Linear Diophantine Equations

By Frederick Dooe

Number Theory
Boston University, summer '09
Instructor – Kalin Kostadinov

I. Introduction

Diophantine equations are named for Diophantus of Alexandria who lived in the third century. He however was not the first to study this subject. Indian mathematicians such as Baudhayana and Apastamba studied Diophantine equations as far back as c. 800-600 b.c.e.. Later, in the Middle Ages, Indian mathematicians became the first to systematically explore ways of finding integral solutions of Diophantine Equations (1). These methods could be found in Indian mathematical texts dating as far back as 499AD. In Europe in the seventeenth century, Fermat made a study of Diophantine equations, and conjectured that x^n+y^n = z^n has no solutions for n greater than two. This conjecture, know as Fermat's Last Theorem, remained as such until in 1994 it was proved by Andrew Wiles. (1) Most of what is known about the laws of Diophantine equations has been discovered in the twentieth century.

II. Linear Diophantine Equations

1. Diophantine Equations are equations with integral coefficients. Linear Diophantine equations are simply linear equations with integral coefficients, and are the simplest type of Diophantine equations. A linear Diophantine equation in two variables is a Diophantine equation of the form ax + by = c (2)
2. An example of such an equation follows (from 2)

   "Twenty-three weary travelers entered the outskirts of a lush and beautiful forest. They fond 63 equal heaps of plantains and seven single fruits, and divided them equally." (2, pg. 189-190)

   Let x be the number of plantains in a heap, and y be the number of plantains received by a traveler. This produces the LDE

   $$63x + 7 = 23y$$

   x and y must be positive. Solving for y,

   $y = (63x + 7) / 23$

   x = 5, and y = 14 is one solution. And in fact, there are an infinite number of solutions. (2)
3. Hundred Fowls Puzzle (from 2, pg 190):

If a rooster is worth 5 coins, a hen is worth 3 coins, and three chicks together are worth one coin, how many birds totaling 100 and be bought for 100 coins.

This data gives 2 equations. Let x = number of roosters, y = number of hens, and z = the number of chicks

$$x + y + z = 100$$

$5x + 3y + z/3 = 100$

from the first equation, $z = 100 – x – y$, and substituting this into the second equation, we get
$5x + 3y + (1/3)(100-x-y) = 100$
This simplifies to
$7x + 4y = 100$
solving for y we get
$y = 25 – (7/4)x$
This implies that for y to be an integer, x must be a multiple of 4. Letting $x = 4t$, where t is an integer, we find
$y = 25 – 7t$ and $z = 75 + 3t$
Since x is greater than or equal to zero, t is greater than or equal to zero. Since y is greater than or equal to zero, $25 – 7t$ is greater than or equal to zero. This implies that t is less than 25/7; therefore, t is less than or equal to 3. so t is greater than or equal to zero and less than or equal to three. This gives 4 solutions – one for each possible value of t (0, 1, 2, or 3) which are,
$x = 0, y = 25, z = 75$
$x = 4, y = 18, z = 78$
$x = 8, y = 11, z = 81$
$x = 12, y = 4, z = 84$

4. Not every linear Diophantine equation has a solution

For example (pg. 192, 2): $2x + 4y = 5$ has no solution, since $2x + 4y$ will always be even and 5 is odd

A LDE of the form $ax + by = c$ is solvable iff d (= gcd(a,b)) divides c, and if x', y' is a solution, then all of the LDE's solutions are given by $x = x' + (b/d)t$ and $y = y' – (a/d)t$
Proof: (from 2, pg. 193)
Given a LDE $ax + by = c$ with a solution
$d = (a,b)$, so d divides a and b. Thus d divides $(ax + by)$ which = c, so d divides c.
Suppose d divides c, then $c = de$ for some integer e. since $d = (a,b)$, there exist integers s.t. $ra + sb = d$ (d is a linear combination of a and b)*
Multiplying both sides by e, we get $rae + sbe = de$, which implies $a(re) + b(se) = c$.
Thus $ax + by = c$ has solutions $x' = re$ and $y' = se$
Therefore the LDE is solvable.
To show $x = x' + (b/d)t$ and $y = y' – (a/d)t$ is a solution, we substitute into the LDE for x and y to get
$ax + by = a(x' + (b/d)t) + b(y' – (a/d)t)$
$= (ax' + by') + (abt/d) – (abt/d)$
$=ax' + by'$

To show every solution x'', y'' is of the desired form:

Since x', y' and x'', y'' are solutions of the LDE,

ax' + by' = c and ax'' + by'' = c

ax' + by' = ax'' + by''

Therefore, a(x'' – x') = b(y' – y'')

Dividing both sides by d,

(a/d)(x'' – x') = (b/d)(y' – y'')

gcd((a/d), (b/d)) = 1

so, b/d divides (x'' – x')

hence x'' – x' = (b/d)t

x'' = x' + (b/d)t

and substituting for (x'' – x')

a(b/d)t = b(y' – y'')

(a/d)t = y' – y''

y'' = y' – (a/d)t

It follows from this theorem that if the LDE ax + by = c has a solution, it has infinitely many solutions

5. The Monkey and Coconuts Puzzle (2, pgs. 197, 226)

Five sailors and a monkey are marooned on a desert island. They spend the day gathering coconuts for food and decide to divide them up in the morning. During the night, one sailor wakes up and decides to divide them himself. He breaks the pile into five equal piles and gives the one remaining coconut to the monkey. He puts four of the piles back together and returns to his sleeping place with his pile. One by one, each of the sailors repeat this process through the course of the night. In the morning, they divide the remaining pile into five portions and give the remaining coconut to the monkey. Let n be the initial number of coconuts, and let u, v, w, x, and y be the numbers of coconuts each sailor took, and let z be the minimum portion received by each from the remaining pile in the morning. This leads to equations:

n = 5u + 1

4u = 5v + 1

4v = 5w + 1

4w = 5x + 1

4x = 5y + 1

4y = 5z + 1

These equations lead to the LDE 15625z – 1024n = -11529, which can be solved by the Euclidean algorithm:

15625 = 15*1024 + 265

1024 = 3*265 + 229

265 = 1*229 + 36

229 = 6*36 + 13

36 = 2*13 + 10
13 = 1*10 + 3
10 = 3*3 + 1
3 = 3*1

1=
= 10 – (3*3)
= 10 – 3*(13-10)
= 4*10 – 3*13
= 4*(36 – 2*13) – 3*13
= 4*36 -11*13
= 4*36 – 11*(229- 6*36)
= 70*36 – 11*229
= 70*(265 – 229) – 11*229
= 70*265 - 81*229
= 70*265 – 81*(1024 – 3*265)
= 313*265 – 81*1024
= 313*(15625 – 15*1024) – 81*1024
1 = 313*15625 – 4776*1024

multiplying by -11529, we get

313*15625*-11529 – 4476*1024*-11529 = -11529, so
15625*(-3608577) – 1024*(-55062504) = -11529

so all of the solutions of the equation are given by
z = -3698577 -1024t and n = -55062504 – 15625t;
n > 0, so -55062504 – 1024t > 0. Thus, t < -55062504/15625, i.e. t< -3524. Because of the equation for n, n is a minimum when t is a maximum,

or alternatively by using congruencies, we find

z = 1/5(4/5(4/5(4/5(4/5(4/5 * (n-1) – 1) -1) -1) -1) -1)

this can be rewritten as n(4/5)^5 – (1+ 4/5 +(4/5)^2 + (4/5)^3 + (4/5)^4 + *4/5)^5) = 5z

= n*(4/5)^5 – (1-(4/5)^6)/(1-4/5)

= n*(4/5)^5 – (5^6 – 4^6)/5^5

5^6 * z= 4^5 * n + 4^6 – 5^6

= (n+4)*4^5 = (Z+1)*5^6

Which is congruent to 0 (mod 5)
But (4^5, 5^6) = 1, so n+4 is congruent to 0 (mod 5). N is a minimum when n+4 = 5^6 = 15625; n = 15621

* The gcd of the positive integers a and b is a linear combination of a and b.

Proof: (2, pg. 159)

Let S be the set pf positive linear combinations of a and b; that is s = {ma + nb s.t. ma + nb > 0, m, n in Z}

To Show that S has a least element:

Since a > 0, a = 1*a + 0*b is in S, so S is nonempty. So, by the well-ordering principal, S has a least positive element d.

To Show that d = (a,b)

Since d belongs to S, d = a'a + b'b for some a' and b'

By the divison algorithm, there exist integers q and r such that a =dq + r, where r is greater than or equal to 0 and less than or equal to d. Substituting for d,

r = a – dq

= a – (a'a + b'b)q

= (1-a'q)a + (-b'q)b, so r is a linear combination of a and b. If r > 0 then r is an element of S. Since r<d, r is the smallest element in S, which is a contradiction. So r = 0; thus a = dq, so d divides a. Similarly, d divides b. Thus d is a common divisor of a and b.

To show that any positive common divisor d' of a and b is less than or equal to d:

Since d' divides a and d' divides b, d' divides (a'a + b'b); that is d' divides d, so d' is less than or equal to d

(This is similar to the proof of Bézout's identity, which states that given nonzero integers a and b whose gcd is d, then there exists integers x and y s.t. ax + by = d

6. Applications
    a. Gaussian Integers
    1. A Gaussian Integer is a complex number of the form a + bi, where a and b are integers
    2. two Gaussian integers are considered prime if their gcd is 1, -1, i, or –i, which is to say that their gcd divides one.
    3. Euclid's Algorithm with Gaussian integers
       To divide a by b in Gaussian integers, one looks for r and q s.t.

       a = bq + r, Norm(r) < Norm(b)

       In the complex numbers, positive and negative are not meaningful concepts, so the norms of two numbers are

used as a substitute concept. The Euclidean algorithm is applied in a similar way to the integers.

b. Fibonacci Numbers and LDE's (from 2, pg. 201)
Consider the LDE $F_{n+1}x + F_n y = c$. Since any two consecutive Fibonacci numbers are prime, $\gcd(F_{n+1}, F_n) = 1$ and the LDE has a solution

By Cassini's formula, $F_{n+1} F_{n-1} - F_n^2 = (-1)^n$

Suppose n is even,
Then $F_{n+1} F_{n-1} - F_n^2 = 1$;
So, $F_{n+1} (cF_{n-1}) - F_n(-cF_n) = c$
Thus, $x' = c F_{n-1}$, $y' = -c F_n$ is a particular solution of the LDE $F_{n+1}x + F_n y = c$.

Suppose n is odd,
Then $F_{n+1} F_{n-1} - F_n^2 = -1$ which implies
$F_{n+1}(-1*F_{n-1}) + F_n^2 = 1$
So, $F_{n+1}(-cF_{n-1}) + F_n(c F_n) = c$.
Thus $x' = -c F_{n-1}$, $y' = cF_n$ is a particular solution of the LDE $F_{n+1}x + F_n y = c$

For example, consider the LDE $34x + 21y = 17$.
Since $F_9F_7 - F_8^2 = 34*13 - 21^2 = (-1)^8$ and $c = 17$
It follows that $x' = cF_7 = 17*13 = 221$, $y' = -cF_8 = -17*21 = -357$ is a particular solution.

So the general solution is $x = x' + bt = 221 + 21t$, $y = y' - at = 357 - 34t$

7. Bibliography

1. www.wikipedia.com
2. Koshy, Thomas. Elementary Number Theory with Applications. Second edition. Burlington, MA: Elsevier, 2007
3. http://mathforum.org/library/drmath/view/62690.html