COT 3100 Notes - 9/29/2020 (Linear Equation Solver)

ax + by = c, where a, b and c are given integers and we find all ordered pairs of integers (x, y), which satisfy the equation.

5x + 10y = 132, there are no solutions because 5 | (5x + 10y), but $5 \nmid 132$.

More generally, if c is NOT divisible by gcd(a, b), then there are no integer solutions, since one side has to be divisible by gcd(a, b) and the other side is not.

But what do I do if it says

5x + 10y = 135???

Extended Euclidean Algorithm

Goal: given positive integers a and b, find integers x and y such that

ax + by = gcd(a, b)

132x + 71y = 1

Goal will be to find integer x and y that satisfy the equation above.

Step 1 - run the regular Euclidean Algorithm

132 = 1 x 71 + 61
71 = 1 x 61 + 10
61 = 6 x 10 + 1, gcd = 1
10 = 10 x 1

Step 2 - write the second to last equation (last one with a non-zero remainder) backwards:

1 x 61 - 6 x10 = 1

So, currently, we are expressing the gcd, which is 1, as a linear combination of 10 and 61.

Goal is to express 1 as a linear combo of 132 and 71…

Of the two numbers in the linear combination, we want to substitute for the smaller one. (So 10 < 61, so we want to substitute for 10.) So take the previous equation and write it backwards

71 = 1 x 61 + 10 → 71 - 1 x 61 = 10

1 x 61 - 6(71 - 1 x 61) = 1

1 x 61 - 6x71 + 6 x 61 = 1

$7 \times 61 - 6 \times 71 = 1$

So now, we have expressed 1 as a linear combination of 61 and 71. (61 < 71, so we sub for 61.)

$132 = 1 \times 71 + 61 \rightarrow 132 - 1 \times 71 = 61$

$7(132 - 1 \times 71) - 6 \times 71 = 1$

$7 \times 132 - 7 \times 71 - 6 \times 71 = 1$

$7 \times 132 - 13 \times 71 = 1$

Thus, a solution to the given equation in integers is $x = 7$, $y = -13$.

Finding a Modular Inverse

Let $c = a^{-1} \bmod b$. Then, by definition $ca \equiv 1 \pmod{b}$.

Using the Extended Euclidean, we can take one extra short step and obtain a modular inverse:

Consider finding $71^{-1} \bmod 132$.

$7 \times 132 - 13 \times 71 = 1$

For an equal equation, we can take it mod any value we want:

$7 \times 132 - 13 \times 71 \equiv 1 \pmod{132}$

$7 \times 0 - 13 \times 71 \equiv 1 \pmod{132}$

$-13 \times 71 \equiv 1 \pmod{132}$

Thus, $71^{-1} \equiv -13 \equiv 119 \pmod{132}$

$71x \equiv 23 \pmod{132}$
$119(71x) \equiv (119)(23) \pmod{132}$
$x \equiv 2737$ (mod 132
$x \equiv 97 \pmod{132}$

$71x \equiv 23 \pmod{132}$
$(-13)(71x) \equiv (-13)(23) \pmod{132}$
$x \equiv -299 \pmod{132}$
$x \equiv 97 \pmod{132}$

Finding ALL solutions to ax+by = gcd(a, b), where gcd(a, b) = 1

7x132 - 13 x 71 = 1

Thus, a solution to the given equation in integers is x = 7, y = -13.

Conisder adding 71 to x and subtracting 132 from y:

132(7+71) + 71(-13-132) = 132x7 + 132x71 + 71x(-13) + 71x(-132)

= 132x7 + 71x(-13)

= 1

So basically, we can always create a new solution, by adding 71 to an old x solution while simultaneously subtracting 132 from the corresponding y solution.

So basically, if (x, y) is one solution, then (x + b, y - a) is another solution. In fact, we can add or subtract any number of copies of a and b, so we write all of our solutions as:

{ (x, y) | x = 7 + 71c, y = -13 - 132c, $c \in Z$}

The offset of using a and b works **ONLY IF GCD(a, b) = 1.**

Now, let's consider solving the equation when gcd isn't equal to 1.

Find all integer solutions to 38x + 28y = 2.

38 = 1 x 28 + 10
28 = 2 x 10 + 8
10 = 1 x 8 + 2
8 = 4 x 2

10 - 1 x 8 = 2
10 - (28 - 2 x 10) = 2
10 - 28 + 2 x 10 = 2
3 x 10 - 1 x 28 = 2
3(38 - 28) - 1 x 28 = 2
3 x 38 - 3 x 28 - 1 x 28 = 2
3 x 38 - 4 x 28 = 2

So, one solution is (3, -4).

If this is true: **3 x 38 - 4 x 28 = 2**, then 38(3 + 14) - 28(4 + 19) = 1 because
3 x 38 + **38 x 14** - 28 x 4 **- 28 x 19**
My offsets are not 28 and 38, respectively, but 14 and 19, respectively.

So, the set of all solutions is

$\{ (x, y) \mid x = 3 + 14c, y = -4 - 19c, c \in Z\}$

So in general, once we have one solution (x_0, y_0), then we can express all solutions as

$$\{ (x, y) \mid x = x_0 + \frac{b}{gcd(a,b)} c, y = y_0 - \frac{a}{gcd(a,b)}, c \in Z\}$$

<u>What do I do if c ≠ gcd(a, b), but gcd(a, b) | c?</u>

Find all integer solutions to 38x + 28y = 136.

From our old work we have:

<u>**3 x 38 - 4 x 28 = 2**</u>

Now, multiply the whole equation through by 136/2 = 68.

68(3 x 38 - 4 x 28) = 68 x 2

(68 x 3)38 - (4 x 68)28 = 136

204 x 38 - 272 x 28 = 136

38 (204 + 14) + 28(-272 -19) = 28 x 204 + 38 x 14 - 28 x 272 - 28 x 19

So, one solution is (204, -272). Thus, all solutions take the form

$\{ (x, y) \mid x = 204 + 14c, y = -272 - 19c, c \in Z\}$

So how can we express this equivalently…
Set c = -14, x = 204 + 14(-14) = 204 - 196 = 8, y = -272 -19(-14) = -272 + 266 = -6

So, another solution is (8, -6)

8 x 38 - 6 x 28 = 304 - 168 = 136, so it works!

$\{ (x, y) \mid x = 8 + 14c, y = -6 - 19c, c \in Z\}$

Two highlighted sets are the same.

Find all solutions to 255x + 104y = 13.

255 = 2 x 104 + 47
104 = 2 x 47 + 10
47 = 4 x 10 + 7
10 = 1 x 7 + 3
7 = 2 x 3 + 1

7 - 2 x 3 = 1

7 - 2(10 - 1 x 7) = 1
7 - 2 x 10 + 2 x 7 = 1
3 x 7 - 2 x 10 = 1
3(47 - 4 x 10) - 2 x 10= 1
3 x 47 - 12 x 10 - 2 x 10 = 1
3 x 47 - 14 x 10 = 1
3 x 47 - 14(104 - 2 x 47) = 1
$\underline{3 \text{ x } 47}$ - 14 x 104 + $\underline{28 \text{ x } 47}$ = 1
31 x 47 - 14 x 104 = 1
31(255 - 2 x 104) - 14 x 104 = 1
31 x 255 - 62 x 104 - 14 x 104 = 1

31 x 255 - 76 x 104 = 1

Now, multiply this equation through by 13:

13 x 31 x 255 - 13 x 76 x 104 = 13
(13 x 31) x 255 + (-13 x 76)x104 = 13
403 x 255 - 988 x 104 = 13

One solution is x = 403, y = -988, so all solutions are:

{ (x, y) | x = 403 + 104c, y = -988 - 255c, $c \in Z$}

Plug in c = -3, x = 403 + 104(-3) = 403 - 312 = 91, y = -988 -255(-3) = -988 + 765 = -223

{ (x, y) | x = 91 + 104c, y = -223 - 255c, $c \in Z$}, this is another way to express the same solution set.

Plug in c = -4, x = 403 + 104(-4) = 403 - 416 = -13, y = -988 -255(-4) = -988 + 1020 = 32

{ (x, y) | x = -13 + 104c, y = 32 - 255c, $c \in Z$}, this is another way to express the same solution set.

Fundamental Theorem of Arithmetic

Each positive integer has a unique prime factorization.

Assume to the contrary, that there is some integer that has two different prime factorizations. Let M be the smallest such integer.

$1 = 2^0 3^0 \ldots$
$2 = 2^1 3^0 ..$

$M = p^a q^b r^c \ldots = p^{a'} q^{b'} r^{c'}$, where either $a \neq a'$, or $b \neq b'$ or $c \neq c'$.

Find some prime factor of M, call it p. Since p | M, we should find a factor of p in both representations.

Take both representations and divide them by p:

$M' = p^{a-1} q^b r^c \ldots = p^{a'-1} q^{b'} r^{c'}$,

So the problem is that M' < M, but I have now shown, two different prime factorizations of M', so this contradicts the assumption that M was the smallest.

For each positive integer n, there exists a unique set of integers a_1, a_2, … such that $n = \prod_{p_i \in Primes} p_i^{a_i}$.

$288 = 2 \times 144 = 2 \times 12 \times 12 = 2 \times 2^2 \times 3 \times 2^2 \times 3 = 2^5 \times 3^2$

Let a = $\prod_{p_i \in Primes} p_i^{a_i}$, and b= $\prod_{p_i \in Primes} p_i^{b_i}$.

$A = 2^3 3^6 5^2 11$, $B = 2^5 3^4 5^7 7$, $\gcd(a, b) = 2^3 3^4 5^2$

$\gcd(a, b) = \prod_{p_i \in Primes} p_i^{min(a_i, b_i)}$.

Calculating Your Grade in a Class

Let your assignments have scores a_1, a_2, …, a_k and have percentages p_1, p_2 …, p_k, (assume assignment scores have been scaled to 100) then your current class grade is

$$\frac{\sum_{i=1}^{k} p_i a_i}{\sum_{i=1}^{k} p_i}$$