Lecture 3: Linear Diophantine equation

Friday, September 30, 2016 9:02 AM

In the previous lecture we proved

Lemma. For any integers a and b,

$$(a \mid b \wedge b \neq 0) \Rightarrow |a| \leq |b|.$$

Let's see some of its applications:

Q. Does the equation $14m - 49n = 1$ have integer solutions? (This type of equations are called Diophantine equations.)

Solution. No! Suppose to the contrary that there are integers m and n such that

$$14m - 49n = 1.$$

Then the left hand side $14m - 49n = 7(2m - 7n)$ is a multiple of 7 as $2m - 7n$ is an integer.

Hence $7 \mid 1$. By the above lemma we get

$$|7| \leq |1|,$$

which is a contradiction. ■

Lecture 03: Linear Diophantine equation

Friday, August 5, 2022 1:16 PM

As I have mentioned in the previous lectures, in math education, the following three items are of key importance:

(1) Problem solving, (2) Pattern recognition, (3) Abstract thinking.

Following this, we want to find the main ideas in the previous example and generalize it. This is a very good example of formulating an abstract result from a concrete example.

In the previous example, we have a linear equation with integer coeff. where the coeff. on the left hand side have a common divisor that do not divide the other side. This leads us to the following statement.

Theorem 1. Suppose a, b, c are integers, and a and b have a common divisor d which do not divide c. Then the Diophantine equation $ax+by=c$ does not have an integer solution.

Theorem 2. Suppose $a,b,c \in \mathbb{Z}$ and $c \neq 0$. If a and b have a common divisor d which is more than $|c|$, then $ax+by=c$ does not have an integer solution.

proof. Suppose to the contrary that it has an integer solution $x=m$ and $y=n$. Since d is a divisor of a and b, there are integers k and ℓ such that $a = dk$ and $b = d\ell$. Hence, $am+bn=c$ implies that $c = dkm + d\ell n = d(km+\ell n)$. (*) Because m, n, k, and ℓ are integers, so is $km+\ell n$. Thus by (*) we have that $d \mid c$. This contradicts the assumption that d does not divide c. ■

Proof of Theorem 2. Using Theorem 1, it is enough to show that d does not divide c. Suppose to the contrary that $d \mid c$. Then because $c \neq 0$ and $d \mid c$, we deduce that $|d| \leq |c|$. This is a contradiction as $|c| < d \leq |d|$. ■

Later in the course we will learn that the converse of Theorem 1 is also true. This means

$ax+by=c$ has an integer solution $\iff$ every common divisor of a, b divides c.

Lecture 03: The well-ordering principle

Friday, August 5, 2022 1:41 PM

As I have mentioned it earlier, in mathematics, we start with certain statements that we take for granted without proof (referred to as axioms or principle) and infer the rest from the axioms. One of the main properties of integers that we take for granted is the well-ordering principle.

Well-ordering principle. Suppose $\mathbb{Z}^{\geq 0}$ is the set of non-negative integers. We can list its elements as $\{0, 1, 2, \cdots\}$ (we use $\{$ and $\}$ in order to list elements of a set.) Let S be a subset of $\mathbb{Z}^{\geq 0}$; that means every element of S is a non-negative integer. For instance

$\mathbb{Z}^{+} = \{1, 2, 3, \cdots\}$, $E = \{0, 2, 4, \cdots\}$, or $O = \{1, 3, 5, \cdots\}$.

Well-ordering principle Suppose S is a non-empty subset of $\mathbb{Z}^{\geq 0}$ (non-empty means S has at least one element). Then S has a minimum.

You can think about the following algorithm to find the minimum of S: Start from 0 and go up; each time ask if the integer is in S. The first time that it is in S, you get the minimum.

Lecture 03: Division algorithm

Friday, August 5, 2022 5:27 PM

We are going to prove the division algorithm using the well-ordering principle, and later we will use it to prove what we claimed about linear Diophantine equations.

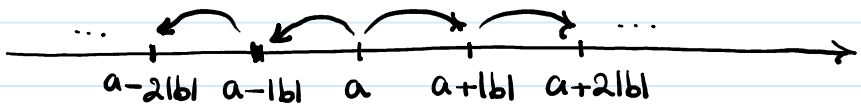
Theorem. (Division Algorithm) Suppose a and b are two integers and $b \neq 0$. Then there are pair of integers q and r such that

(1) $a = bq + r$ and (2) $0 \leq r < |b|$.

Moreover, such a pair of integers is unique.

We need to show the existence and the uniqueness of such a pair of integers.

Proof. (Existence) To find r, we have to consider non-negative numbers of the form $a - bk$ where k is an integer. Notice that integers of the form $a - bk$ are in an arithmetic progression. We can visualize this arithmetic progression; start at a and take steps of length $|b|$ either to the right or to the left



Lecture 03: Division algorithm

Friday, August 5, 2022 5:42 PM

Let S be the set of all non-negative numbers of the form $a - bk$ for some integer k.

Claim 1. S is not empty; that means $a - bk$ is not negative for some integer k.

Proof of Claim 1. Using the visualization, we start at a, and we ask ourselves how many steps of length $|b|$ should we go to the right in order pass 0. If $a \geq 0$, no step is needed. If $a < 0$, we need at most $|a|$ many steps to pass 0. This means, we claim $a + |b||a| \geq 0$. To show this, notice that $b \neq 0$ implies $|b| \geq 1$. Hence $|b||a| \geq |a|$. Since $|a| \geq -a$, we obtain that $|b||a| \geq -a$, and so $a + |a||b|$.

Notice that $|b| = \operatorname{sgn}(b)\, b$ where $\operatorname{sgn}(b) = \begin{cases} 1 & \text{if } b > 0, \\ 0 & \text{if } b = 0, \\ -1 & \text{if } b < 0. \end{cases}$

Therefore $a + |a||b| = a - b\underbrace{(-\operatorname{sgn}(b)|a|)}_{\text{an integer}} \geq 0$. □

Because S is not empty, by the well-ordering principle it has

a minimum. Suppose r is the minimum of S. Hence r is of the form $a-bq$ for some integer q and $r \geq 0$. So far, we have $a = bq+r$ and $0 \leq r$. Next we want to show that $r < |b|$.

Claim 2. $r < |b|$.

Proof of Claim 2. Suppose to the contrary that $r \geq |b|$. Then $r - |b| \geq 0$ and $r - |b| = a - bq + |b| = a - b(q - \text{sgn}(b))$, and so $r-|b|$ is in S. Therefore $r-|b|$ is at least the minimum of S. This means $r - |b| \geq r$, which implies that $|b| \leq 0$. This is a contradiction as $b \neq 0$.

Altogether we have that $a = bq+r$ and $0 \leq r < |b|$. This finishes proof of the existence part.

Uniqueness. Suppose (q_1, r_1) and (q_2, r_2) satisfy the mentioned properties we have to show $q_1 = q_2$ and $r_1 = r_2$. That means we have to show

$$\left.\begin{array}{l} a = bq_1 + r_1 = bq_2 + r_2 \\ 0 \leq r_1, r_2 < |b| \end{array}\right\} \overset{?}{\Longrightarrow} q_1 = q_2 \text{ and } r_1 = r_2.$$

Lecture 03: Division algorithm

Saturday, August 6, 2022 12:25 AM

$bq_1 + r_1 = bq_2 + r_2$ implies $bq_1 - bq_2 = r_2 - r_1$, and so

$b(q_1 - q_2) = r_2 - r_1$. Therefore $b \mid r_2 - r_1$. ..... (1)

On the other hand, since $0 \le r_1 < |b|$, we have $-|b| < -r_1 \le 0$. ..... (2)

Adding (2) to $0 \le r_2 < |b|$, we obtain that

$$-|b| < r_2 - r_1 < |b|.$$

Thus $|r_2 - r_1| < |b|$. ..... (3)

By (1), either $r_2 - r_1 = 0$ or $|b| \le |r_2 - r_1|$. The latter contradicts (3). Hence $r_2 - r_1 = 0$, which implies $r_1 = r_2$.

Therefore $b(q_1 - q_2) = r_2 - r_1 = 0$. Because $b \neq 0$, we obtain that $q_1 - q_2 = 0$. Thus $q_1 = q_2$. ■

In algebra, you will learn about other system of numbers with a similar property. Division algorithm plays an important role in understanding various divisibility properties of integers. Here is an example.

<u>Definition</u>. An integer n is called <u>even</u> if n is a multiple of 2.

• An integer is called <u>odd</u> if it is not even.

Lecture 03: Even and odd numbers

Saturday, August 6, 2022 12:43 AM

Ex. For an integer n, n is even if and only if $n = 2k$ for some integer k.

Solution. n is even $\iff 2 \mid n \iff n = 2k$ for some integer k.

Ex. For an integer n, n is odd if and only if $n = 2k+1$ for some integer k.

To show a biconditional proposition is true, we have to prove both directions $\Rightarrow$ and $\Leftarrow$.

Proof. ($\Rightarrow$) Suppose n is odd. By the division algorithm, there are integer pairs q and r such that $n = 2q+r$ and $0 \leq r < 2$.

Hence r is either 0 or 1.

Claim $r = 1$.

Proof of Claim. Suppose to the contrary $r \neq 1$. Therefore $r = 0$, which implies $n = 2q$. We obtain that n is even which is a contradiction.

By the previous Claim, $n = 2q+1$

($\Leftarrow$) Suppose to the contrary that n is even. This means $n = 2\ell$ for

integer ℓ. Hence $2k+1 = 2\ell$; and so $2(k-\ell) = 1$. Thus $2 \mid 1$, which implies $2 \leq 1$. This is a contradiction. ∎