Math 3110: Summary of Linear Diophantine Equations

January 30, 2019

Goal: Given $a, b, c \in \mathbb{Z}$, to find all integer solutions (x, y) to $ax + by = c$.

The Homogeneous Case

The term *homogeneous* means the number after the $=$ is zero.

Theorem 1 (Homogeneous Case)**.** *Let $a, b \in \mathbb{Z}$. The set of integer solutions (x, y) to the equation $ax + by = 0$ is*

$$\left\{ \left(\frac{bk}{\gcd(a,b)}, \frac{-ak}{\gcd(a,b)} \right) : k \in \mathbb{Z} \right\}.$$

Proof. See Course Notes of Mon, Jan 28 (used the $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$ theorem). □

The principle of adding solutions

If

$$(x, y) \text{ is a solution to } ax + by = c,$$

and

$$(x', y') \text{ is a solution to } ax + by = c',$$

then

$$(x + x', y + y') \text{ is a solution to } ax + by = c + c'.$$

Extended GCD Replacement

Theorem 2 (Extended GCD Replacement)**.** *Let $A, B \in \mathbb{Z}$. Let $k \in \mathbb{Z}$, and write $C = A + kB$. Then*

1. $\gcd(A, B) = \gcd(B, C)$
2. *Let $a, b \in \mathbb{Z}$. Suppose $\gcd(a, b) = 1$. Suppose that $(x_A, y_A) \in \mathbb{Z}^2$ is a solution to $ax + by = A$ and (x_B, y_B) is a solution to $ax + by = B$. Then $(x_A + kx_B, y_A + ky_B)$ is a solution to $ax + by = C$.*

Proof. Item 1 is the GCD Replacement Theorem (proven in class) for A, B and $C = A + kB$. The additional statement, Item 2, is a consequence of the principle of adding solutions. □

Extended Euclidean Algorithm

The regular Euclidean Algorithm is written in regular typeface (to match your course notes), and the Extended Euclidean Algorithm includes the extra *italicized* parts.

Suppose we wish to solve $ax + by = \gcd(a, b)$. Assume $a > b > 0$.

1. Let $c_0 = a$ and $c_1 = b$.

   Also let $(x_0, y_0) = (1, 0)$ and $(x_1, y_1) = (0, 1)$.

   Note: $ax_i + by_i = c_i$ for $i = 0, 1$.

2. Let $i = 1$.

3. Then, until $c_i = 0$, repeat the following:

   (a) Use the division algorithm to write

   $$c_{i-1} = c_i q + r, \quad 0 \leq r < c_i.$$

   (b) Let $c_{i+1} = c_{i-1} - c_i q = r$.

   And let $(x_{i+1}, y_{i+1}) = (x_{i-1}, y_{i-1}) - (x_i, y_i)q$.

   Note: We now have $ax_{i+1} + by_{i+1} = c_{i+1}$, by Extended GCD Replacement.

   (c) Increment i.

4. When we are done ($c_i = 0$), we have $c_{i-1} = \gcd(a, b)$.

   But also, (x_{i-1}, y_{i-1}) is a solution to $ax + by = c_{i-1} = \gcd(a, b)$.

Example

The example below illustrates the process for solving $24x + 17y = 1$.

1. Computing the $gcd(24, 17)$ using the Euclidean algorithm:

$$\begin{aligned} 24 &= 1 \cdot 17 + 7 \\ 17 &= 2 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

2. The corresponding Extended Euclidean Algorithm:

   Notation: The card

(x, y) gives c

   tells you that the linear combination $24x + 17y = c$.

$(1, 0)$ gives 24	$= 1 \cdot$	$(0, 1)$ gives 17	$+$	$(1, -1)$ gives 7
$(0, 1)$ gives 17	$= 2 \cdot$	$(1, -1)$ gives 7	$+$	$(-2, 3)$ gives 3
$(1, -1)$ gives 7	$= 2 \cdot$	$(-2, 3)$ gives 3	$+$	$(5, -7)$ gives 1
$(-2, 3)$ gives 3	$= 3 \cdot$	$(5, -7)$ gives 1	$+$	$(-17, 24)$ gives 0

Now, simply observe that the second to last card on the right column reads out the needed solution: $24(5) + 17(-7) = 1$. Doing the algorithm to the bitter end (the card $24(-17) + 17(24) = 0$) is a way to check your work.

Existence of Solutions

Theorem 3 (Existence of Solutions)**.** *Let $a, b, c \in \mathbb{Z}$. The equation $ax + by = c$ has integer solutions if and only if $\gcd(a, b) \mid c$. If there is a solution, it can be found using the Extended Euclidean Algorithm.*

Proof. Suppose that $ax+by = c$ has an integer solution (x, y). Then $\gcd(a, b) \mid ax$ and $\gcd(a, b) \mid by$, so that $\gcd(a, b) \mid c$.

Now suppose $\gcd(a, b) \mid c$. The Extended Euclidean Algorithm guarantees a solution (x, y) to $ax+by = \gcd(a, b)$ (this follows from the description of the algorithm). Then, writing $c = k \gcd(a, b)$, then (kx, ky) is a solution to $ax + by = c$. □

One Gives All

Theorem 4 (One Gives All Theorem)**.** *Let $a, b, c \in \mathbb{Z}$. Suppose that (x_0, y_0) is one integer solution to $ax + by = \gcd(a, b)$. Then the set of all integer solutions to the equation $ax + by = c \gcd(a, b)$ is*

$$S = \left\{ \left(cx_0 + \frac{bk}{\gcd(a,b)}, cy_0 + \frac{-ak}{\gcd(a,b)} \right) : k \in \mathbb{Z} \right\}.$$

Proof. **Everything in S is a solution:** Since $ax_0 + by_0 = \gcd(a, b)$, we have $a(cx_0) + b(cy_0) = c \gcd(a, b)$. Therefore (cx_0, cy_0) is an integer solution to $ax + by = c \gcd(a, b)$. By the theorem governing the homogeneous case, the entire family of integer solutions to $ax + by = 0$ is

$$\left\{ \left(\frac{bk}{\gcd(a,b)}, \frac{-ak}{\gcd(a,b)} \right) : k \in \mathbb{Z} \right\}.$$

By the principle of addition, every element of S is an integer solution to $ax + by = c \gcd(a, b)$.

Every solution is in S: If (x', y') is another solution to $ax+by = c \gcd(a, b)$, then the difference $(x' - cx_0, y' - cy_0)$ is a solution to $ax + by = 0$. Therefore $(x', y') \in S$. □