Lecture 06: Factorization into irredcuibles

Saturday, October 15, 2016 9:46 PM

Let's recall that an integer p is called <u>irreducible</u> if $p \neq 0$, $p \neq \pm 1$, and for every integer a and b, $p = ab$ implies $a = \pm 1$ or $b = \pm 1$.

<u>Ex.</u> $6 = 2 \times 3$, and so 6 is not irreducible.

Notice that p is irreducible if and only if it does not have a divisor d such that $1 < d < |p|$ and $p \neq 0$ and $p \neq \pm 1$.

<u>Proof.</u> ($\Longrightarrow$) Suppose to the contrary that there is an integer d such that $1 < d < |p|$ and $d \mid p$. So $p = dk$ for some integer k. Since p is irreducible, either $d = \pm 1$ or $k = \pm 1$. The former is not possible as $1 < d$. Hence, $k = \pm 1$, which implies $d = \pm p$. Thus $|d| = |p|$. Because $d > 1$, we obtain $d = |p|$ which contradicts $d < |p|$.

($\Longleftarrow$) Since $p \neq 0$ and $p \neq \pm 1$, it is enough to show that for every integers a and b, $p = ab$ implies $a = \pm 1$ or $b = \pm 1$.

Since $p = ab$, $a \mid p$. Thus $|a| \leq |p|$ and $|a|$ is a positive divisor of p. By the assumption, p has no advisor from 2 to $|p| - 1$. Hence

Lecture 06: Factorization into irreducibles

Saturday, October 15, 2016   9:58 PM

$|a|=1$ or $|p|$.

<u>Case 1.</u> $|a|=1$. We are done.

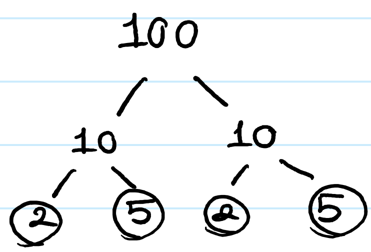
<u>Case 2.</u> $|a|=|p|$. In this case, $|p|=|a|\,|b|$, which implies $|b|=1$. $\blacksquare$

<u>Ex.</u>
- 2 is irreducible as its positive divisors are 1 and 2.
- 3 is irreducible as its positive divisors are 1 and 3.

Irreducibles can be viewed as "atoms" of integers based on multiplication. In the sense that, we cannot write them as a product of integers with smaller absolute values.

Starting with an integer $n \geq 2$, we repeatedly factor it till we cannot! This way we write every such integer as a product of irreducibles.

Ex. Write 100 as product of irreducibles:



Next we make this argument formal.

Lecture 06: Factorization into irreducibles

Saturday, October 15, 2016 10:11 PM

Lemma. Every 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 $\underline{1}$ term. For instance $2 = 2$ is how we write 2 as a product of irreducibles. Or $3 = 3$ is the way we write 3 as a 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

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

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 that every integer $2 \le l \le k$ can be written as product of irreducibles. We have to show that $k+1$ can be written as product of irreducibles.

Case 1 $k+1$ is irreducible.

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

Case 2. $k+1$ is NOT irreducible.

Hence there are integers a, b such that

$$k+1 = ab, \quad a \ne \pm 1, \quad \text{and} \quad b \ne \pm 1.$$

Therefore $k+1 = |ab| = |a| \cdot |b|$, $|a| \ne 1$, and $|b| \ne 1$.

Since $k+1 \ne 0$, $|a| \ne 0$ and $|b| \ne 0$. Hence, $|a|, |b| \ge 2$. Therefore $|a|\,|b| \ge 2\,|b|$, which implies $k+1 \ge 2\,|b|$. Thus $|b| \le \frac{k+1}{2}$, and by symmetry, $|a| \le \frac{k+1}{2}$. Notice that $\frac{k+1}{2} \le k$ (as $\frac{k+1}{2} \le k \Leftarrow k+1 \le 2k \Leftarrow 1 \le k$.). Hence, $2 \le |a|, |b| \le k$. By the strong induction hypothesis, $|a|$ and $|b|$ can be written as products of irred.

Lecture 6: Factorization into irreducibles

Friday, August 12, 2022 8:30 PM

That means $|a| = p_1 \cdots p_s$ and $|b| = q_{r_1} \cdots q_{r_t}$ for some irreducibles p_i's and q_{r_j}'s. Then

$$k+1 = |a|\,|b| = p_1 \cdots\cdots p_s \cdot q_{r_1} \cdot \cdots \cdot q_{r_t}$$ can be written as a product of irreducibles. ∎

Next we use strong induction to solve a stamp problem.

<u>Stamp problem</u> We have two types of stamps. The first type is 3-cent, and the second type is 5-cent. What is the largest postage value which cannot be made using these types of stamps?

(The same problem can be asked for a-cent and b-cent stamps where the greatest factor of a and b is 1.)

Before giving a formal solution to the mentioned stamp problem, we try to figure it out by going over the positive integers one-by-one.

1	4	7	10 ⟶
2	5	8	⟶
3	6	9	⟶

We write integers in three rows, and circle every value which can be made. Notice that, if a value can be made,

Lecture 06: Stamp problem

Friday, August 12, 2022 8:59 PM

then all the number after that in the same can be made as well, by adding sufficently many 3-cent stamps.

Notice that $7-3=4$ and $7-5=2$ cannot be made, and so 7 cannot be made. From this analysis, we see the largest value which cannot be made is 7. Next we use strong induction to show:

Every value $n \geq 8$ can be made using 3-cent and 5-cent stamps.

Proof We use strong induction on n.

Base of strong induction. $8=3+5$, and so 8 can be made by 3-cent and 5-cent stamps.

Strong induction step. Suppose for an integer k the following holds: for every integer $8 \leq l \leq k$, l value can be made by 3-cent and 5-cent stamps. (strong induction hypothesis). We have to show that $k+1$ can be made by 3-cent and 5-cent stamps.

Case 1. $(k+1)-3 \geq 8$.

In this case $8 \leq (k+1)-3 \leq k$, and so by the strong induction

Lecture 06: Stamp problem

Friday, August 12, 2022 9:16 PM

hypothesis, $(k+1)-3$ can be made using 3-cent and 5-cent stamps.

Adding one more 3-cent stamp, we can make $\underline{k+1}$.

<u>Case 2</u>. $(k+1)-3<8$.

In this case, $k<10$. Hence $8 \leq k \leq 9$. Then $k+1$ is either 9 or 10.

$9=3+3+3$ and $10=5+5$, which means both 9 and 10 can be made by 3-cent and 5-cent stamps. Hence, in this case $k+1$ can be made as well. $\blacksquare$

<u>Remark</u>. If the greatest common divisor of a and b is 1, then the largest value which <u>cannot</u> be made by a-cent and b-cent stamps is $ab-a-b$. This is a very nice challenging problem.