## Lecture 4

Handout or Document Camera or Class Exercise

**Instructor's Comments: Clicker Questions to start every 4th lecture.**

Suppose $A$, $B$ and $C$ are all true statements.

The compound statement $(\neg A) \vee (B \wedge \neg C)$ is

A) True

B) False

**Solution:** The answer is False.

**Instructor's Comments: This should take about 5 minutes. For all clicker questions, if the results are poor - get them to talk to each other and repoll.**

**Recall:**

**Proposition:** Let $A$ and $B$ be statements. Then $A \Rightarrow B \equiv \neg A \vee B$.

**Proposition:** Let $A$ and $B$ be statements. Then $\neg(A \Rightarrow B) \equiv A \wedge \neg B$. Reworded, the negation of an implication is the hypothesis and the negation of the conclusion.

**Proof:**

$$\begin{aligned} \neg(A \Rightarrow B) &\equiv \neg(\neg A \vee B) && \text{By the above proposition} \\ &\equiv \neg(\neg A) \wedge \neg B && \text{De Morgan's Law} \\ &\equiv A \wedge \neg B && \text{By proposition from class} \end{aligned}$$

This completes the proof. ■

**Instructor's Comments: This is the 10 minute mark. Note it is important to do the negation of implication with them.**

**Definition:** Denote the set of integers by $\mathbb{Z}$.

**Note:** We use $\mathbb{Z}$ since this is the first letter of the word integer... in German! (Zählen)

**Definition:** Let $m, n \in \mathbb{Z}$. We say that $m$ divides $n$ and write $m \mid n$ if (and only if) there exists a $k \in \mathbb{Z}$ such that $mk = n$. Otherwise, we write $m \nmid n$, that is, when there is no integer $k$ satisfying $mk = n$.

**Note:** The "(and only if)" part will be explained in a few lectures.

**Instructor's Comments: I tell my students that definitions in mathematics should be if and only if however mathematicians are sloppy and do not do this in practice.**

**Example:**

(i) $3 \mid 6$

(ii) $2 \mid 2$

(iii) $7 \mid 49$

(iv) $3 \mid -27$

(v) $6 \nmid 8$

(vi) $55 \mid 0$

(vii) $0 \mid 0$

(viii) $0 \nmid 3$

**Instructor's Comments: This is the 17 minute mark**

**Example:** Does $\pi \mid 3\pi$? This question doesn't make sense since in the definition of $\mid$, we required both $m$ and $n$ to be integers (there are ways to extend the definition but here we're restricting ourselves to talk only about integers when we use $\mid$).

**Example:** (Direct Proof Example) Prove $n \in \mathbb{Z} \wedge 14 \mid n \Rightarrow 7 \mid n$.

**Proof:** Let $n \in \mathbb{Z}$ and suppose that $14 \mid n$. Then $\exists k \in \mathbb{Z}$ s.t. $114k = n$. Then $(7 \cdot 2)k = n$. By associativity, $7(2k) = n$. Since $2k \in \mathbb{Z}$, we have that $7 \mid n$.

**Note:** The symbol $\exists$ means "there exists". the letters s.t. mean " such that".

**Instructor's Comments: This is the 30 minute mark. It is not necessary to mention associativity above but I'll introduce rings at some point and so this seems like a good opportunity to remind students of what things they can take as axioms.**

**Recall:** An integer $n$ is

(i) Even if $2 \mid n$

(ii) Odd if $2 \mid (n-1)$.

**Proposition:** Let $n \in \mathbb{Z}$. Suppose that $2^{2n}$ is an odd integer. Show that $2^{-2n}$ is an odd integer.

**Proof:** Note that the hypothesis is only true when $n = 0$. If $n < 0$, then $2^{2n}$ is not an integer. If $n > 0$ then $2^{2n} = 2 \cdot 2^{2n-1}$ and since $2n - 1 > 0$, we see that $2^{2n}$ is even. Hence $n = 0$ and thus $2^{2n} = 1 = 2^{-2n}$. Thus $2^{-2n}$ is an odd integer. ■

**Note:** Ask yourself when is the hypothesis true. Then consider that/those case(s). Breaking up into cases is a great way to prove statements. Sometimes breaking a statement into even and odd, or positive and negative are great strategies.

**Instructor's Comments: This is the 40 minute mark. Ask the students to attempt to give you a good definition of prime. This is a good exercise for students to make precise definitions.**

**Definition:** An integer $p$ is said to be *prime* if (and only if) $p > 1$ and its only positive divisors are 1 and $p$.

**Example:** Show that $p$ and $p + 1$ are prime only when $p = 2$.

**Instructor's Comments: Can do this example if you have time. Otherwise it's fine to leave it as an exercise**

**Proposition:** Bounds by Divisibility (BBD).

$$a \mid b \wedge b \neq 0 \Rightarrow |a| \leq |b|$$

**Proof:** Let $a, b \in \mathbb{Z}$ such that $a \mid b$ and $b \neq 0$. Then $\exists k \in \mathbb{Z}$ such that $ak = b$. Since $b \neq 0$, we know that $k \neq 0$. Thus, $|a| \leq |a||k| = |ak| = |b|$ as required. ■

**Instructor's Comments: This is probably the 50 minute mark. If you have time, state TD and DIC below.**

**Proposition:** Transitivity of Divisibility (TD)

$$a \mid b \wedge b \mid c \Rightarrow a \mid c$$

**Proof:** There exists a $k \in \mathbb{Z}$ such that $ak = b$. There exists an $\ell \in \mathbb{Z}$ such that $b\ell = c$. This implies that $(ak)\ell = c$ and hence $a(k\ell) = c$. Since $k\ell \in \mathbb{Z}$, we have that $a \mid c$. ■

**Proposition:** Divisibility of Integer Combinations (DIC). Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $a \mid c$. Then for any $x, y \in \mathbb{Z}$, we have $a \mid (bx + cy)$.