Proofs: divisibility, II

Monday, October 5, 2015 11:10 AM

In the previous lecture we were proving:

<u>Theorem</u>. For any integer n, n is odd $\Longleftrightarrow$ $n = 2k+1$ for some integer.

We proved $(\Longrightarrow)$. For $(\Longleftarrow)$ look at my previous note.

<u>Corollary</u>. For any integers m and n, mn is odd if and only if m and n are odd.

<u>Pf</u>. $(\Longrightarrow)$

Given	Goal
mn is odd	m is odd <u>and</u> n is odd

<u>Proof by contradiction</u>

Given	Goal
$2 \nmid mn$ $\neg(2 \nmid m \wedge 2 \nmid n)$	Contradiction

Given	Goal
$2 \nmid mn$ $2 \mid m \vee 2 \mid n$	Contradiction

We need to show <u>two</u> things

We need to show two things

Given	Goal
$2 \nmid mn$ $2 \mid m$	Contradiction

and

Given	Goal
$2 \nmid mn$ $2 \mid n$	Contradiction

They look the same: changing the roles of m and n we get the same statement.

In this kind of scenarios, we say "by symmetry it is enough to show that ..." or "without loss of generality we can and will assume that ..."

$2 \mid m \implies m = 2k$ for some integer k

$\implies mn = 2kn$ (and kn is an integer)

$\implies 2 \mid mn$

which contradicts our assumption that mn is odd.

($\Leftarrow$)

Given	Goal
$2 \nmid m \wedge 2 \nmid n$	mn is odd

$$\left.\begin{array}{l} 2 \nmid m \implies m = 2k+1 \text{ for some integer } k \\ 2 \nmid n \implies n = 2k'+1 \text{ for some integer } k' \end{array}\right\}$$

So we have

$$mn = (2k+1)(2k'+1) = 4kk' + 2k + 2k' + 1$$

$$= 2\underbrace{(2kk'+k+k')}_{\text{is an integer}}+1$$

Hence $mn = 2k''+1$ for some integer k''.

Therefore mn is odd. ■

Ex. Does the equation $14m - 49n = 1$ have an integer solution?

Solution. No, it does NOT.

Suppose to the contrary that it does have a solution.

So $14m - 49n = 1$ for some integers m and n.

Therefore $7(2m - 7n) = 1$, which implies

$$7 \mid 1$$

as $2m-7n$ is an integer. By our earlier result we should have $|7| \le |1|$ which is a contradiction. ■

Remark Equation $ax+by=1$ has an integer solution if and only if a and b have no common divisors except ± 1.

We will prove this later, but $(\Longrightarrow)$ is easy and the same argument as above works.

Lemma. Let a, b, c be integers. If for some integers x and y, $ax+by=c$, and d is a common divisor of a and b, then $d \mid c$.

Pf.

Given	Goal
$ax+by=c$ $d \mid a$ $d \mid b$	$d \mid c$

$d \mid a \Rightarrow$ for some integer k, $a = dk$ (I)

$d \mid b \Rightarrow$ for some integer k', $b = dk'$ (II)

By (I), (II), and our assumption,

$$c = ax + by = dkx + dk'y$$

$$\Rightarrow \quad c = d\underbrace{(kx+k'y)}_{\text{is an integer}}$$

$$\Rightarrow \quad d \mid c. \quad \blacksquare$$

Ex. There are no integers m and n such that

$$66m - 110n = 2.$$

Pf. Suppose to the contrary that there are such integers. Then $11(6m-10n) = 2$, which implies $11 \mid 2$. Therefore we should have $11 \leq 2$, which is a contradiction. $\blacksquare$

An alternative approach: Suppose to the contrary that there are such integers m and n. So, by the above lemma, since 11 is a common divisor of 66 and 110, it should be a divisor of 2. Hence we should have $11 \leq 2$, which is a contradiction. ■