remainder) being mutually divided (until the remainder becomes zero), the last quotient should be multiplied by an optional integer and then added (in case the number of quotients of the mutual division is even) or subtracted (in case the number of quotients is odd) by the difference of the remainders. (Place the other quotients of the mutual division successively one below the other in a column; below them the result just obtained and underneath it the optional integer.) Any number below (that is, the penultimate) is multiplied by the one just above it and added by that just below it. Divide the last number (obtained so doing repeatedly) by the divisor corresponding to the smaller remainder; then multiply the residue by the divisor corresponding to the grater remainder and add the greater remainder. (The result will be) the number corresponding to the two divisors.

Aryabhaṭa's Formulation of Problem

Following three problems are equivalent to the problem of solving a linear Diophantine equation.

- Find an integer which when divided by two given integers leave two given remainders.
  Find N such that $N = ax + R_1 = by + R_2$
- Find a number x such that when multiplied by a and incresed / decreased by c is divisible by b.
  $ax + c = by$ or $ax - c = by$.
- Find two number x and y such that when multiplied by a and b give a constant difference c.
  $ax - by = c$.

ślokas from Bhāskarācharya's bījagaṇitam

bhājyo hāraḥ kṣepakaḥ ca-apavartaḥ
kenāpyādau sam̊bhave kuṭṭakārtham
yena cchinnau bhājyahārau na tena
kṣepaśetad duṣṭam-uddiṣṭam-eva

First the dividend(bhājya = a), divisor(hāra = b) and the constant(kṣepaka) should be simplified by dividing by the greatest common divisor, if any, for the solution of the kuṭṭaka $ax + c = by$

If it is not possible to divide the constant by the GCD of the dividend and divisor, such simplification is not possible.

ślokas from Bhāskarācharya’s bījagaṇitam

parasparam bhājitayoḥ yayoḥ yaḥ
śeṣaḥ tayoḥ syād apavartanam saḥ
tena apavartena vibhājitau yau tau
bhājyahārau dṛḍhsajñakau staḥ
mitho bhajetau dṛḍhabhājya harau
yāvat vibhājye bhavatīha rūpam
phalāni adaḥ adaḥ tad-adho niveśyaḥ
kṣepaḥ thatha ante khaṁ upa-antimena
svordhe hate-antena yute tad antyam tyajew
muhuḥ syād iti rāś yugmam
ūrdho vibhājyena dṛdhena taṣṭaḥ
phalam guṇaḥ syād aparo hareṇa

ślokas from Bhāskarācharya's bījagaṇitam

From the mutual division of divisor and dividend what remains is the common factor. Dividing them by the common factor, the quotients left are called steady(dṛḍha) coefficients. Mutually divide such simplified coefficients, till the remainder becomes unity.

Place the coefficients of mutual division one below the other and below them the constant and lastly zero to form a column. With the penultimate term of this column multiply the factor above and add the term below. The result should be used to replace the factor above. Delete the last term from the column and form the truncated column.

ślokas from Bhāskarāсharya's bījagaṇitam

Continue this process till only two factors are left in the column. Reduce these numbers by dividing the top one by the dividend and the lower one by the divisor.

The remainders so left will be the values of Labdhi (y) and guṇa (x) respectively, subject to the conditions to be stated below.

ślokas from Bhāskarācharya's bījagaṇitam

evaṁ tadeva atra yadā samāptāḥ
syuḥ labdayaḥ ced viṣmāḥ tadānīm
yathāgatau labdhi guṇau viśdhyo
sva tatkṣaṇāt śṣamitau tu tau staḥ

In this manner, the results (x and y) obtained are true if the number of quotients (of mutual division) is even.

If the number of quotients is odd, the results (x and y) so obtained should be subtracted from the dividend and the divisor respectively and remainder derived will be the correct values of labdhi (y) and guṇa (x) respectively.

ślokas from Bhāskarācharya's bījagaṇitam

iṣṭāhataḥ sva sva hareṇ yukto
te vā bhavetāṁ bahudhā guṇāptī

Multiply the divisor and dividend by any optional number and add them to the respective value of x and y and obtain many values of x and y. This is to find the general solution for x and y.

An Example

ekaviṁśati yutaṁ śatadvayaṁ
yad guṇaṁ gaṇaka pañca ṣaṣṭhi yuk
pañca varjita śatadvayoddhrutaṃ
śuddhimeti guṇakaṁ vada āśu tam

Which number (x) multiplied by 221 and increased by 65 is completely divisible by 195?

$$221x + 65 = 195y$$

13 is the GCD of 221, 65 and 195

Dividing by 13, we get

$$17x + 5 = 15y$$

An Example .. Contd

$17x + 5 = 15y$

Dividend(bhājya) $=$ 17, Divisor(hāra) $=$ 15, kṣepaka(constant) $=$ 5

Dividend	Divisor	Quotient	Remainder
17	15	1	2
15	2	7	1

Valli:

Place the quotients, constant and zero in a column.

1
7
5
0

1	1
7	7*5+0=35
5	5
0	

1	(35*1+5)=40
7	(7*5+0)=35
5	-
0	-

An Example .. Contd

17x + 5 = 15y

1	(35*1+5=) 40
7	(7*5+0=) 35
5	-
0	-

(35,40) is a possible solution. Since (x+kn,y+kn) is a general solution, to get the smallest solution, we divide the values of y and x by dividend and divisor respectively such that the quotient is same.

40 / 17 : 40 = 17*2 + 6 ; y = 6
35 / 15 : 35 = 15*2 + 5 ; x = 5

Verification: 17x + 5 = 17 * 5 + 5 = 90 = 15 * 6 15y

General solution is $(15n + 5, 17n + 6)$

Thus possible solutions are
(x,y) = (5,6), (20,23), (35,40),...

Another Example

Find all possible solutions of the equation
$60x + 3 = 13y$

Dividend $= 60$
Divisor $= 13$
Constant $= 3$

Another Example .. contd

Dividend	Divisor	Quotient	Remainder
60	13	4	8
13	8	1	5
8	5	1	3
5	3	1	2
3	2	1	1

Place the quotients, constant and zero in a column.

4
1
1
1
1
3
0

Another Example .. contd

4	$15*4+9 = 69$
1	$9*1+6 = 15$
1	$6*1+3 = 9$
1	$3*1+3 = 6$
1	$3*1+0 = 3$
3	
0	

Since there are odd number of quotients,
$y = 60 - 69 = -9$
$x = 13 - 15 = -2$
So the solution is (-2,-9).

verification: $60 * -2 + 3 = -117$ and $13 * -9 = -117$

All possible solutions are
$x = 13n-2$, and $y = 60n-9$.
(-2,-9), (11,51), (24,111), ...

Negative constant

yogaje tatkṣaṇāt śddhe
guṇāpti sto voyogaje
dhana bhājyod bhave tad vad
bhavetāṁ ṛṇa bhājayo

The values of x and y obtained by reducing the results of kuṭṭaka with positive constant, should be subtracted from the divisor and dividend respectively for the solution of kuṭṭaka with negative constant.

If the solution of the equation $ax + c = by$ is $x = \alpha, y = \beta$, then the solution of the equation $ax - c = by$ is $x = b - \alpha, y = a - \beta$

Negative dividend

Similarly if the dividend is negative, the result obtained with positive dividend should be subtracted from dividend and divisor to get the results.

Similarly, for the equation $-ax + c = by$, the solution will be $x = b - \alpha, y = \beta - a$, where $x = \alpha, y = \beta$ is the solution for $ax + c = by$.

Example

The possible solutions of $60x+3 = 13y$ are (-2,-9), (11,51), ...
Or in general, $x = 13n-2$, and $y = 60n-9$.

What is the solution of $60x-3=13y$?

Since the constant is negative, the solution will be
$x = 13-11 = 2$, and $y = 60 - 51 = 9$
In general the solution will be
$x = 13n+2$ and $y = 60n+9$.
The solutions are: (2,9), (15,69),...

What is the solution of $-60x+3=13y$?

Since the dividend is negative, the solution will be
$x= 13-11 = 2$, and $y = -(60 - 51) = -9$

What is the solution of $-60x-3=13y$?
Since the constant is negative, the solution will be
$x = 13-2 = 11$, and $y = -60 -(-9) = -51$

Reduction factors

bhavati kuṭṭvidheḥ yuti bhājyayoḥ
samapavartitayorapi vā guṇaḥ
bhavati yo yuti bhājakayoḥ punaḥ
sa ca bhavet apavartana saṁguṇaḥ

If the constant and dividend of the kuṭṭaka are simplified by dividing with a common factor the value of the guṇa (x) obtained as solution of simplified kuṭṭaka will be correct but that of the labdhi(y) should be corrected by multipying with the reduction factor to give the solution of the original kuṭṭaka.

Similarly, if the constant term and divisor are reduced by dividing with a common reduction factor, the solution of the simplified kuṭṭaka will give the correct value of labdhi (y), but the guṇa (x) should be multiplied by the reduction factor to get the solution of the original kuṭṭaka.

Reduction factor: explanation

For example, consider the equation $ax + c = by$.
If a and c have a common factor, say, k.
Let $\frac{a}{k} = a_1$ and $\frac{c}{k} = c_1$.
Reduced kuṭṭaka is $a_1x + c_1 = by$.
Let the solution of this be (α, β).
Then the solution of $ax + c = by$ will be $(\alpha, k * \beta)$

Similarly, If b and c have a common factor, say, k.

Let $\frac{b}{k} = a_1$ and $\frac{c}{k} = c_1$.
Reduced kuṭṭaka is $ax + c_1 = b_1 y$.
Let the solution of this be (α, β).
Then the solution of $ax + c = by$ will be $(k * \alpha, \beta)$

Another Example

yad guṇā kṣayaga ṣṣṭiravintā
varjitā ca yadi vā trībhi tataḥ
syāt trayodaśa hṛtā niragrakā
tam guṇam gaṇaka me pṛthak vada

Which number when multiplied by -60 and increased or decreased by 3 is divisible without remainder by 13. O, mathematician, please tell me the number.

The given equations are
$-60x + 3 = 13 y$
and $-60x - 3 = 13y$.

The dividend and the constant can be reduced by dividing by 3.
The redced equations are
$-20x + 1 = 13y$, and
$-20x - 1 = 13y$

Reduction factors

Let us solve $20x + 1 = 13y$

Dividend	Divisor	Quotient	Remainder
20	13	1	7
13	7	1	6
7	6	1	1

Place the quotients, constant and zero in a column.

1	1	$(1*2+1) = 3$
1	1	$(1*1+1) = 2$
1	1	$(1*1+0) = 1$
1	1	1
0	0	-

$y = 3$ and $x = 2$

Example ... Contd

Since the number of quotients is odd,
x = 13 - 2 = 11
y = 20 -3 = 17
So the solution for $20x + 1 = 13y$ is (11,17).

The solution for $-20x + 1 = 13y$, will be
x = 13-11 = 2, and y = -(20-17) = -3

Solution for $-60x + 3 = 13y$ will be
x = 2, y = 3 * -3 = -9
Solution for $-60x - 3 = 13y$ will be
x = 13-2 = 11 and y = -(60-(-9)) = -51

An example

śatam hatam yena yutam navatyā
vivarjitam vā vihṛtam triṣaṣṭyā
niragrakam syād vaxa me guṇam tam
spṣṭaṁ paḍīyān yadi kuṭṭake asi

Which number when multiplied with 100 and increased or reduced by 90 can be divided by 63 without remainder. If you are an expert in kuṭṭaka, please tell me that number.

The equation is: $100x + 90 = 63y$
Reduce the dividend by 10 and divisor by 9
So the reduced equation is:
$10x + 1 = 7y$

Dividend	Divisor	Quotient	Remainder
10	7	1	3
7	3	2	1

Solution ... contd

Place the quotients, constant and zero in a column.

1	(1*2+1) = 3
2	(2*1+0) = 2
1	1
0	-

So the solution of $10x + 1 = 7y$ is (x,y) = (2,3).

The solution of $100x + 90 = 63y$ will be

x = 2*9 = 18; y = 3*10 = 30

So the general solution is (63n + 18, 100n + 30)

Example ... Contd

Solution of $100x - 90 = 63y$ will be
x = 63 - 18 = 45, and
y = 100 - 30 = 70
So the general solution is (63n+45, 100n+70)

Example

aṣṭādaśa guṇāḥ kena daśāḍhyā vā daśonitāḥ
śuddhaṃ bhāgaṁ prayacchanti kṣyagaikādaśoddhṛtāḥ

Which number when multiplied by 18 and increased or reduced by 10 becomes completely divisible by -11?

The equations are $18x + 10 = -11y$ & $18x - 10 = -11y$
Let us start with $18x + 10 = 11y$

Example ... Contd

Let us start with $18x + 10 = 11y$

Dividend	Divisor	Quotient	Remainder
18	11	1	7
11	7	1	4
7	4	1	3
4	3	1	1

Place the quotients, constant and zero in a column.

1	1*30+20 = 50
1	1*20+10 = 30
1	(1*10+10) = 20
1	(1*10+0) = 10
10	10
0	-

Since there are even number of quotients,

y = 50 mod 18 = 14

x = 30 mod 11 = 8

So the solution for $18x + 10 = 11y$ is (8,14)

Solution for $18x + 10 = -11y$ is (8,-14)

Solution for $18x - 10 = -11y$ is

x = -11-8 = -19 and y = 18-(-14) = 32

Constant larger than divisor

harataṣṭe dhanakṣepa guṇa labdhitu pūrvavt
kṣepa takṣaṇa lābhādyā labdhiḥ śddhau tu varjitā

If the constant c is positive, and $c > b$, the constant c can be reduced by dividing it by b and using the remainder c_1 as the new constant.
Suppose the solution of the new equation $ax + c_1 = by$ is (x_1,y_1), then the solution of $ax + c = by$ will be $(x_1,y_1 + m)$, where $m = \frac{c}{b}$.
If the constant is negative, the solution will be $(x_1,\ y_1 - m)$.

Constant larger than divisor

athavā bhāhāreṇa taṣṭayoḥ kṣepabhājyayoḥ
guṇaḥA prāgvat tato labdhiḥ bhājyāddhata yutoddhṛtāt

An alternative method is: Divide both dividend and constant by the divisor and simplify. The value of x will be correct. To get the value of y, multiply x by a and add c, divide the result by b.

Example

yena samgunnṇitāḥ pañca trayooviṁśati saẏutāḥ
varjitā vā tribhiḥ bhaktā niragrāḥ syuḥ saḥ ko guṇāḥ

Which number when multiplied by 5 and increased or reduced by 23 and divided by 3 leaves no remainder?

The equation is $5x + 23 = 3y$
The constant (23) is larger than the divisor(3). So divide the constant 23 by 3, and take the remainder as new constant.
So the new equation is $5x + 2 = 3y$

Dividend	Divisor	Quotient	Remainder
5	3	1	2
3	2	1	1

the quotients written in a column with constant and 0

1	(1*2+2) = 4
1	(1*2+0) = 2
2	2
0	-

The number of quotients is even.

So y = 4, x = 2

The solution of $5x + 23 = 3y$ is (2,4+7), where 7 = 23 div 3

General solution is (2+3n, 11+5n).

The solution of $5x - 23 = 3y$ is

x = 3 - 2 = 1, y = 5 - 11 = -6

So the general solution is (1+3n, -6+5n)

Constant is Zero

kṣepābhāve athavā yatra kṣepaḥ śudheyd haroxdhṛtaḥ
j neyaḥ śūnyaṁ guṇaḥ tatra kṣepo harahṛtaḥ phalaṁ

In the absence of numerical constant in the equation or when the constant is completely divisible by the divisor, the value of x will be zero and the constant divided by the divisor will be the value of y.
In $ax + c = by$, if $c = 0$, $ax = by$
$\rightarrow x = 0$ (and $y = 0$) is the solution

If c is an integral multiple of b, (c=bn), then the general solution is $y = n$ (and $x = 0$).

An Example

yena pa nca guṇitaḥ kha saṁyutāḥ
pa nca ṣaṣṭi sahitāḥ ca te athavā
syuḥ trayodaśa hṛtā niragrakā
tam guṇaṁ gaṇaka kīrtayāśu me

Which number, multiplied by 5 and combined with zero or increased by 65 is divisible by 13 without remainder? O Mathematician, please give me that number quickly.

The equation is $5x + 0 = 13y$ and $5x + 65 = 13y$

An Example ... Contd

The equation is $5x + 0 = 13y$
When the constant is zero, $(x, y) = (0, 0)$ is the solution
Hence general solution is:
x = 13m, y = 5m, m = 1,2,3,...

The equation is $5x + 65 = 13y$
13 is the common factor.

So the solution is:
$x = 0, y = \frac{65}{13} = 5$

General Solution is:
x = 13m, y = 5m + 5, m =1,2,3,..

sthira (invariant) kuṭṭaka

kṣepam viśuddhiṁ parikalpya rūpaṁ
pṛthak tayoḥ ye guṇakāra labdhi
abhīpsita kṣepa viśuddhi nighne
sva hāra taṣṭe bhavataḥ tayoḥ te

In a kuṭṭaka assuming constant c to be equal to 1, find the value of x and y. For an equation with the constant having the desired value (say c), multiply the values of x and y by this desired number. Reduce the results by dividing by b and a respectively and get the remainders as the values of x and y.

Sthira kuṭṭaka: Example

The solution for $8x + 1 = 3y$ is $(x, y) = (1, 3)$.

The solution for $8x + 2 = 3y$ will be $(x, y) = (1 * 2, 3 * 2) = (2, 6)$

Sthira kuṭṭaka:Proof

Let the solution for $ax + 1 = by$ be $(x, y) = (\alpha, \beta)$.

Multiply this equation throughout by c.
We get $acx + c = bcy$.
Let $cx = x_1$ and $cy = y_1$.

So we get $ax_1 + c = by_1$,
where $(x_1, y_1) = (cx, yx) = (c * \alpha, c * \beta)$.

Finding the smallest positive solution

guṇaḥ labdhyoḥ samam grāhyaṁ
dhīmatā takṣaṇe phalaṁ

While reducing the values of guṇa (x) and labdhi (y), by dividing with divisor, and dividend, an intelligent person should take the value of quotients to be equal. The values of y and x will be the remainders of such division.

This follows from the fact that the general solution is $(x + bn, y + an)$.

An Example

The solution of $8x + 1 = 3y$ is $(x, y) = (1, 3)$.

Hence the solution of $8x + 11 = 3y$ would be $(x, y) = (11, 33)$.

To get the smallest solution, divide x and y by a 3 and 8 respectively, such that the quotient is same. Thus we get

$11/3 = 3 + 2/3; 33/8 = 3 + 9/8$.
So the above solution may be reduced to (2,9), as the smallest positive solution.

Mixed Kuttaka saṁśliṣṭa kuṭṭaka

eko haraḥ ced guṇakau vibhinnau
tadā guṇaikyaṃ parikalpya bhājyaṁ
agraikyamagram kṛta uktavadyaḥ
saṁśliṣṭa samj naḥ sputakuṭṭakaḥ asau

In two kuṭṭakas, with common divisor, but different dividend and constants, the kuṭṭaka formed with the sum of dividends as new dividend and sum of constants as a new constant with the same divisor is called a mixed or conjunct kuṭṭaka.

For example, if $a_1 x + c_1 = by$ and $a_2 x + c_2 = by$ are two kuṭṭakas, then
$(a_1 + a_2)x + (c_1 + c_2) = by$ is called the saṁśliṣṭa kuṭṭaka.

Example

kaḥ pa ncanighno vihṛtaḥ triṣaṣṭyā
sapta-avaśeṣaḥ atha saḥ eva rāśiḥ
daśāhataḥ syād vihṛtaḥ triṣaṣṭyā
caturdaśa agraḥ vada rāśimena

What is the number which when multiplied by 5 and divided by 63 leaves a remainder 7? and when multiplied by 10 and divided by 63 gives 14 as remainder? Please tell me the number.

The two equations are
$5x - 7 = 63y$ and
$10x - 14 = 63y$.

So the mixed kuṭṭaka is $15x - 21 = 63y$.
On reduction, we get $5x - 7 = 21y$.

Example ... Contd

Solution of $5x + 7 = 21y$ is
$(x, y) = (28, 7) or (28 mod 21, 7 mod 5) = (7, 2)$.
Solution of $5x - 7 = 21y$ will be $(x, y) = (21 - 7, 5 - 2) = (14, 3)$
Hence $x = 14$ is the solution.

Quick Recap

Aryabhaṭa's Algorithm for solving Linear Diophantine Equations

- Reduce the given equation to a simplified form removing the common factors(GCD).
- Get the quotient of division of dividend and divisor. Repeat the process with the divisor and the remainder till the remainder is 1.
- Prepare a valli of quotients followed by the constant and 0.
- multiply the penultimate term with the factor above and add the next term. Expunge the last term and repeat this process till you have only 2 values in the column.
- If the number of quotients are even, these are the values of y and x modulo b and a respectively, if ax+c=by were the equation.
- If the number of quotients are odd, then subtract these values from b and a respectively.

Quick Recap .. Contd

- If the solution of $ax + c = by$ is (α,β) then the solution of $ax - c = by$ is $(b - \alpha,a - \beta)$
- If the solution of $ax + c = by$ is (α,β) then the solution of $-ax + c = by$ is $(-\alpha,\beta)$, and the solution of $ax + c = -by$ is $(\alpha,-\beta)$.
- If in $ax + c = by$, $c > b$, and let $c = bm + c_1$, and let the solution of $ax + c_1 = by$ be (α,β) then the solution of $ax + c = by$ is $(\alpha,\beta + m)$.
- if $a = \frac{a_1}{k}$ and $c = \frac{c_1}{k}$, and the solution of $a_1x - c_1 = by$ is (α,β), then the solution of $ax - c = by$ is $(\alpha,k * \beta)$.
- if $b = \frac{b_1}{k}$ and $c = \frac{c_1}{k}$, and the solution of $ax - c_1 = b_1y$ is (α,β), then the solution of $ax - c = by$ is $(k * \alpha,\beta)$.
- If the solution of $ax + 1 = by$ is (α, β), then the solution of $ax + c = by$ is $(c * \alpha, c * \beta)$.

Proofs

If the solution of $ax + c = by$ is (α,β)
then show that the solution of $ax - c = by$ is $(b - \alpha, a - \beta)$

Proof: (α,β) is the solution of $ax + c = by$.
Hence $a\alpha + c = b\beta$.

Subtracting each side from ab,
$ab - a\alpha - c = ab - b\beta$
$a(b - \alpha) - c = b(a - \beta)$
Hence the solution of $ax - c = by$ is $(b - \alpha, a - \beta)$

Exercise

- If (α,β) is the solution of $ax + c = by$ prove that the solution of $-ax + c = by$ is $(-\alpha,\beta)$, and the solution of $ax + c = -by$ is $(\alpha,-\beta)$.
- If in $ax + c = by$, $c > b$, and let $c = bm + c_1$, and let the solution of $ax + c_1 = by$ be (α,β) then prove that the solution of $ax + c = by$ is $(\alpha,\beta + m)$.
- if $a = \frac{a_1}{k}$ and $c = \frac{c_1}{k}$, and the solution of $a_1 x - c_1 = by$ is (α,β), then prove that the solution of $ax - c = by$ is $(\alpha,k * \beta)$.
- if $b = \frac{b_1}{k}$ and $c = \frac{c_1}{k}$, and the solution of $ax - c_1 = b_1 y$ is (α,β), then prove that the solution of $ax - c = by$ is $(k * \alpha,\beta)$.

Simple equation

Do you need a kuṭṭaka method to solve

$$ax + c = y\ ?$$

Intuition behind the Kuṭṭaka

Example: $20x + 1 = 13y$

Let $y = \frac{20x+1}{13} = x + \frac{7x+1}{13}$
For an integer solution of (x,y), $\frac{7x+1}{13}$ need to be an integer.

Let $z = \frac{7x+1}{13}$
So $x = \frac{13z-1}{7} = z + \frac{6z-1}{7}$
For an integer solution of (x,z), $\frac{6z-1}{7}$ need to be an integer.

Let $u = \frac{6z-1}{7}$
So $z = \frac{7u+1}{6} = u + \frac{u+1}{6}$
For an integer solution of (z,u), $\frac{u+1}{6}$ need to be an integer.

Let $t = \frac{u+1}{6}$
i.e., $6t = u + 1$, whose integer solutions are
$(t, u) = (n, 6n - 1), n = 1, 2, 3, ...$

Intuition behind the Kuṭṭaka .. Contd

Let us start with $t = 1$.
$u = 6t - 1$. Hence $u = 5$.
$z = u + t$. Hence $z = 5 + 1 = 6$.
$x = z + u$. Hence $z = 6 + 5 = 11$.
$y = x + z$. Hence $y = 11 + 6 = 17$.

Hence the solution is (11,17).

Kuṭṭaka: Continued Fractions

The above solution may be represented as follows.

Example: $20x + 1 = 13y$

$$\frac{20}{13} = 1 + \frac{7}{13}$$

$$\frac{20}{13} = 1 + \frac{1}{\frac{13}{7}}$$

$$\frac{20}{13} = 1 + \frac{1}{1+\frac{6}{7}}$$

$$\frac{20}{13} = 1 + \frac{1}{1+\frac{1}{\frac{7}{6}}}$$

$$\frac{20}{13} = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{6}}}$$