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*

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

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

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

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

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

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

$\square$

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

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

for any prime p, or show that

$$\left[\frac{m+n}{p^k}\right] \geq \left[\frac{m}{p^k}\right] + \left[\frac{n}{p^k}\right]$$

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 $[5x] + [5y] \geq [x] + [y] + [3x + y] + [3y + x]$.

Exercise 2.7. *Deduce from Exercise 6 that $\mathrm{ord}_p n! \leq \frac{n}{p-1}$ and that $n!^{\frac{1}{n}} \leq \prod_{p|n!} p^{\frac{1}{p-1}}$.*

Proof.

$$\begin{aligned}
\mathrm{ord}_p n! &= \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots \\
&\leq \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \cdots \\
&= \frac{\frac{n}{p}}{1 - \frac{1}{p}} \\
&= \frac{n}{p-1}.
\end{aligned}$$

Thus,

$$n! = \prod_{p|n!} p^{\mathrm{ord}_p n!} \leq \prod_{p|n!} p^{\frac{n}{p-1}} = \left(\prod_{p|n!} p^{\frac{1}{p-1}}\right)^n,$$

or

$$n!^{\frac{1}{n}} \leq \prod_{p|n!} p^{\frac{1}{p-1}}.$$

□

Exercise 2.8. *Use Exercise 7 to show that there are infinitely many primes. [Hint: $(n!)^2 \geq n^n$.] (This proof is due to Eckford Cohen.)*

Claim. $(n!)^2 \geq n^n$.
Proof of Claim. Write $(n!)^2 = \prod_{k=1}^n k \prod_{k=1}^n (n+1-k) = \prod_{k=1}^n k(n+1-k)$, and $n^n = \prod_{k=1}^n n$. It suffices to show that $k(n+1-k) \geq n$ for each $1 \leq k \leq n$. Notice that $k(n+1-k) - n = (n-k)(k-1) \geq 0$ for $1 \leq k \leq n$. The inequality holds. □

The inequality can be written as $(n!)^{\frac{1}{n}} \geq \sqrt{n}$.

Proof. By Exercise 7 and Claim,

$$\prod_{p|n!} p^{\frac{1}{p-1}} \geq (n!)^{\frac{1}{n}} \geq \sqrt{n}.$$

Assume that there are finitely many primes, the value $\prod_{p|n!} p^{\frac{1}{p-1}}$ is a finite number whenever the value of n. However, $\sqrt{n} \to \infty$ as $n \to \infty$, which leads to a contradiction. Hence there are infinitely many primes. $\square$

Exercise 2.27. *Show that* $\sum' \frac{1}{n}$*, the sum being over square free integers, diverges. Conclude that* $\prod_{p \leq N}(1 + \frac{1}{p}) \to \infty$ *as* $N \to \infty$*. Since* $e^x > 1 + x$*, conclude that* $\sum_{p \leq N} \frac{1}{p} \to \infty$*. (This proof is due to I. Niven.)*

There are many proofs of $\sum_p \frac{1}{p}$ diverges.

Proof.

(1) For any positive integers n, we can write $n = a^2 b$ where $a \in \mathbb{Z}^+$ and b is a square free integer. Given N,

$$\sum_{n \leq N} \frac{1}{n} \leq \left(\sum_{a=1}^{\infty} \frac{1}{a^2} \right) \left(\sum_{b \leq N}{}' \frac{1}{b} \right).$$

Notices that $\sum_{a=1}^{\infty} \frac{1}{a^2}$ converges. Since $\sum_{n \leq N} \frac{1}{n} \to \infty$ as $N \to \infty$, $\sum_{b \leq N}' \frac{1}{b} \to \infty$ as $N \to \infty$.

(2) By the unique factorization theorem on $n \leq N$,

$$\prod_{p \leq N} \left(1 + \frac{1}{p}\right) \geq \sum_{n \leq N}{}' \frac{1}{n}.$$

Since $\sum_{n \leq N}{}' \frac{1}{n} \to \infty$ as $N \to \infty$, $\prod_{p \leq N}(1 + \frac{1}{p}) \to \infty$ as $N \to \infty$.

(3) By applying the inequality $e^x > 1 + x$ on any prime p,

$$\exp\left(\frac{1}{p}\right) > 1 + \frac{1}{p}.$$

Now multiplying the inequality over all primes $p \leq N$ and noticing that $\exp(x) \cdot \exp(y) = \exp(x + y)$, we have

$$\exp\left(\sum_{p \leq N} \frac{1}{p}\right) > \prod_{p \leq N} \left(1 + \frac{1}{p}\right).$$

So $\exp\left(\sum_{p \leq N} \frac{1}{p}\right) \to \infty$ as $N \to \infty$, or $\sum_{p \leq N} \frac{1}{p} \to \infty$ as $N \to \infty$. $\square$