§2. Unique Factorization and Least Common Multiple in $\mathbb{N}$.

It is a matter of experience that

✓ Each integer $n>1$ is either a prime or a product of primes,

e.g. $6 = 2.3$, $24 = 2.2.2.3$

If we agree to say that a prime is a product of primes (with only one prime factor and no multiplications), then we have a simpler statement

✓ Each integer $n>1$ is a product of primes.

The gain in simplicity justifies the agreement. Even simpler would be

Each $n \in \mathbb{N}$ is a product of primes

but to accomodate $n=1$ we must also agree to say that 1 is a product, with no prime factors and no multiplications.

THM A. $\square$ is a true statement (granting our agreements).

Proof. For each $n \in \mathbb{N}$, denote by $\square_n$ the statement that

n is a product of primes.

Then to prove $\square$, we must prove infinitely many statements: $\square_1, \square_2, \square_3, \cdots$.
This is easier than it looks. We just do them one by one:

$\square_1$ is true, by one of our agreements.

$\square_2$ and $\square_3$ are true by one of our agreements, since 2 and 3 are primes.

$\square_4$: $4 = 2.2$ ✓

To save time, suppose we have proved $\square_n$ for all $n<l$. What about $\square_l$?

If l is prime, then $\square_l$ is true, by one of our agreements

If l is not prime, then l has a divisor d other than 1 or l; so $l = dq$ with $d, q \in \mathbb{N}$ and $d<l$, $q<l$. By the underlined supposition, $\square_d$ & $\square_q$ are true: d and q are products of primes, so l ($=dq$) is a product of primes: $\square_l$ is true.

REMARK In the example with $n=24$, we could write

$$24 = 2.2.2.3 = 2.2.3.2 = 2.3.2.2 = 3.2.2.2,$$

four ways of writing 24 as a product of primes. They are all the same, if we agree not to distinguish between prime factorizations in which the prime factors are permuted, i.e. written in a different order. With this agreement, there is a unique (i.e. only one) way to write 24 as a product of primes. The same is true for each $n \in \mathbb{N}$!

THM B (Unique Factorization Theorem) The factorization of a positive integer n into primes is unique, i.e. if

$$n = p_1 \cdots p_r = q_1 \cdots q_s$$

where the p's and q's are primes, then $r=s$; and, after a possible permutation (i.e. reordering) of the q's, we have $p_1 = q_1, \dots, p_r = q_r$.

Proof. Let $\mathcal{O}_n$ be the statement of THM B, applied to n.

For $n=1$, there are no p's or q's, i.e. $r=s=0$, so $\mathcal{O}_1$ is true.

Let $\ell \geq 1$ and suppose we have proved $\mathcal{O}_n$ for all $n < \ell$. What about $\mathcal{O}_\ell$?

Let

$$\ell = p_1 \cdots p_r = q_1 \cdots q_s \quad (\checkmark)$$

be any two prime factorizations of ℓ. Here $r \geq 1$ and $s \geq 1$, since $\ell > 1$.

Since $\ell = (p_1 \cdots p_{r-1})\, p_r$, we get $p_r \mid \ell$, i.e. $p_r \mid q_1 \cdots q_s$.

By THM G in §1, p_r is one of the q's. After possibly reordering of the q's, we may suppose $p_r = q_s$. Cancelling p_r in $\checkmark$ now gives

$$(\checkmark\checkmark) \quad n = p_1 \cdots p_{r-1} = q_1 \cdots q_{s-1}, \text{ with } n = \ell / p_r$$

two factorizations of n (an integer $< \ell$!!). Since $\mathcal{O}_n$ is true, we have $r-1 = s-1$ and, after a possible reordering of the q's, $p_1 = q_1, \dots, p_{r-1} = q_{r-1}$, giving $r=s$ and $p_1 = q_1, \dots, p_r = q_r$. Thus $\mathcal{O}_\ell$ is also true.

NOTATION. Just as $24 = 2^3 \cdot 3$ and $180 = 2^2 \cdot 3^2 \cdot 5$, we may write the prime factorization of each $n \in \mathbb{N}$ in the form

$$n = 2^{\nu_2} 3^{\nu_3} 5^{\nu_5} \cdots = \prod p^{\nu_p},$$

Here, for each prime p, ν_p denotes the number of times p occurs in the prime factorization of n. In this formula, each ν_p is an integer ≥ 0, and $\nu_p = 0$ except for finitely many p — the prime divisors of n — so there is no danger of having to multiply forever. The symbol $\prod$ stands for "product." For $n = 24$, $\nu_2 = 3$, $\nu_3 = 1$ and $\nu_p = 0$ for all primes $p \neq 2, 3$.

THM C Let $d, e, m, n \in \mathbb{N}$. Then:

(1) If $d = \prod p^{\delta_p}$ and $e = \prod p^{\varepsilon_p}$, then $de = \prod p^{\delta_p + \varepsilon_p}$.

(2) If $d = \prod p^{\delta_p}$ and $n = \prod p^{\nu_p}$, then $d \mid n \iff \delta_p \leq \nu_p$ for all p.

(3) If $m = \prod p^{\mu_p}$ and $n = \prod p^{\nu_p}$, then $(m, n) = \prod p^{\min\{\mu_p, \nu_p\}}$.

Proof. (1) This follows from $p^{\varepsilon} p^{\delta} = p^{\varepsilon + \delta}$.

(2) If $d \mid n$, then $n = de$ for some $e \in \mathbb{N}$, so by (1) for each p, $\delta_p + \varepsilon_p = \nu_p$, so $\delta_p \leq \nu_p$, since $\varepsilon_p \geq 0$. Conversely, if $\delta_p \leq \nu_p$ for each p, put $\varepsilon_p = \nu_p - \delta_p$. Then $\varepsilon_p \geq 0$ for each p and $\varepsilon_p = 0$ except for finitely many p. Putting $e = \prod p^{\varepsilon_p}$, we get $de = n$, so $d \mid n$.

(3) Let $d \in \mathbb{N}$. Then d divides both m and $n \iff$ for each prime p,

$$\delta_p \leq \mu_p \text{ and } \delta_p \leq \nu_p$$

i.e. $\delta_p \leq \min\{\mu_p, \nu_p\}$.

The greatest common divisor of m and n is the largest such d, which has for each p

$$\delta_p = \min\{\mu_p, \nu_p\}$$

DEF. For $m, n \in \mathbb{N}$ an integer ℓ is a common multiple of m and n if both $m|\ell$ and $n|\ell$. (For example, mn is a common multiple of m and n.) The least positive common multiple of m and n is called the least common multiple of m and n, and is denoted by $[m,n]$.

THM D Let $m, n \in \mathbb{N}$. Then

(1) If $m = \prod p^{\mu_p}$ and $n = \prod p^{\nu_p}$, then $[m,n] = \prod p^{\max\{\mu_p, \nu_p\}}$.

(2) Each common multiple of m and n is a multiple of $[m,n]$.

(3) $(m,n)[m,n] = mn$

EXERCISE 1 Prove THM D.

COR. If $\ell, m, n \in \mathbb{N}$ and $m|\ell$ and $n|\ell$ and $(m,n)=1$, then $mn|\ell$.

Proof. $[m,n]|\ell$, by (2), and $[m,n] = mn$, by (1).

THM E. Let $\ell, m, n \in \mathbb{N}$. Put $\ell = \prod p^{\lambda_p}$, $m = \prod p^{\mu_p}$, $n = \prod p^{\nu_p}$. Then

(1) The greatest common divisor (ℓ, m, n) of ℓ, m, n is given by $\prod p^{\min\{\lambda_p, \mu_p, \nu_p\}}$.

(2) The least common multiple $[\ell, m, n]$ of ℓ, m, n is given by $\prod p^{\max\{\lambda_p, \mu_p, \nu_p\}}$.

(3) $(\ell, m, n)[mn, \ell n, \ell m] = \ell m n$

EXERCISE 2. Prove THM E. Hint for (3): $\min\{\lambda,\mu,\nu\} + \max\{\mu+\nu, \lambda+\nu, \lambda+\mu\} = ?$

THM F (due Euclid) There are infinitely many primes.

Proof. If there are only finitely many primes, let P be their product, and let p be a prime divisor of $P+1$. Then p divides $(P+1)-P = 1$, impossible.

REMARK. Moving ahead 2000 years, Gauss conjectured $\simeq 1800$, and Hadamard and de la Vallee Poussin proved independently in 1896 the Prime Number Theorem:

The number $\pi(x)$ of primes $p \le x$ satisfies $\pi(x) \sim \frac{x}{\log x}$ (i.e. $\frac{\pi(x)}{\frac{x}{\log x}} \to 1$ for $x \to \infty$).

In particular $\frac{\pi(x)}{x} \to 0$, i.e. "almost no positive integers are prime."