__Lecture 6__: Applications of UF.

In the previous lecture we proved the extremely important theorem:

__Thm__ (Fundamental theorem of Arithmetics)

Any integer $n > 1$ can be uniquely written as

$$p_1^{k_1} \cdot \cdots \cdot p_\ell^{k_\ell}$$

where $p_1 < \cdots < p_\ell$ are primes and $k_1, \ldots, k_\ell$ are positive integers.

__Cor.__ (Euclid) There are infinitely many primes.

__Pf.__ Suppose to the contrary that there are only finitely primes:

$$p_1 < \cdots < p_n.$$

Consider $N = p_1 \cdot \cdots \cdot p_n + 1$, and let p be a prime divisor of N. Then $p = p_i$ for some i. So

$$\left.\begin{array}{l} p_i \mid p_1 \cdots p_n + 1 \\ p_i \mid p_1 \cdot \cdots \cdot p_n \end{array}\right\} \Longrightarrow p_i \mid 1, \quad \text{which is a contrad.}$$

■

So there are infinitely many primes: $2, 3, 5, 7, \ldots$

and any integer $n > 1$ can be __uniquely__ written as $2^{v_2} \cdot 3^{v_3} \cdot 5^{v_5} \cdot \ldots$

where $v_i \geq 0$ and we use the convention that product of infinitely many $\underline{1}$ is $\underline{1}$.

Def. For any prime p and non-zero integer $\underline{n}$ let $v_p(n)$ be the power of p in the prime decomposition of $\underline{n}$.

Exp.
$$\begin{cases} v_2(12) = v_2((2^2)(3)) = 2 \\ v_3(12) = 1 \\ v_p(12) = 0 \quad \text{for any } p \geq 5. \end{cases}$$

- $v_p(1) = 0$ for any p.
- $v_5(-10) = 1$.

Basic Properties of $v_p(n)$

1. For any positive integer we have
$$n = \prod_{p \text{ prime}} p^{v_p(n)}.$$

2. For any prime p and positive integers n and m we have:

$$v_p(mn) = v_p(m) + v_p(n)$$

Pf ① is just the def. of $v_p(n)$.

② $$\left.\begin{array}{l} n = \prod p^{v_p(n)} \\ m = \prod p^{v_p(m)} \end{array}\right\} \Rightarrow \begin{array}{l} mn = \prod p^{v_p(n)+v_p(m)} \\ \Rightarrow v_p(mn) = v_p(m) + v_p(n). \end{array}$$

■

Cor. Let d and n be two positive integers. Then

$$d \mid n \iff \forall p \in \mathcal{P},\ v_p(d) \leq v_p(n).$$

Pf. ($\Rightarrow$) $d \mid n \Rightarrow n = dd'$

$$\Rightarrow v_p(n) = v_p(d) + v_p(d') \geq v_p(d).$$

($\Leftarrow$) $$n = \prod p^{v_p(n)} = \Big(\underbrace{\prod p^{v_p(d)}}_{= d}\Big)\Big(\underbrace{\prod p^{v_p(n) - v_p(d)}}_{\in \mathbb{Z}}\Big)$$

$$\Rightarrow d \mid n.$$

■

Having the prime decomposition of an integer n helps us to compute $f(n)$ for various arithmetic functions f. (The so-called multiplicative functions.) To see one such example consider:

Def. $d(n) := |\{m \mid m \geq 1 \text{ and } m|n\}|$

(The number of positive divisors of n.)

Exp. • $d(1) = 1$

• $d(p) = 2$ if $p \in \mathcal{P}$.

• $d(10) = 4 \rightsquigarrow 1, 2, 5, 10$.

• $d(2^{100}) = 101 \rightsquigarrow 2^i$ for $0 \leq i \leq 100$.

Proposition $d(n) = \prod_{p \in \mathcal{P}} (v_p(n) + 1)$.

Pf.

$$m \mid n = \prod p^{v_p(n)} \iff 0 \leq v_p(m) \leq v_p(n)$$

So, for any p, $v_p(m)$ has $\underline{v_p(n)+1}$ possibilities

so by the multiplication principle

$$m = \prod p^{v_p(m)} \quad \text{and} \quad 0 \leq v_p(m) \leq v_p(n)$$

has $\prod (v_p(n)+1)$ many possibilities. ■

Proposition $\sqrt{2}$ is irrational.

Pf. Suppose to the contrary that $\sqrt{2} = \frac{m}{n}$

$$\Rightarrow 2 = \frac{m^2}{n^2} \Rightarrow 2n^2 = m^2$$

$$\Rightarrow v_2(2n^2) = v_2(m^2) \Rightarrow v_2(2) + 2v_2(n) = 2v_2(m)$$

$\Longrightarrow \quad 1 = 2(v_2(m) - v_2(n)) \Longrightarrow 2 \mid 1$ which is a contradiction. $\blacksquare$

By a similar argument one can prove that

Proposition A positive integer a is a perfect square, i.e. $a = n^2$ for some integer n, if and only if $2 \mid v_p(a)$ for any p.