

Chapter 2: Applications of Unique Factorization

Author: Meng-Gen Tsai

Email: plover@gmail.com

Exercise. If $\frac{a}{b} \in \mathbb{Z}_p$ is not a unit, prove that $\frac{a}{b} + 1$ is a unit.

Proof. $\frac{a}{b} \in \mathbb{Z}_p$ is not a unit iff $p \mid a$ and $p \nmid b$. Thus $p \nmid (a + b)$. That is, $\frac{a}{b} + 1 = \frac{a+b}{b} \in \mathbb{Z}_p$ is a unit. \square

Exercise 2.6. (p -adic valuation.) For a rational number r let $[r]$ be the largest integer less than or equal to r , e.g., $[\frac{1}{2}] = 0$, $[2] = 2$, $[3\frac{1}{3}] = 3$. Prove

$$\text{ord}_p n! = \left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right] + \left[\frac{n}{p^3} \right] + \cdots.$$

Notice that $\left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right] + \left[\frac{n}{p^3} \right] + \cdots$ is a finite sum.

Proof. For any $k = 1, 2, \dots, n$, we can express k as $k = p^s t$ where $s = \text{ord}_p k$ is a non-negative integer and $(t, p) = 1$. There are $\left[\frac{n}{p^a} \right]$ numbers such that $p^a \mid k$ for $a = 1, 2, \dots$. Therefore, there are

$$\left[\frac{n}{p^a} \right] - \left[\frac{n}{p^{a+1}} \right]$$

numbers such that $\text{ord}_p k = a$ for $a = 1, 2, \dots$. Hence,

$$\begin{aligned} \text{ord}_p n! &= \left(\left[\frac{n}{p} \right] - \left[\frac{n}{p^2} \right] \right) + 2 \left(\left[\frac{n}{p^2} \right] - \left[\frac{n}{p^3} \right] \right) + 3 \left(\left[\frac{n}{p^3} \right] - \left[\frac{n}{p^4} \right] \right) + \cdots \\ &= \left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right] + \left[\frac{n}{p^3} \right] + \cdots. \end{aligned}$$

\square

Supplement. Related problems.

(1) Prove that

$$\frac{(m+n)!}{m!n!}$$

is an integer for all non-negative integers m and n .

Proof. It is sufficient to show that

$$\text{ord}_p(m+n)! \geq \text{ord}_p m! + \text{ord}_p n!$$

for any prime p , or show that

$$\left\lfloor \frac{m+n}{p^k} \right\rfloor \geq \left\lfloor \frac{m}{p^k} \right\rfloor + \left\lfloor \frac{n}{p^k} \right\rfloor$$

for any prime p and $k \in \mathbb{Z}^+$ by Exercise 4.6, or show that

$$[x+y] \geq [x] + [y]$$

for any rational (or real) numbers x and y . It is trivial by considering that the sum of two fractional parts $\{x\} = x - [x]$ might be greater than or equal to 1, so $[x+y] = [x] + [y]$ or $[x] + [y] + 1$. \square

Note. $\frac{(m+n)!}{m!n!}$ is a binomial coefficient. Similarly, a multinomial coefficient is

$$\frac{(n_1 + n_2 + \cdots + n_k)!}{n_1!n_2! \cdots n_k!}.$$

We can show that the multinomial coefficient is an integer by using the above argument.

(2) *Prove that*

$$\frac{(2m)!(2n)!}{m!n!(m+n)!}$$

is an integer for all non-negative integers m and n .

Proof. Similar to (1), it is sufficient to show that

$$[2x] + [2y] \geq [x] + [y] + [x+y]$$

for any rational (or real) numbers x and y . Notice that $[2x] = [x] + [x + \frac{1}{2}]$, and thus we might show that $[x + \frac{1}{2}] + [y + \frac{1}{2}] \geq [x+y]$. Again it is trivial and we omit the tedious calculation. \square

(3) *Hermite's identity:* $[nx] = \sum_{k=0}^{n-1} [x + \frac{k}{n}]$ for $n \in \mathbb{Z}^+$.

Let $n = 2$ and we can get $[2x] = [x] + [x + \frac{1}{2}]$ too.

Proof. Consider the function $f(x) = \sum_{k=0}^{n-1} [x + \frac{k}{n}] - [nx]$. Notice that $f(x + \frac{1}{n}) = f(x)$. f has period $\frac{1}{n}$. It then suffices to prove that $f(x) = 0$ on $[0, \frac{1}{n})$. But in this case, the integral part of each summand in f is equal to 0. Therefore $f = 0$ on \mathbb{R} . \square

(4) *Show*

$$\frac{(5m)!(5n)!}{m!n!(3m+n)!(3n+m)!}$$

is an integer for all non-negative integers m and n .

Try to deduce the inequality $[5x] + [5y] \geq [x] + [y] + [3x + y] + [3y + x]$.