Lecture 4: 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 4: Diophantine

Friday, September 30, 2016 9:23 AM

The same argument implies.

<u>Lemma</u>. Suppose a and b are two integers.

If a and b have a common divisor d greater than 1,

then the equation $ax+by=1$ has <u>no</u> integer solutions.

<u>Draft / Proof.</u>

Given	$\overset{?}{\Longrightarrow}$	Goal
$d\mid a,\ d\mid b,\ d>1$ x, y : integer		$ax+by\neq 1$

Proof by contradiction

Given	$\overset{?}{\Longrightarrow}$	Goal
$d\mid a,\ d\mid b,\ d>1,$ x,y : integer $ax+by=1$		Contradiction

$d\mid a \Longrightarrow$ for some integer a'

$a = d a'$

$d \mid b \Longrightarrow$ for some integer b'

$b = d b'$

$\Longrightarrow ax+by = da'x + db'y$

$= d(a'x+b'y)$

$\Longrightarrow d \mid ax+by = 1$

$\overset{\text{by lemma}}{\Longrightarrow} |d| \leq 1,$

which is a contradiction. ■

Lecture 4: Biconditional proposition, odd and even

Friday, September 30, 2016 9:38 AM

In fact, the converse of this lemma is also correct, but it is harder to prove. We will do it later in this course.

Converse of $P \Rightarrow Q$ is $Q \Rightarrow P$. In general $P \Rightarrow Q$ might be true and at the same time $Q \Rightarrow P$ be false.

Biconditional Proposition $P \Leftrightarrow Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$.

- P if and only if Q.
- P is necessary and sufficient for Q.
- $P \Leftrightarrow Q$ is true exactly when P and Q have the same truth value.

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Definition. Let n be an integer. We say n is even if $2 | n$.

We say n is odd if n is NOT even.

Important remark. Since the above conditional proposition is defining a phrase, it gets promoted to a biconditional proposition.