Libraria Algebrae

Liam Gardner

November 12, 2020

Contents

Chapter 1

Linear Diophantine Equations in $\mathbb{Z}^2$

Note that for the general equation $ax + by$, we assume that $ab \neq 0$, since if one is 0, then the equation is trivial. We wish to answer three fundamental problems

1. Does there exist an integer solution?
2. If the answer is yes, find an integer solution.
3. Can we find *all* solutions?

It is common for existential theorems (those that say solutions exist) to not give a means of how to find said solutions.

1.0.1 Example

Solve $506x + 391y = 23$. Notice that $\gcd(506, 391) = 23$. Thus, by bézout's lemma, a solution exists. We can use the EEA (Extended Euclidean Algorithm) to find a solution to the equation.

x	y	r	q
1	0	506	0
0	1	391	0
1	-1	115	1.0
-3	4	46	3.0
7	-9	23	2.0
-17	22	0	2.0

Thus, we know that $(7, -9)$ is a solution. Now, we can subtract the equation $506x + 391y = 23$ with $506x_0 + 391y_0 = 23$, which gives $506(x - x_0) + 391(y - y_0) = 0$. Thus, we get $506(x - x_0) = -391(y - y_0)$. We can divide by the GCD of 506 and 391 to get the equation $22(x - x_0) = -17(y - y_0)$. Since the GCD is a common divisor to 506 and 391, we get that both $\frac{506}{23}$ and $\frac{391}{23}$ are integers and are coprime to each other. Now, since we know that $-17|-17(y - y_0)$, and that $-17(y - y_0) = 22(x - x_0)$, we get that $-17|22(x - x_0)$. Thus, by CAD, we get $17|(x - x_0)$. Therefore, we find that $x - x_0 = 17n$ for some $n \in \mathbb{Z}$. Thus, a solution for x can be found with $x_0 + 17n$, $\forall n \in \mathbb{Z}$.

Following the same process, we get that $y = y_0 + 22n$. Therefore, all solutions to the Linear Diophantine Equation $506x + 391y = 23$ are given by the points $(7 + 17n, -9 - 22n)$.

Solve $506x + 391y = 24$.

There are no sol$^{\text{n}}$: Since $23 = \gcd(506, 391)$, we get that $23|506x + 391y$ however, $23 \nmid 24$, therefore, we've run into a contradiction.

Solve $506x + 391y = 46 = 2 \cdot 23$. We know that $506 \cdot 7 + 391 \cdot (-9) = 23$, thus if we multiply both sides by two, we get that $506(7 \cdot 2) + 391(-9 \cdot 2) = 2 \cdot 23 = 46$. $506(14) + 391(-18) = 46$ gives the sol$^{\text{n}}$ (14,-18).

Theorem: LDET Part 1

Suppose $a, b, c \in \mathbb{Z}$ and $ab \neq 0$ then $ax + by = c$ has a sol$^{\text{n}}$ in integers if and only if $\gcd(a, b)|c$.

1.0.2 Proof of forwards direction

Assume $ax + by = c$ has an integer sol^n (x_0, y_0). Let $d = \gcd(a, b)$. Since $d|a$ and $d|b$, and since $c = ax_0 + by_0$, then by Divsibility of Integer Combinations, $d|c$.

1.0.3 Proof of backwards direction

Let $d = \gcd(a, b)$, and assume that $d|c$, thus $c = kd \oint$ integer k. Then By Bézout's Lemma, we can find x_0 and $y_0 \in \mathbb{Z}$ such that $ax_0 + by_0 = d$, but then $k(ax_0 + by_0) = kd$. Thus $a(kx_0) + b(ky_0) = c$

1.0.4 Remark

if $d|c$ then the proof tells us how to find a sol^n .

1. solve $ax + by = d$ using EEA to get $(x, y) = (x_0, y_0)$.
2. take $x = kx_0$ and $y = ky_0$, where $k = \frac{c}{d}$.

Theorem: LDET Part 2

Suppose that (x_0, y_0) is a particular solution to the LDE $ax + by = c$.

Then the set of all sol^n $\in \mathbb{Z}$ is given by the following set:

$$S = \left\{ (x, y) \mid x = x_0 + \frac{b \cdot n}{\gcd(a, b)},\ \ y = y_0 - \frac{a \cdot n}{\gcd(a, b)} \right\}$$

1.0.5 Proof

Let D be the set of all integer solutions to $ax + by = c$. I.E.

$$D = \{(x, y) \mid x, y, \in \mathbb{Z}, ax + by = c\}$$

This can be proven by showing $S \subseteq D$ and $D \subseteq S$

$S \subseteq D$:

Let $(x, y) \in S$, thus $x = x_0 + \frac{bn}{d}$ and $y = y_0 - \frac{an}{d}$.

$$ax + by = a\left(x_0 + \frac{bn}{d}\right) + b\left(y_0 - \frac{an}{d}\right)$$

$$= ax_0 + by_0 = c$$

since by definition, we know that x_0 and y_0 are a particular solution to the equation. Therefore, $S \subseteq D$

$D \subseteq S$:

Let $(x, y) \in D$, thus $x, y \in \mathbb{Z}$ and $ax + by = c$. Since, $(x_0, y_0) \in D$, we know that $ax_0 + by_0 = c$. We can subtract $ax_0 + by_0 = c$ from $ax + by = c$ to get $a(x - x_0) + b(y - y_0) = 0$. Dividing by the GCD of a and b, we get that $\frac{a(x-x_0)}{d} = \frac{-b(y-y_0)}{d}$. Thus, since $\frac{b}{d}|\frac{a}{d}(x - x_0)$ then by CAD, we get that $\frac{b}{d}|(x - x_0)$, since $\frac{b}{d}$ and $\frac{a}{d}$ are coprime. Then we get $x - x_0 = n\frac{b}{d} \Rightarrow x = x_0 + \frac{bn}{d} \oint n \in \mathbb{Z}$. Similarly, we get $y = y_0 - \frac{an}{d}$. Therfore, $(x, y) \in S$.

1.1 More Examples

$12x + 18y = 13$.

$\gcd(12, 18) = 6$. Since $6 \nmid 13$ the equation has no sol^n by LDET1

$14x - 49y = 28$

$\gcd(14, -49) = 7$. Since $7|28$ the equation has solutions by LDET2

Consider $14x - 49y = 7 \Rightarrow 2x - 7y = 1$ which has sol^n $(4, 1)$. If we multiply $14(4) - 49(1) = 7$ by 4, we get that $14(x_0 \cdot 4) - 49(y_0 \cdot 4) = 7$, and from this we can get all sol^n using LDET2.

Find all sol^n to $15x + 35 = 5$.

x	y	r	q
1	0	15	0
0	1	35	0
1	0	15	0.0
-2	1	5	2.0
7	-3	0	3.0

Thus, we know that $\gcd(15, 35) = 5$, and $5|5$, there is a sol$^{\text{n}}$. By EEA, we find $x = -2, y = 1$ is a sol$^{\text{n}}$. Then, we can find the general solution using LDET2 to be $x = -2 + \frac{35n}{5} \Rightarrow 7n - 2$, $y = 1 + \frac{15n}{5} \Rightarrow 1 + 3n$

1.1.1 Geometric Understanding

Graphing the line $15x + 35y = 5$ or $3x + 7y = 1$, we can rearrange for y to get $y = \frac{-3}{7}x + \frac{1}{7}$. Thus, picking any lattice point, we can construct a triangle of length 7 and height 3 from that point to find the next lattice point.

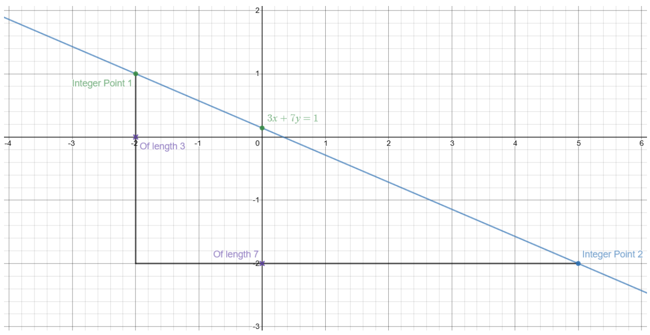

Figure 1.1: Triangle formed from moving between two lattice points

1.1.2 Nonnegative sol$^{\text{n}}$

The solutions to $15x + 35y = 5$ is given by $(-2 + 7n, 1 - 3n)$, these will be nonnegative if $x \geq 0$ and $y \geq 0$.

$$-2 + 7n \geq 0 \iff n \geq \frac{2}{7}$$

$$1 - 3n \geq 0 \iff n \leq \frac{1}{3}$$

Thus, since there are no integer solutions in the range $\frac{2}{7} \leq n \leq \frac{1}{3}$, as $n \in \mathbb{Z}$ there are no nonnegative solutions.

1.1.3 Find all integer sol$^{\text{n}}$ to $15x + 35y^2 = 5$

Let $Y = y^2$, then, since we have the sol$^{\text{n}}$ to $15x + 35Y = 5$, given by $(-2 + 7n, 1 - 3n)$, all we have to do is see when $1 - 3n$ is a perfect square. One way to solve this is to say let $z = y^2$ and solve $1 - 3n = z$. We can also solve this algebraically

$$\begin{aligned} &\iff & 1 - 3n = y^2 & \\ &\iff & -3n = y^2 - 1 & \\ &\iff & 3|y^2 - 1 & \quad \text{by euclid's lemma} \\ &\iff & 3|(y-1)(y+1) & \end{aligned}$$

By Euclid's Lemma, we know either $3|(y - 1)$ or $3|(y + 1)$, though not both. Suppose $3|(y - 1) \iff y - 1 = 3k \iff y = 3k + 1 \oint k \in \mathbb{Z}$ Then, if $y = 3k + 1$, we get that $y^2 = (1 + 3k)^2 = 1 - 3(-2k - 3k^2)$. Let $n = (-2k - 3k^2)$, then we get $y^2 = 1 - 3n$. Thus, if we take $x = -2 + 7n = -2 + 7(-2 - 3k^2)$ and $y = 1 - 3k$, we get a perfect square sol$^{\text{n}}$ to the diophantine equation.

If $3|y + 1$, then we have $y = -1 + 3l \oint l \in \mathbb{Z}$. Then $y^2 = (-1 + 3l)^2 = 1 - 3(2l + 3l^2)$. Thus, $y = 1 - 3l$ and $x = -2 + 7(2l + 3l^2)$. Therfore, we can generate infinitely many perfect square solutions.

Chapter 2

Congruence and Modular Arithmetic

2.1 Clockwork Arithmetic Analogy

Imagine a clock, we know that a clock has 12 spokes. If we look at it and see the hour hand at 2, and we know that 12 has already passed, then we also know that the clock really means it's 14. Thus, we can say $2 \approx 14$

2.2 Definition

$\forall a, b \in \mathbb{Z}$, we say that "$a$ is congruent to b mod(ulo) 12" if $m|(a-b)$.
Notation: $a \equiv b \pmod{m}$

2.3 Examples

$m = 1$ then $a \equiv b \pmod{1} \iff 1|(a-b)$ which is true $\forall a, b \in \mathbb{Z}$
$m = 2$ then $a \equiv b \pmod{2} \iff 2|(a-b) \iff a-b$ is even $\iff a$ and b are both even or both odd.
$2 \equiv -116 \pmod{2}$, however $3 \not\equiv 10024 \pmod{2}$
$14 \equiv 2 \pmod{12} \iff 12|(14-2)$
$6 \equiv 26 \pmod{10} \iff 10|(6-26)$
$6 \not\equiv -26 \pmod{10} \implies 10 \nmid (6+26)$

Proposition: Congruence is an Equivalence Relation

$\forall m \in \mathbb{N}, \forall a, b, c, \in \mathbb{Z}$	Congruence is
$a \equiv a \pmod{m}$	symmetric
if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$	transitive
$a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$	Reflexive

Remark: Any relation $a \sim b$ that satisfies all above properties is called an equivalence relation.
In calculus, we say two functions $f(x) \sim g(x)$ are an equivalence relation if $f'(x) = g'(x)$

2.4 Recap

Fix $m \in \mathbb{N}$, $\forall a, b \in \mathbb{Z}$

$$\begin{aligned} a \equiv b \pmod{m} &\iff m|(a-b) \\ &\iff a-b = mk \not\ni k \in \mathbb{Z} \\ &\iff a = b + mk \end{aligned}$$

Proposition: Arithmetic Rules of Congruence

Suppose $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$ then,

1. $a + b \equiv a' + b' \pmod{m}$

2. $a - b \equiv a' - b' \pmod{\mathrm{m}}$
3. $ab \equiv a'b' \pmod{\mathrm{m}}$

2.4.1 Examples

$$2 \equiv 9 \pmod{7} \wedge 3 \equiv 17 \pmod{7} \implies 2 + 3 \equiv 9 + 17 \pmod{7} \implies 5 = 26$$

$$56 \cdot 30 \pmod{40}$$
$$56 = 16 + 40 \equiv 16 \pmod{40}$$
$$30 = -10 \equiv \pmod{40}$$
$$56 \cdot 30 \equiv 16 \cdot (-10) \pmod{40}$$
$$\equiv -160 \pmod{40}$$
$$\equiv -40 \cdot 4 \pmod{40} \equiv 0 \pmod{40}$$

2.4.2 Proof of addition

Since $a \equiv a' \pmod{\mathrm{m}}$ and $b \equiv b' \pmod{\mathrm{m}}$ then $m|(a - a')$ and $m|(b - b')$
We have $(a + b) - (a' - b') = a - a' + b - b'$, thus by DIC we get $m|((a + b) - (a' + b'))$. Therefore $a + b \equiv a' + b' \pmod{\mathrm{m}}$

2.4.3 Remark on Division

Care is needed with division $ab \equiv ac \pmod{\mathrm{m}} \not\Longrightarrow b \equiv c \pmod{\mathrm{m}}$ even if $a \not\equiv 0 \pmod{\mathrm{m}}$

$$10 \equiv 4 \pmod{6}$$
$$2 \cdot 5 \equiv 2 \cdot 2 \pmod{6}$$
$$5 \not\equiv 2 \pmod{6}$$

Proposition: Congruent Division

If $ab \equiv ac \pmod{\mathrm{m}}$ and a is coprime to m, then $b \equiv c \pmod{\mathrm{m}}$

2.4.4 Proof

$$ab \equiv bc \pmod{\mathrm{m}} \iff m|(ab - ac) \iff m|a(b - c)$$

Then by CAD we get $m|(b - c)$ since m and a are coprime
$\implies b \equiv c \pmod{\mathrm{m}}$
By applying the above proposition repeatedly; if $a_1 \equiv a'_1 \pmod{\mathrm{m}}, a_2 \equiv a'_2 \pmod{\mathrm{m}}, \cdots a_n \equiv a'_n \pmod{\mathrm{m}}$, then we get the following result

1. $a_1 + \cdots + a_n \equiv a'_1 + \cdots a'_n \pmod{\mathrm{m}}$
2. $a_1 - \cdots - a_n \equiv a'_1 - \cdots a'_n \pmod{\mathrm{m}}$
3. $a_1 \cdots a_n \equiv a'_1 \cdots a'_n \pmod{\mathrm{m}}$
4. (special case) $\forall q \in \mathbb{N}, a^q \equiv (a')^q \pmod{\mathrm{m}}$

2.4.5 More Examples

Simplify $4^10 \pmod{18}$

$4^{10} = \left(4^2\right)^5 = 16^5 = (18-2)^5$
$(18-2)^5 \equiv -2^5 \pmod{18}$
$\equiv -32 \pmod{18}$
$-32 + 2 \cdot 18 \pmod{18}$
$4 \pmod{18}$

Is $3^9 + 62^{2020} - 20$ divisible by 7?

Let $n = 3^9 + 62^{2020} - 20$. We know that $7|n \iff 7|(n-0) \iff n \equiv 0 \pmod 7$
We can compute $3^9 = \left(3^3\right)^3 = 27^3 = (28-1)^3$
$\equiv (-1)^3 \pmod 7$
$\equiv -1 \pmod 7$
We also know that $62^{2020} = (63-1)^{2020} \equiv (-1)^{2020} \pmod 7 \equiv 1$
$20 = 21 - 1 \equiv -1 \pmod 7$
Using The arithmetic rules we get that $n \equiv -1+1-(-1) \pmod 7 \equiv 1 \pmod 7$ and thus n is not divisible by 7.

Theorem: Congruence and Remainders

2.4.6 Example

What day of the week is it going to be a year from now?
Since days cycle every 7, let's determine $365 \pmod 7$. We know that $350 = 50 \cdot 7$ and thus
$365 = 350 + 15$
$= 7 \cdot 50 + 14 + 1$
$= 7 \cdot 50 + 7 \cdot 2 + 1$
$= 7(50+2) + 1$
$\equiv 1 \pmod 7$.
$365 \equiv 1 \pmod 7$
Therefore, the day of the week one year from now is the same as the day of the week tomorrow.

2.4.7 Observation

if $n \in \mathbb{Z}$
Any block of consecutive numbers will cycle through the numbers 0-6 inclusive:

$$\{\cdots, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, \cdots\}$$

$$\equiv \{\cdots, 0, 1, 2, 3, 4, 5, 6, 0, 1, 2, 3, 4, 5, 6, 0, 1, 2, 3, 4, 5, 6, \cdots\} \pmod 7$$

2.5 Warning

$\forall a, b, b' \in \mathbb{N}$, if $b \equiv b' \pmod{m}$ then in general $a^b \not\equiv a^{b'} \pmod{m}$

2.5.1 Example

$4 \equiv 1 \pmod 3$
$2^4 = 16 \equiv 1 \pmod 3$ however $2^1 \equiv 2 \pmod 3$
Thus $4 \equiv 1 \pmod 3$ however $2^4 \not\equiv 2^1 \pmod 3$

Proposition: Finite Integers

$\forall a, b, \in \mathbb{Z} a \equiv b \pmod{m} \iff a$ and b have the same remainder after division by m

2.5.2 Proof

Applying the division algorithm, we get $a = qm + b$ and $b = q'm + r'$ where $0 \leq r, r' < m$.
Notice if $a \equiv b$ (mod m), we get that $m|(a - b)$ and thus $m|(qm + r - q'm - r')$
$\implies m|(m(q + q') + (r - r'))$ Then by DIC it follows that
$\iff m|(r - r')$
Now since $0 \leq r < m$ and $0 \leq r' < m$, we get that $-m \leq r - r' < m$. Now, since $m|(r - r')$, we get that by BBD, that $m \leq |r - r'|$ and so for both inequalities to hold, $r = r'$.