

Review

Given $a \neq b$ in our universe \mathbb{Z} , there are two generators g and $-g$ of the ideal

$$((a, b)) \stackrel{\text{def}}{=} \{xa + yb : x, y \in \mathbb{Z}\}$$

of all linear combinations of a, b . Both of them are common divisors of a, b with the property that any other common divisor of a, b divides either; this makes either a greatest common divisor. Thus the two greatest common divisors of a, b agree with the two generators of $((a, b))$. The positive one among them is from now on called **The Greatest Common Divisor of a, b** and is denoted by $\gcd(a, b)$.

Lemma: Let $a \neq b \in \mathbb{Z}$ and set $g \stackrel{\text{def}}{=} \gcd(a, b)$. There are unique α, β with $a = g\alpha$ and $b = g\beta$, and α, β are relatively prime.

The Least Common Multiple

Let $a, b \in \mathbb{Z}$. We know that $((a)) \cap ((b))$ is an ideal. There exists therefore an integer l so that

$$((a)) \cap ((b)) = ((l)) .$$

Clearly (why?)

$$a|l \quad \text{and} \quad b|l .$$

This makes l a **Common Multiple of a, b** .

Let now m be another common multiple of a and b . Then $m \in ((a))$ and $m \in ((b))$,

and therefore

$$m \in ((a)) \cap ((b)) = ((l)) \quad \text{and} \quad l|m :$$

That is to say, l is a common multiple of a and b that divides every other common multiple of them: l is reasonably called a **Least Common Multiple**. [“Least” does not refer to the order \leq on \mathbb{Z} !].

Unless ???, there are exactly two least common multiples of a and b differing by a factor of -1 (why?). We shall denote the positive least common multiple of a and b by $\text{lcm}(a, b)$ and call it **THE** least common multiple.

Lemma: Let $0 < a, b \in \mathbb{Z}$. Then

$$\text{gcd}(a, b) \times \text{lcm}(a, b) = a \times b .$$

Proof: There are $x, y, \alpha, \beta \in \mathbb{Z}$ such that

$$g \stackrel{\text{def}}{=} \gcd(a, b) = xa + yb \quad \text{and} \quad a = \alpha g, \quad b = \beta g.$$

Set $l \stackrel{\text{def}}{=} \text{lcm}(a, b)$. Then $gl = xal + ybl$, whence $ab|gl$ and $g\alpha g\beta|gl$ and $g\alpha\beta|l$. Thus $g\alpha\beta = l$ (Why?) and $ab = gl$. **QED**

Lemma: Let $a, b, p \in \mathbb{Z}$, p prime. Then

$$p|(ab) \implies p|a \vee p|b.$$

Proof: We prove the equivalent statement

$$p|(ab) \wedge p \nmid a \implies p|b.$$

Now if $p \nmid a$ then a, p are relatively prime and there are x, y with

$$xa + yp = 1 \implies xab + ybp = b \quad \text{and} \\ p|b. \quad \text{QED}$$

Corollary: $\sqrt{2}$ is irrational.

Proof: BWoC assume $\sqrt{2}$ is rational; then there are strictly positive integers m, n such that

$$\sqrt{2} = \frac{m}{n} .$$

WLoG $\gcd(m, n) = 1$ (why?). Then

$$2m^2 = n^2 \quad \text{and} \quad 2|n^2 \quad \text{and} \quad 2|n .$$

Thus there is a $k \in \mathbb{Z}$ with $n = 2k$ and so

$$2m^2 = 2^2k^2 \quad \text{and} \quad m^2 = 2k^2 \quad \text{and} \quad 2|m .$$

This contradiction proves the claim. QED

The Fundamental Theorem of Arithmetic: Every integer $n > 1$ can be written as a product of primes, uniquely up to order.

Proof of Existence: If this were not so then there would be a least integer $l > 1$

that could not be written as a product of primes. l is not a prime, because a prime is a “product of one primes.” So l is composite. There are q, k with $1 < q, k < l$ and $qk = l$. Both q and k are products of primes, and then so is l . This contradiction proves the claim. **QED**

Proof of Uniqueness: Suppose $n > 1$ can be written as

$$\begin{aligned} n &= p_1 \cdot p_2 \cdots p_k \quad \text{and} \\ &= \bar{p}_1 \cdot \bar{p}_2 \cdots \bar{p}_l . \end{aligned}$$

We can reorder the rows so that $k \leq l$ and

$$\begin{aligned} p_1 &\leq p_2 \leq \cdots \leq p_k \quad \text{and} \\ \bar{p}_1 &\leq \bar{p}_2 \leq \cdots \leq \bar{p}_l . \end{aligned}$$

Let p'_1 the smaller (\leq) of p_1, \bar{p}_1 . If $p'_1 = p_1$

then since

$$p_1 | (\bar{p}_1 \cdot \bar{p}_2 \cdots \bar{p}_l) ,$$

we must have $p_1' = p_1 = \bar{p}_1$. By the same argument, if $p_1' = \bar{p}_1$ then $p_1' = \bar{p}_1 = p_1$. In any case, $p_1 = \bar{p}_1$ and therefore

$$\begin{aligned} & p_2 \cdot p_3 \cdots p_k \\ &= \bar{p}_2 \cdot \bar{p}_3 \cdots \bar{p}_l . \end{aligned}$$

We continue this argument to show that always the first listed prime in both rows are the same. Clearly then all the primes in the two rows are the same and are the same in number. QED

Corollary: Let $1 < n \in \mathbb{N}$. There exist unique primes $p_1, \dots, p_k \geq 0$ and exponents

$e_1, \dots, e_k \geq 1$ so that

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k} .$$

The number of positive divisors of this integer n is

$$\prod_{i=1}^k (e_i + 1) \stackrel{\text{def}}{=} (e_1 + 1) \cdot (e_2 + 1) \cdots (e_k + 1) .$$