MTH26001 - Elementary Number Theory

Name: Nguyen Minh Duc

Student ID: 20202026

ASSIGNMENT 5.

Sec 6.1.

Problem 7.

(a) ⊗ Suppose $\tau(n)$ is odd.

Factorize $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ (p_i is prime and $k_i \in \mathbb{N}$)&

$\Rightarrow \tau(n) = (k_1+1)(k_2+2)\dots(k_r+1)$.

Since $\tau(n)$ is odd, the right hand side must be odd.

$\Rightarrow k_i + 1$ is odd $\forall i \in [1, r]$

$\Rightarrow k_i$ is even $\forall i \in [1, r]$.

$\Rightarrow k_i = 2u_i \; \forall i \in [1, r]$ ($u_i \in \mathbb{Z}$).

Thus, $n = p_1^{2u_1} p_2^{2u_2} \dots p_r^{2u_r} = (p_1^{u_1} p_2^{u_2} \dots p_r^{u_r})^2$

$\Rightarrow n$ is a perfect square. — (1)

⊗ Conversely, suppose n is a perfect square.

$\Rightarrow n = a^2$ for $a \in \mathbb{Z}$. Factorize $a = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$.

$\Rightarrow n = p_1^{2k_1} p_2^{2k_2} \dots p_r^{2k_r}$.

$\Rightarrow \tau(n) = (2k_1+1)(2k_2+1)\dots(2k_r+1)$.

Since each of $2k_i+1$ is odd $\forall i \in [1, r]$, $\tau(n)$ is odd. — (2).

⊗ From (1) and (2), $\tau(n)$ is odd $\Leftrightarrow$ n is a perfect square.

(b) ⊗ Suppose $\sigma(n)$ is odd.

Factorize $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ (p_i is prime and $k_i \in \mathbb{N}$).

$\Rightarrow \sigma(n) = (1 + p_1 + p_1^2 + \dots + p_1^{k_1})(1 + p_2 + p_2^2 + \dots + p_2^{k_2}) \dots (1 + p_r + p_r^2 + \dots + p_r^{k_r})$.

Since $\sigma(n)$ is odd, each $1 + p_i + p_i^2 + \dots + p_i^{k_i}$ is odd $\forall i \in [1, r]$.

If $p_i = 2$ then each p_i^j is even $\forall j \in [1, k_i]$.

$\Rightarrow 1 + p_i + p_i^2 + \dots + p_i^{k_i} = 1 + 2 + 2^2 + \dots + 2^{k_i}$ is odd $\forall k_i$.

If $p_i > 2$, i.e, an odd prime, Then if k_i is ~~even~~ odd, we have an odd number of terms $p_i + p_i^2 + \dots + p_i^{k_i}$, which is odd.

$\Rightarrow 1 + p_i + p_i^2 + \dots + p_i^{k_i}$ is even.

Hence, k_i must be even so that $1 + p_i + p_i^2 + \dots + p_i^{k_i}$ to be odd.

$\Rightarrow k_i = 2u_i$ for $u_i \in \mathbb{Z} \Rightarrow p_i^{k_i} = p_i^{2u_i} = (p_i^{u_i})^2$.

Now, if $2 \mid n$, then:

$$n = 2^{k_1} (p_2^{u_2} p_3^{u_3} \dots p_r^{u_r})^2.$$

$$= 2^{k_1} a^2 \text{ for } a = p_2^{u_2} p_3^{u_3} \dots p_r^{u_r}.$$

For k_1 is even, $k_1 = 2s$ $(s \in \mathbb{Z})$.

$\Rightarrow n = 2^{2s} a^2 = (2^s a)^2$ is a perfect square — (1)

For k_1 is odd, $k_1 = 2s + 1$ $(s \in \mathbb{Z})$

$\Rightarrow n = 2^{2s+1} a^2 = 2(2^{2s} a^2) = 2(2^s a)^2$ is twice a perfect square. — (2)

If $2 \nmid n$, then

$n = (p_1^{u_1} p_2^{u_2} \dots p_r^{u_r})^2$ is a perfect square — (3).

From (1), (2) and (3), n will be either perfect square or twice — (*)

(*) a perfect square

Conversely, suppose n is a perfect square or twice a perfect square

<u>Case 1.</u> $n = a^2$, Factorize $a = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$

$\Rightarrow n = p_1^{2k_1} p_2^{2k_2} \dots p_r^{2k_r}$.

$\Rightarrow \sigma(n) = (1 + p_1 + p_1^2 + \dots + p_1^{2k_1})(1 + p_2 + p_2^2 + \dots + p_2^{2k_2}) \dots (1 + p_r + p_r^2 + \dots + p_r^{2k_r})$

Similar to the above proof,

if $p_i = 2$, $1 + p_i + p_i^2 + \dots + p_i^{2k_i}$ is always odd.

if $p_i > 2$, $1 + p_i + p_i^2 + \dots + p_i^{2k_i}$ is odd when $2k_i$ is even, which is true.

Thus, $1 + p_i + p_i^2 + \dots + p_i^{2k_i}$ is odd. $\forall i \in [1, r]$

$\Rightarrow \sigma(n)$ is odd. — (1).

<u>Case 2:</u> $n = 2a^2$. Factorize $a = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$

$\Rightarrow n = 2 p_1^{2k_1} p_2^{2k_2} \dots p_r^{2k_r}$. WLOG, assume $p_1 < p_2 < \dots < p_r$.

- If $2 \mid n \Rightarrow p_1 = 2 = 2^{2k_1+1} p_2^{2k_2} \dots p_r^{2k_r} = n$.

$\Rightarrow \sigma(n) = (1 + 2 + 2^2 + \dots + 2^{2k_1+1})(1 + p_2 + p_2^2 + \dots + p_2^{2k_2}) \dots (1 + p_r + p_r^2 + \dots + p_r^{2k_r})$.

We know that: $1 + 2 + 2^2 + \dots + 2^{2k_1+1}$ is always odd.

$1 + p_i + p_i^2 + \dots + p_i^{2k_i+1}$ is odd for $p_i > 2 = p_1$.

$\Rightarrow \sigma(n)$ is odd. — (2)

- If $2 \nmid n \Rightarrow n = 2 p_1^{2k_1} p_2^{2k_2} \dots p_r^{2k_r}$.

$\Rightarrow \sigma(n) = \sigma(2) \sigma(p_1^{2k_1} p_2^{2k_2} \dots p_r^{2k_r})$ ($\because$ 2 and p_i are coprime).

Since $\sigma(2) = 1 + 2 = 3$ is odd and $\sigma(p_1^{2k_1} p_2^{2k_2} \dots p_r^{2k_r})$ is odd as shown above, $\sigma(n)$ is odd — (3)

From ①, ② and ③, $\sigma(n)$ is odd. — (∗∗)

Therefore, from (∗) and (∗∗), $\sigma(n)$ is odd $\Leftrightarrow$ n is perfect square or twice.

Problem 10.

(a) It is clear that $\sigma(n) \geq n+1 > n$.

$$\Rightarrow \frac{n}{\sigma(n)} < 1. \Rightarrow 1 > \frac{n}{\sigma(n)} \quad — ①$$

Note that $\sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1} \cdot \frac{p_2^{k_2+1}-1}{p_2-1} \cdots \frac{p_r^{k_r+1}-1}{p_r-1}$.

$$\Rightarrow \frac{n}{\sigma(n)} = \frac{p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}(p_1-1)(p_2-1)\cdots(p_r-1)}{(p_1^{k_1+1}-1)(p_2^{k_2+1}-1)\cdots(p_r^{k_r+1}-1)}.$$

$$= \frac{(p_1-1)(p_2-1)\cdots(p_r-1)}{\frac{(p_1^{k_1+1}-1)(p_2^{k_2+1}-1)\cdots(p_r^{k_r+1}-1)}{p_1^{k_1}\ p_2^{k_2}\ \cdots\ p_r^{k_r}}}.$$

$$= \frac{(p_1-1)(p_2-1)\cdots(p_r-1)}{\left(p_1-\frac{1}{p_1^{k_1}}\right)\left(p_2-\frac{1}{p_2^{k_2}}\right)\cdots\left(p_r-\frac{1}{p_r^{k_r}}\right)}. \ (*)$$

Now, observe that $p_i > p_i - \frac{1}{p_i^{k_i}} \Rightarrow \frac{1}{p_i-\frac{1}{p_i^{k_i}}} > \frac{1}{p_i}$.

From $(*)$, $\frac{n}{\sigma(n)} > \frac{(p_1-1)(p_2-1)\cdots(p_r-1)}{p_1\ p_2\ \cdots\ p_r} = \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$. — ②

From ① and ②, $1 > \frac{n}{\sigma(n)} > \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$.

(b) Firstly, let's prove $\sum_{d|n} \frac{1}{d} = \frac{\sigma(n)}{n}$. $\forall n > 0$.

Note that if $d|n$ then $\frac{n}{d} | n$ as $d\frac{n}{d} = n$.

$\Rightarrow$ The set of divisors of n $\{d_1, d_2, \dots, d_k\} = \{\frac{n}{d_1}, \frac{n}{d_2}, \dots, \frac{n}{d_k}\}$

$\Rightarrow \sigma(n) = \sum_{i=1}^{k} d_i = \sum_{i=1}^{k} \frac{n}{d_i} = n \sum_{i=1}^{k} \frac{1}{d_i}$.

$\Rightarrow \sigma(n) = n \sum_{d|n} \frac{1}{d}$

$\Rightarrow \frac{\sigma(n)}{n} = \sum_{d|n} \frac{1}{d}$.

Clearly, $1, 2, 3, \dots, n$ are divisors of $n!$

$$\Rightarrow \frac{\sigma(n!)}{n!} = \sum_{d \mid n!} \frac{1}{d} \geq \frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{n}.$$

$$\Rightarrow \frac{\sigma(n!)}{n!} \geq 1 + \frac{1}{2} + \dots + \frac{1}{n}.$$

(c) Since n is composite, $\exists d : d \mid n$ and $1 < d < n$

$$\Rightarrow 1 < \frac{n}{d} < n \text{ and } \frac{n}{d} \mid n.$$

Suppose $d \leq \sqrt{n}$, assume that $\frac{n}{d} < \sqrt{n}$, then

$$n = d\,\frac{n}{d} < \sqrt{n}\sqrt{n} = n. \text{ This is contradiction.}$$

Hence, if $d \leq \sqrt{n}$ then $\frac{n}{d} \geq \sqrt{n}$.

Let $\sigma(n) = 1 + d_1 + d_2 + \dots + d_k + n$. WLOG, assume $1 < d_1 < d_2 < \dots < d_k < n$.

Since n is composite, $\exists d_i : d_i \leq \sqrt{n} \Rightarrow \frac{n}{d_i} \geq \sqrt{n}$.

As $\frac{n}{d_i} \mid n$, $\exists d_j : d_j = \frac{n}{d_i}$ $(j \geq i)$.

Now, $d_j \geq \sqrt{n} \Rightarrow 1 + d_j > \sqrt{n} \Rightarrow 1 + d_1 + d_2 + \dots + d_k > \sqrt{n}$

$$\Rightarrow \sigma(n) > n + \sqrt{n}.$$

Problem 20.

(a) Let $f(n) = 2^{\omega(n)}$

Let m, n be 2 coprime integers, i.e, $\gcd(m,n) = 1$.

Factorize $m = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$

$$n = q_1^{t_1} q_2^{t_2} \dots q_s^{t_s}.$$

Since $\gcd(m,n) = 1$, $p_i \neq q_j$ $\forall i,j : 1 \leq i \leq r,\ 1 \leq j \leq s$.

Note that $\omega(m) = r$,

$\omega(n) = s$.

$mn = p_1^{k_1} \dots p_r^{k_r} q_1^{t_1} \dots q_s^{t_s}$ has $r+s$ distinct prime factors.

$$\Rightarrow \omega(mn) = r + s = \omega(m) + \omega(n).$$

$$\Rightarrow f(mn) = 2^{\omega(mn)} = 2^{\omega(m)+\omega(n)} = 2^{\omega(m)} \cdot 2^{\omega(n)} = f(m) f(n).$$

$\Rightarrow f(mn) = f(m) f(n)$ for coprime m, n.

$\Rightarrow 2^{\omega(n)}$ is multiplicative.

(b) Since $f(n) = 2^{\omega(n)}$ is multiplicative, $F(n) = \sum_{d|n} f(d) = \sum_{d|n} 2^{\omega(d)}$ is multiplicative

Factorize $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$.

$$\Rightarrow F(n) = F(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}).$$

$$= F(p_1^{k_1}) F(p_2^{k_2}) \ldots F(p_r^{k_r})$$

$$= \left(\sum_{d|p_1^{k_1}} 2^{\omega(d)}\right)\left(\sum_{d|p_2^{k_2}} 2^{\omega(d)}\right) \cdots \left(\sum_{d|p_r^{k_r}} 2^{\omega(d)}\right).$$

~~To~~ Note that $\begin{cases} \text{the divisors of } p_i^{k_i} \text{ are } 1, p_i, p_i^2, \ldots, p_i^{k_i}. \\ \omega(p_i^{\alpha_i}) = 1 \text{ for } 1 \leq \alpha_i \leq k_i \\ \omega(p_i^0) = \omega(1) = 0. \end{cases}$

$$\Rightarrow \sum_{d|p_i^{k_i}} 2^{\omega(d)} = 2^0 + \underbrace{2^1 + 2^1 + \ldots + 2^1}_{k_i \text{ terms}}$$

$$= 1 + 2k_i$$

Thus, $F(n) = \left(\sum_{d|p_1^{k_1}} 2^{\omega(d)}\right)\left(\sum_{d|p_2^{k_2}} 2^{\omega(d)}\right) \cdots \left(\sum_{d|p_r^{k_r}} 2^{\omega(d)}\right)$

$$= (2k_1+1)(2k_2+1)\ldots(2k_r+1)$$

Note that $n^2 = p_1^{2k_1} p_2^{2k_2} \ldots p_r^{2k_r}$.

$$\Rightarrow \tau(n^2) = (2k_1+1)(2k_2+1)\ldots(2k_r+1)$$

$$= F(n).$$

$$\Rightarrow \tau(n^2) = \sum_{d|n} 2^{\omega(d)}.$$

Sec 6.2

Problem 2.

⊗ Consider the sum $\sum_{d|n} \Lambda(d)$.

Let factorize $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$.

$$\Rightarrow \sum_{d|n} \Lambda(n) = \sum_{i=1}^{r} \sum_{j=1}^{k_i} \Lambda(p_i^j)$$

$$= \sum_{i=1}^{r} \sum_{j=1}^{k_i} \log p_i = \sum_{i=1}^{r} k_i \log p_i = \sum_{i=1}^{r} \log p_i^{k_i} = \log\left(\prod_{i=1}^{r} p_i^{k_i}\right)$$

$$= \log n.$$

$$\Rightarrow \log n = \sum_{d|n} \Lambda(n).$$

By Mobius inversion formula,

$$\Lambda(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \log d = \sum_{d|n} \mu(d) \log \frac{n}{d}$$

$$= \sum \mu(d)(\log n - \log d)$$

$$= \sum_{d|n} \mu(d) \log n - \sum_{d|n} \mu(d) \log d.$$

$$= \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d.$$

If $n = 1$, $\log n = 0$ Then $\Lambda(n) = -\sum_{d|n} \mu(d) \log d$.

If $n \neq 1$, $\sum_{d|n} \mu(d) = 0$, then $\Lambda(n) = -\sum_{d|n} \mu(d) \log d$.

Therefore, $\Lambda(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \log d = -\sum_{d|n} \mu(d) \log d$

Problem 3.

⊗ From the hint, $F(n) = \sum_{d|n} \mu(d) f(d)$ is multiplicative.

⊗ Consider $F(p^k)$, p is prime, $k \in \mathbb{N}$.

$$F(p^k) = \sum_{d|p^k} \mu(d) f(d) = \mu(1) f(1) + \mu(p) f(p) + \dots + \mu(p^k) f(p^k)$$

$$= \mu(1) f(1) + \mu(p) f(p) \quad (\because \mu(p^i) = 0 \text{ for } i \geq 2).$$

$$= f(1) - f(p)$$

$$= 1 - f(p) \quad (\because f(n) \text{ is not identical } 0).$$

Since $F(n)$ is multiplicative, we have: $F(n) = \sum_{d|n} \mu(d) f(d) = F(p_1^{k_1}) F(p_2^{k_2}) \dots F(p_r^{k_r})$.

$$= (1 - f(p_1))(1 - f(p_2)) \dots (1 - f(p_r)).$$

Problem 6.

⊗ Firstly, let's prove that they are multiplicative.

Consider $f(n) = \frac{\mu^2(n)}{\tau(n)}$ and $g(n) = \frac{\mu^2(n)}{\sigma(n)}$

We know that $\mu(n), \sigma(n), \tau(n)$ are multiplicative.

Let m, n be coprime intergers,

- $f(mn) = \frac{\mu^2(mn)}{\tau(mn)} = \frac{\mu^2(m)\mu^2(n)}{\tau(m)\tau(n)} = f(m)f(n)$.

$\Rightarrow f(mn) = f(m)f(n)$

$\Rightarrow f$ is multiplicative. — (1)

- $g(mn) = \frac{\mu^2(mn)}{\sigma(mn)} = \frac{\mu^2(m)\mu^2(n)}{\sigma(m)\sigma(n)} = g(m)g(n)$

$\Rightarrow g(mn) = g(m)g(n)$

$\Rightarrow g$ is multiplicative. — (2).

⊗ From (1) and (2), we obtain that.

$$F(n) = \sum_{d|n} f(d) = \sum_{d|n} \frac{\mu^2(d)}{\tau(d)} \text{ and } G(n) = \sum_{d|n} \frac{\mu^2(d)}{\sigma(d)} = \sum_{d|n} g(d)$$

are multiplicative.

⊗. Let $n = p^k$, p is prime and $k \in \mathbb{N}$.

$$F(p^k) = \sum_{d|p^k} \frac{\mu^2(d)}{\tau(d)} = \frac{\mu^2(1)}{\tau(1)} + \frac{\mu^2(p)}{\tau(p)} + \frac{\mu^2(p^2)}{\tau(p^2)} + \dots + \frac{\mu^2(p^k)}{\tau(p^k)}$$

$$= \frac{1}{1} + \frac{1}{2} + 0 + \dots + 0$$

$$= \frac{3}{2}.$$

$$G(p^k) = \sum_{d|p^k} \frac{\mu^2(d)}{\sigma(d)} = \frac{\mu^2(1)}{\sigma(1)} + \frac{\mu^2(p)}{\sigma(p)} + \frac{\mu^2(p^2)}{\sigma(p^2)} + \dots + \frac{\mu^2(p^k)}{\sigma(p^k)}$$

$$= \frac{1}{1} + \frac{1}{p+1} + 0 + \dots + 0$$

$$= \frac{p+2}{p+1}.$$

⊗ Let $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$.

$$\Rightarrow \begin{cases} F(n) = F(p_1^{k_1}) F(p_2^{k_2}) \dots F(p_r^{k_r}) = \left(\frac{3}{2}\right)\left(\frac{3}{2}\right)\dots\left(\frac{3}{2}\right) = \left(\frac{3}{2}\right)^r \\ G(n) = G(p_1^{k_1}) G(p_2^{k_2}) \dots G(p_r^{k_r}) = \left(\frac{p_1+2}{p_1+1}\right)\left(\frac{p_2+2}{p_2+1}\right)\dots\left(\frac{p_r+2}{p_r+1}\right) \end{cases}$$

$$\Rightarrow \begin{cases} \sum_{d|n} \frac{\mu^2(d)}{\tau(d)} = \left(\frac{3}{2}\right)^r \\ \sum_{d|n} \frac{\mu^2(d)}{\sigma(d)} = \left(\frac{p_1+2}{p_1+1}\right)\left(\frac{p_2+2}{p_2+1}\right)\dots\left(\frac{p_r+2}{p_r+1}\right) = \left(1+\frac{1}{p_1+1}\right)\left(1+\frac{1}{p_2+1}\right)\dots\left(1+\frac{1}{p_r+1}\right). \end{cases}$$

Sec 6.3

Problem 5(b)

* The ~~no~~ number of trailling zeros depends on the highest power of 10 in its factorization.

$10 = 2 \times 5 \Rightarrow$ It depends on the ~~number~~ power of 2 and 5 in the factorization.

Among the first n integers, powers of 5 is rarer than 2.

$\Rightarrow$ It depends on the power of 5 in the factorization.

* Power of 5 in n! : $\sum_{k=1}^{\infty} \left\lfloor \frac{n}{5^k} \right\rfloor$

$\Rightarrow$ # of trailling zeros in n! : $\sum_{k=1}^{\infty} \left\lfloor \frac{n}{5^k} \right\rfloor$.

* we need to find n such that $\sum_{k=1}^{\infty} \left\lfloor \frac{n}{5^k} \right\rfloor = 37$.

For $n < 150$, we have:

$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{5^k} \right\rfloor < \sum_{k=1}^{\infty} \left\lfloor \frac{150}{5^k} \right\rfloor = \left\lfloor \frac{150}{5} \right\rfloor + \left\lfloor \frac{150}{5^2} \right\rfloor + \left\lfloor \frac{150}{5^3} \right\rfloor + \left\lfloor \frac{150}{5^4} \right\rfloor + \dots$$

$$= 30 + 6 + 1 + 0 + \dots$$

$$= 37$$

$\Rightarrow \sum_{k=1}^{\infty} \left\lfloor \frac{n}{5^k} \right\rfloor < 37$.

$\Rightarrow n < 150$ is not enough.

For $n > 154$, we have:

$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{5^k} \right\rfloor > \sum_{k=1}^{\infty} \left\lfloor \frac{154}{5^k} \right\rfloor = \left\lfloor \frac{154}{5} \right\rfloor + \left\lfloor \frac{154}{5^2} \right\rfloor + \left\lfloor \frac{154}{5^3} \right\rfloor + \left\lfloor \frac{154}{5^4} \right\rfloor + \dots$$

$$= 30 + 6 + 1 + 0 + \dots$$

$$= 37$$

$\Rightarrow \sum_{k=1}^{\infty} \left\lfloor \frac{n}{5^k} \right\rfloor > 37$.

$\Rightarrow n > 154$ has more than 37 zeros.

Thus, for $150 \le n \le 154$, n! has 37 trailling zeros.

Problem 6.

(a) From theorem 6.10, $\binom{2n}{n} = \frac{(2n)!}{n!(2n-n)!} = \frac{(2n)!}{(n!)^2}$ is an integer.

Rewrite it: $\frac{(2n)!}{(n!)^2} = \frac{2n(2n-1)!}{n(n-1)!\,n!} = 2\frac{(2n-1)!}{n!(n-1)!} = 2\binom{2n-1}{n}$.

By theorem 6.10, $\binom{2n-1}{n} \in \mathbb{Z}$.

$\Rightarrow \frac{(2n)!}{(n!)^2}$ is an even integer.

(b) For any prime p, let k be the highest power of p that divides $n!$

Since $n! \mid (2n)!$, $p \mid (2n)!$

Let s be the highest power of p that divides $(2n)!$

$\Rightarrow \frac{p^s}{p^k} = p^{s-k} \Rightarrow s-k$ is the highest power of p dividing $\frac{(2n)!}{n!}$

$\Rightarrow s-2k$ is the highest power of p dividing $\frac{(2n)!}{(n!)^2}$

Note that $s = \sum_{i=1}^{\infty}\left\lfloor\frac{(2n)}{p^i}\right\rfloor$ and $k = \sum_{i=1}^{\infty}\left\lfloor\frac{(n)}{p^i}\right\rfloor$.

Thus, the highest power of p dividing $\frac{(2n)!}{(n!)^2}$ is

$$\sum_{i=1}^{\infty}\left\lfloor\frac{2n}{p^i}\right\rfloor - 2\sum_{i=1}^{\infty}\left\lfloor\frac{n}{p^i}\right\rfloor = \sum_{k=1}^{\infty}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor\right)$$

(c) Since $n < p$, $\frac{n}{p} < 1 \Rightarrow \left\lfloor\frac{n}{p}\right\rfloor = 0$.

$\Rightarrow \left\lfloor\frac{n}{p^k}\right\rfloor = 0$ for $k > 0$.

From (b), the highest power of p is $\sum_{k=1}^{\infty}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor\right)$

$= \sum_{k=1}^{\infty}\left\lfloor\frac{2n}{p^k}\right\rfloor$.

Since $\frac{n}{p} < 1$, $\frac{2n}{p} < 2$.

But $p < 2n \Rightarrow \frac{2n}{p} > 1$

$\Rightarrow 1 < \frac{2n}{p} < 2 \Rightarrow \left\lfloor\frac{2n}{p}\right\rfloor = 1$.

Moreover, $\frac{2n}{p^k} < \frac{2}{p^k} \leq \frac{2}{2^k} < \frac{2}{2} = 1$ for $p \geq 2$ and $k > 1$.

$\Rightarrow \left\lfloor\frac{2n}{p^k}\right\rfloor = 0$ for $k > 1$.

Thus, the highest power of p dividing $\frac{(2n)!}{(n!)^2}$ when $n < p < 2n$ is

$$\sum_{k=1}^{\infty}\left\lfloor\frac{2n}{p^k}\right\rfloor = \left\lfloor\frac{2n}{p}\right\rfloor = 1.$$

Problem 7.

* The highest power of p in $n!$ is

$$\sum_{k=1}^{\infty}\left\lfloor \frac{n}{p^k}\right\rfloor = \left\lfloor a_k p^{k-1} + \dots + a_1 + \frac{a_0}{p}\right\rfloor$$
$$+\left\lfloor a_k p^{k-2} + \dots + \frac{a_1}{p} + \frac{a_0}{p^2}\right\rfloor$$
$$+ \dots$$
$$+\left\lfloor a_k + \dots + \frac{a_1}{p^{k-1}} + \frac{a_0}{p^k}\right\rfloor$$
$$+\left\lfloor \frac{a_k}{p} + \dots + \frac{a_1}{p^k} + \frac{a_0}{p^{k+1}}\right\rfloor. \quad \text{——} (1)$$

* lemma: $(p-1)\left(\frac{1}{p}+\frac{1}{p^2}+\dots+\frac{1}{p^n}\right) < 1$ for $p \geq 2$ and $n \geq 1$

Proof: $(p-1)\left(\frac{1}{p}+\frac{1}{p^2}+\dots+\frac{1}{p^n}\right) = (p-1)\left(\frac{p^{n-1}+p^{n-2}+\dots+1}{p^n}\right)$.

$$= \frac{(p-1)(p^{n-1}+p^{n-2}+\dots+1)}{p^n}$$
$$= \frac{p^n - 1}{p^n}$$
$$= 1 - \frac{1}{p^n} < 1 \text{ for } p \geq 2,\ n \geq 1.$$

* Consider all terms in (1) that is divided by a power of p.

$a_i \leq p-1 \Rightarrow \frac{a_i}{p^k} \leq \frac{p-1}{p^k} \Rightarrow \sum \frac{a_i}{p^k} \leq (p-1)\sum\frac{1}{p^k} < 1$ ($\because$ By lemma).

Thus, all terms in (1) that is divided by a power of p inside the integer notation ($\lfloor\ \rfloor$) will add up to less than 1.

$$\Rightarrow \left\lfloor \frac{a_i}{p^k}\right\rfloor = 0.$$

* Now, (1) becomes:

$$\begin{aligned} &\lfloor a_k p^{k-1} + \dots + a_2 p + a_1 \rfloor \\ &+ \lfloor a_k p^{k-2} + \dots + a_3 p + a_2 \rfloor \\ &+ \dots \\ &+ \lfloor a_k p + a_{k-1} \rfloor \\ &+ \lfloor a_k \rfloor. \end{aligned} = \begin{aligned} &a_k p^{k-1} + \dots + a_2 p + a_1 \\ &+ a_k p^{k-2} + \dots + a_3 p + a_2 \\ &+ \dots \\ &+ a_k p + a_{k-1} \\ &+ a_k \end{aligned}$$

* Note that $\left\lfloor \frac{n}{p^k}\right\rfloor p = a_k p = \left\lfloor \frac{n}{p^{k-1}}\right\rfloor - a_{k-1}$.

Do that recursively, we obtain.

$$\left\lfloor \frac{n}{p} \right\rfloor p = n - a_0$$

$$\left\lfloor \frac{n}{p^2} \right\rfloor p = \left\lfloor \frac{n}{p} \right\rfloor - a_1$$

$$\dots$$

$$+ \quad \left\lfloor \frac{n}{p^{k-1}} \right\rfloor p = \left\lfloor \frac{n}{p^{k-2}} \right\rfloor - a_{k-2}$$

$$\left\lfloor \frac{n}{p^k} \right\rfloor p = \left\lfloor \frac{n}{p^{k-1}} \right\rfloor - a_{k-1}$$

$$0 = \left\lfloor \frac{n}{p^k} \right\rfloor - a_k$$

$$\left(\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \dots + \left\lfloor \frac{n}{p^k} \right\rfloor \right) p = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \dots + \left\lfloor \frac{n}{p^k} \right\rfloor + n - (a_0 + a_1 + \dots + a_k).$$

$$\Rightarrow \left(\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \dots + \left\lfloor \frac{n}{p^k} \right\rfloor \right)(p-1) = n - (a_0 + a_1 + \dots + a_k)$$

$$\Rightarrow \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \frac{n - (a_0 + a_1 + \dots + a_k)}{p-1}.$$

Therefore, the highest power of p in $n!$ is:

$$\frac{n - (a_0 + a_1 + \dots + a_k)}{p-1}$$