# Lecture 10: Irreducible numbers

Saturday, October 15, 2016 9:46 PM

<u>Definition</u>. An integer $n \geq 2$ is called <u>irreducible</u> if the following holds:

For any integers $a, b$, $n = ab \Rightarrow (n = \pm a \vee n = \pm b)$

<u>Lemma</u>. Suppose $n$ is an integer larger than 1.

$n$ is irreducible if and only if the only positive divisors of $n$ are 1 and $n$. (Alternatively, there is <u>no</u> $d \mid n \wedge 1 < d < n$.)

<u>Proof</u>. ($\Leftarrow$) Suppose to the contrary that there is

$$d \mid n \wedge 1 < d < n.$$

So $n = dk$ for some integer $k$. Since $n$ is irreducible, $n = \pm d$ <u>or</u> $n = \pm k$. Since $d$ and $n$ are positive, so is $k$.

Thus $(n = |n| = |\pm d| = d)$ or $(n = |n| = |\pm k| = k)$.

<u>Case 1</u>. $n = d$, which contradicts $d < n$.

<u>Case 2</u>. $n = k$. This implies $k = dk$. So either $k = 0$ or $d = 1$, and they contradict $k > 0$ and $d > 1$.

# Lecture 10: Factorization into irreducibles

Saturday, October 15, 2016 9:58 PM

($\Leftarrow$) Suppose $n = ab$. Then $n = |n| = |ab| = |a||b|$.

Hence $|a| \mid n$. Therefore $|a| \le n$ as $n$ is positive.

Since $n$ has no divisor in the open interval $(1, n)$, $|a| = 1$ or $n$.

<u>Case 1.</u> $|a| = 1$. In this case, $n = |a||b| = |b|$. So

$$n = \pm b.$$

<u>Case 2.</u> $|a| = n$, so $n = \pm a$. ∎

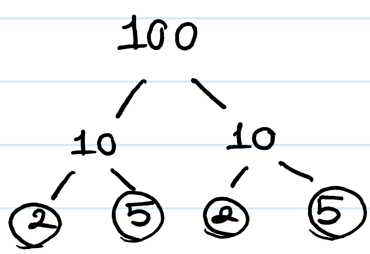
<u>Ex.</u> • 6 is NOT irreducible as $2 \mid 6$ and $1 < 2 < 6$.

• 2 is irreducible as its positive divisors are 1 and 2.

• 3 is irreducible as its positive divisors are 1 and 3.

We would like to write an integer $\ge 2$ as a product of smaller numbers. We continue this till we reach to numbers that we cannot factor further. These "atom" like numbers are precisely irreducibles.

Ex. Write 100 as product of irreducibles:



# Lecture 10: Factorization into irreducibles

Saturday, October 15, 2016 10:11 PM

**Lemma.** Any integer $n \geq 2$ can be written as product of irreducibles

**Remark 1.** We are using this convention that the above product can have only 1 term. For instance $2 = 2$ is how we write 2 as product of irreducibles. Or $3 = 3$ is the way we write 3 as product of irreducibles.

**Remark 2.** Later we will prove that for an integer $n \geq 2$

$$n \text{ is irreducible} \iff n \text{ is prime}.$$

In your HW assignment, you are proving

$$\text{prime} \Rightarrow \text{irreducible}.$$

**Remark 3.** Later we will prove (or maybe you will see this in Math 100 or 104) that this factorization is unique upto permutation of irreducible factors.

**Proof of Lemma.** We use strong induction on $n$.

**Base of strong induction.** $n=2$. As we said in Remark 1, $2=2$ is such factorization.

**Strong induction step.** For a given integer $k \geq 2$, we assume

# Lecture 10: Factorization into irreducibles

Saturday, October 15, 2016 10:25 PM

that any integer $2 \leq i \leq k$ can be written as product of irreducibles. We have to show that $k+1$ can be written as product of irreducibles.

<u>Case 1</u> $k+1$ is irreducible.

In this case $k+1 = k+1$ gives us a factorization of $k+1$ into irreducibles.

<u>Case 2.</u> $k+1$ is NOT irreducible.

Hence there are integers $a, b$ such that

$$k+1 = ab \quad \wedge \quad k+1 \neq \pm a \quad \wedge \quad k+1 \neq \pm b.$$

Therefore $k+1 = |ab| = |a| \cdot |b| \ \wedge \ k+1 \neq |a| \ \wedge \ k+1 \neq |b|$.

Thus (why?) $1 < |a|, |b| < k+1$, which implies

$$2 \leq |a|, |b| \leq k.$$

So by the strong induction hypothesis $|a|$ and $|b|$ can be written as product of irreducibles, say $|a| = p_1 \cdot \ldots \cdot p_r$ and $|b| = q_1 \cdot \ldots \cdot q_s$ where $p_1, \ldots, p_r$ and $q_1, \ldots, q_s$ are irreducibles. Then $k+1 = p_1 \cdots p_r \cdot q_1 \cdots q_s$ is a factorization of $k+1$ into irreducibles. ■

# Lecture 10: Language of set theory

Saturday, October 15, 2016 11:09 PM

In this course we do NOT carefully study set theory (and its axioms). We casually introduce what a set is, and go over the basics of its language.

"Definition" A well-defined collection of objects.

$\boxed{\text{What to expect from a set.}}$ A box containing certain objects.

For instance:
- The set of integers is denoted by $\mathbb{Z}$. (Stands for Zahlen.)
- The set of rationals is denoted by $\mathbb{Q}$.
- The set of reals is denoted by $\mathbb{R}$.
- The set of complex numbers is denoted by $\mathbb{C}$.