**forthright48**
learning never ends

# Linear Diophantine Equation


forthright48 on July 27, 2015

## Problem

Given the value of integers $A, B$ and $C$ find a pair of integers $(x, y)$ such that it satisfies the equation $Ax + By = C$.

For example, if $A = 2, B = 3$ and $C = 7$, then possible solution of $(x, y)$ for equation $2x + 3y = 7$ would be $(2, 1)$ or $(5, -1)$.

The problem above is a type of Diophantine problem. In the Diophantine problem, only integer solutions to an equation are required. Since $Ax + By = C$ is a linear equation, this problem is a **Linear Diophantine Problem** where we have to find a solution for a **Linear Diophantine Equation**.

For now, let us assume that $A$ and $B$ are non-zero integers.

## Existence of Solution

Before we jump in to find the solution for the equation, we need to determine whether it even has a solution. For example, is there any solution for $2x + 2y = 3$? On the left side we have $2x + 2y$

is odd. This equation is impossible to satisfy using integer values.

So how do we determine if the equation has a solution? Suppose $g = gcd(A, B)$. Then $Ax + By$ is a multiple of $g$. In order to have a valid solution, since left side of the equation is divisible by $g$, the right side too must be divisible by $g$. Therefore, if $g \not| C$, then there is no solution.

# Simplifying the Equation

Since both side of equation is divisible by $g$, i.e, $g \mid (Ax + By), C$ , we can safely divide both side by $g$ resulting in a equivalent equation.

Let $a = \frac{A}{g}$, $b = \frac{B}{g}$ and $c = \frac{C}{g}$. Then,

$$(Ax + By = C) \equiv (ax + by = c)$$

After simplification, $gcd(a, b)$ is either $1$ or $-1$. If it is $-1$, then we need multiply $-1$ with $a, b$ and $c$ so that $gcd(a, b)$ becomes $1$ and the equation remains unchanged. Why did we make the $gcd(a, b)$ positive? You will find the reason below.

# Using Extended Euclidean Algorithm

Recall that in a previous post "Extended Euclidean Algorithm", we learned how to solve the Bezout's Identity $Ax + By = gcd(A, B)$. Can we apply that here in any way?

Yes. Using `ext_gcd()` function, we can find Bezout's coefficient for $ax + by = gcd(a, b)$. But we need to find solution for $ax + by = c$. Note that $gcd(a, b) = 1$, so when we use `ext_gcd()` we find a solution for $ax + by = 1$. Let this solution be $(x_1, y_1)$. We can extend this solution to solve our original problem.

Since we already have a solution where $ax_1 + by_1 = 1$, multiplying both sides with $c$ gives us $a(x_1c) + b(y_1c) = c$. So our result is $(x, y) = (x_1c, y_1c)$. This is why we had to make sure that $gcd(a, b)$ was $1$ and not $-1$. Otherwise, multiplying $c$ would have resulted $ax + by = -c$ instead.

# Summary of Solution

Here is a quick summary of what I described above. We can find solution for Linear Diophantine Equation $Ax + By = C$ in 3 steps:

1. **No Solution**: First check if solution exists for given equation. Let $g = gcd(A, B)$. If $g \not| C$

then no solution exists.

2. **Simplify Equation**: Let $a = \frac{A}{g}, b = \frac{B}{g}$ and $c = \frac{C}{g}$. Then finding solution for $Ax + By = C$ is same as finding solution for $ax + by = c$. In simplified equation, make sure $GCD(a, b)$ is $1$. If not, multiply $-1$ with $a, b, c$.
3. **Extended Euclidean Algorithm**: Use `ext_gcd()` to find solution $(x_1, y_1)$ for $ax + by = 1$. Then multiply the solution with $c$ to get solution for $ax + by = c$, where $x = x_1 \times c, y = y_1 \times c$.

Let us try few examples.

## Example 1: $2x + 3y = 7$

**Step** $1$**:** $g = GCD(2, 3) = 1$. Since $1$ divides $7$, solution exists.
**Step** $2$**:** Since $g$ is already $1$ there is nothing to simplify.
**Step** $3$**:** Using `ext_gcd()` we get $(x, y) = (-1, 1)$. But this is for $ax + by = 1$. We need to multiply $7$. So our solution is $(-7, 7)$.

$2 \times -7 + 3 \times 7 = -14 + 21 = 7$. The solution is correct.

## Example 2: $4x + 10y = 8$

**Step** $1$**:** $g = GCD(4, 10) = 2$. Since $2$ divides $8$, solution exists.
**Step** $2$**:** $a = \frac{4}{2}, b = \frac{10}{2}, c = \frac{8}{2}$. We will find solution of $2x + 5y = 4$.
**Step** $3$**:** Using `ext_gcd()` we get $(x, y) = (-2, 1)$. But this is for $ax + by = 1$. We need to multiply $4$. So our solution is $(-8, 4)$.

$ax + by = 2 \times -8 + 5 \times 4 = -16 + 20 = 4 = c$.
Also, $Ax + By = 4 \times -8 + 10 \times 4 = -32 + 40 = 8 = C$. The solution is correct. Both $ax + by = c$ and $Ax + By = C$ are satisfied.

# Finding More Solutions

We can now find a possible solution for $Ax + By = C$, but what if we want to find more? How many solutions are there? Since the solution for $Ax + By = C$ is derived from Bezout's Identity, there are infinite solutions.

Suppose we found a solution $(x, y)$ for $Ax + By = C$. Then we can find more solutions using the formula: $(x + k\frac{B}{g}, y - k\frac{A}{g})$, where $k$ is any integer.

# Code

Let us convert our idea into code.

```
1  bool linearDiophantine ( int A, int B, int C, int *x, int *y ) {
2      int g = gcd ( A, B );
3      if ( C % g != 0 ) return false; //No Solution
4
5      int a = A / g, b = B / g, c = C / g;
6      ext_gcd( a, b, x, y ); //Solve ax + by = 1
7
8      if ( g < 0 ) { //Make Sure gcd(a,b) = 1
9          a *= -1; b *= -1; c *= -1;
10     }
11
12     *x *= c; *y *= c; //ax + by = c
13     return true; //Solution Exists
14 }
15
16 int main () {
17     int x, y, A = 2, B = 3, C = 5;
18     bool res = linearDiophantine ( A, B, C, &x, &y );
19
20     if ( res == false ) printf ( "No Solution\n" );
21     else {
22         printf ( "One Possible Solution (%d %d)\n", x, y );
23
24         int g = gcd ( A, B );
25
26         int k = 1; //Use different value of k to get different solutions
27         printf ( "Another Possible Solution (%d %d)\n", x + k * ( B / g ),
28     }
29
30  return 0;
31 }
```

`linearDiophantine()` function finds a possible solution for equation $Ax + By = C$. It takes in $5$ parameters. $A, B, C$ defines the coefficients of equation and *x, *y are two pointers that will carry our solution. The function will return $true$ if solution exists and $false$ if not.

In line $2$ we calculate $gcd(A, B)$ and in line $3$ we check if $C$ is divisible by $g$ or not. If not, we return $false$.

Next on line $5$ we define $a, b, c$ for simplified equation. On line $6$ we solve for $ax + by = 1$ using `ext_gcd()`. Then we check if $g < 0$. If so, we multiply $-1$ with $a, b, c$ to make it positive. Then we multiply $c$ with $x, y$ so that our solution satisfies $ax + by = c$. A solution is found so we return true.

In $\text{main}()$ function, we call $\text{linearDiophantine}()$ using $A = 2, B = 3, C = 5$. In line $22$ we print a possible solution. In line $27$ we print another possible solution using formula for more solutions.

# $A$ and $B$ with Value $0$

Till now we assumed $A, B$ have non-zero values. What happens if they have value $0$?

## When Both $A = B = 0$

When both $A$ and $B$ are zero, the value of $Ax + By$ will always be $0$. Therefore, if $C \neq 0$ then there is no solution. Otherwise, any pair of value for $(x, y)$ will act as a solution for the equation.

## When $A$ or $B$ is $0$

Suppose only $A$ is $0$. Then equation $Ax + By = C$ becomes $0x + By = C \; \equiv \; By = C$. Therefore $y = \frac{C}{B}$. If $B$ does not divide $C$ then there is no solution. Else solution will be $(x, y) = (k, \frac{C}{B})$, where $k$ is any intger.

Using same logic, when $B$ is $0$, solution will be $(x, y) = (\frac{C}{A}, k)$.

# Coding Pitfalls

When we use $gcd(a, b)$ in our code, we mean the result from Euclidean Algorithm, not what we understand mathematically. $gcd(4, -2)$ is $-2$ according to Euclidean Algorithm whereas it is $2$ in common sense.

# Resources


1. Wiki - Diophantine Equation - https://en.wikipedia.org/wiki/Diophantine_equation
2. forthright48 - Extended Euclidean Algorithm - https://forthright48.com/2015/07/extended-euclidean-algorithm.html




**Category:** CPPS, Number Theory

**Previous:**
**Extended Euclidean Algorithm**

**Next:**
**Simple Hyperbolic Diophantine Equation**

Guest

Your comment...

5 comments

Sort by oldest

Anonymous
12 months ago

Suppose only A is 0. Then equation Ax+By=C becomes 0x+By=C≡By=C. Therefore y=C/B. If B does not divide C then there is no solution. Else solution will be (x,y)=(C/B,k), where k is any intger. Instead of this solution will be (x,y)=(k,C/B).If I m not mistaken please correct it.And similarly for when B is 0.

Reply 0

Mohammad Samiul Islam
12 months ago

You are right. It has been fixed now. Thank you :)

Reply 0

Sowmen D. Dragneel
12 months ago

When A is 0 shouldn't it be (x,y)=(k,C/B)? I think you wrote it reversed. Or did i understand wrong?

Reply 0

BIDDUT SARKER BIJOY
12 months ago

vai, when more than two variables then... what can i do?

Reply 0

Mohammad Samiul Islam
12 months ago

Yes. It has been fixed. Thank you :)

Reply 0

## Archives

September 2018 (2)

February 2018 (1)

January 2018 (1)

November 2017 (2)

September 2015 (7)

August 2015 (13)

July 2015 (15)

## Categories

CPPS (40)

- Combinatorics (3)
- Number Theory (33)

Meta (1)

## Recent Comments

forthright48 on Number of Divisors of an Integer

Sohana Akter on Number of Divisors of an Integer

forthright48 on Number of Divisors of an Integer

forthright48 on Prufer Code: Linear Representation of a Labeled Tree

Mohammad Samiul Islam on SPOJ LCMSUM – LCM Sum