Sol VIPGCD

Time Limit: 2.0s **Memory Limit:** 977M

Vì lời giải của bài này khá dài nên mình mong các bạn kiên trì để hiểu hơn bài toán này nhé

Mình sẽ chia lời giải gồm 2 phần:

- **Phần 1:** Gồm những định nghĩa, công thức và những bổ để cần dùng (kèm theo chứng minh)
- **Phần 2:** Ta sẽ áp dụng Phần 1 để giải quyết bài toán đề ra.

Phần 1: Định nghĩa, công thức và những bổ để cần dùng (kèm theo chứng minh)

- Ta định nghĩa $[P] = 1$ nếu $P = true$ và $[P] = 0$ nếu $P = false$. (P được hiểu ở đây là một mệnh đề) $\rightarrow (I)$

  Xét một số nguyên dương n phân tích ra thừa số sẽ có dạng $p_1^{a_1}.p_2^{a_2}.p_3^{a_3}...p_r^{a_r}$ với $p_i (1 \leq i \leq r)$ là các số nguyên tố.

Khi đó ta có các hàm số học kinh điển sau:

- Hàm Mobius $\mu(n)$:
  - $\mu(n) = 1$
  - $\mu(n) = 0$ nếu tồn tại $a_i > 1$
  - $\mu(n) = (-1)^r$ nếu $n = p_1.p_2....p_r$ hay $a_i = 1$ với mọi $i = \overline{1,r}$
- Hàm Phi Ơ-le (Euler's totient function):
  - $\phi(n)$ là số lượng số nguyên tố cùng nhau với N trong đoạn từ 1 đến N
- Công thức nghịch đảo Mobius (Mobius's inversion formula):
  - $\forall n \geq 1, g(n) = \sum_{d|n} f(d) \implies f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d})$
- **Bổ đề 1:** $\sum_{d|n} \phi(d) = n$

Chứng minh:

Kí hiệu: $S = \{1, 2, \ldots, n\}$

$\rightarrow$ Bây giờ ta sẽ phân hoạch tập S này thành các tập như sau:

- Với mỗi d là ước của n, đặt $A(d) = \{k \in S : gcd(k, n) = d\}$

Khi đó ta có một nhận xét như sau:

- $A(p) \cap A(q) = \emptyset$ với mọi $p \neq q$ và p, q lần lượt là các ước của n
- $\bigcup_{d|n} A(d) = S$

Nên từ đây ta suy ra được:

- $\sum_{d|n} |A(d)| = |S| = n$ (trong đó $|X|$ - kí hiệu số lượng phần tử của tập X) $\rightarrow (II)$

Bây giờ ta sẽ đi tìm $|A(d)|$.

Ta sẽ đi chứng minh: $|A(d)| = \phi(\frac{n}{d})$

Thật vật, ta có: $A(d) = \{k \in S : gcd(k, n) = d\} \iff A(d) = \left\{k \in S : gcd(\frac{k}{d}, \frac{n}{d}) = 1\right\}$

Đặt $z = \frac{k}{d}$ khi đó ta có $1 \leq z \leq \frac{n}{d}$ (Vì $1 \leq k \leq n$)

Do đó $|A(d)|$ chính bằng số lượng số $z \in [1; \frac{n}{d}]$ và z nguyên tố cùng nhau với $\frac{n}{d}$

Nên từ đây ta suy ra được: $|A(d)| = \phi(\frac{n}{d})$ (Theo định nghĩa của hàm Phi Ơ-le)

Từ (II) ta suy ra được: $n = \sum\limits_{d|n} |A(d)| = \sum\limits_{d|n} \phi(\frac{n}{d}) = \sum\limits_{d|n} \phi(d)$

Ps: Mình xin giải thích một chút vì sao : $\sum\limits_{d|n} \phi(\frac{n}{d}) = \sum\limits_{d|n} \phi(d)$? .

Đáp: Là bởi cả hai vế trái và phải chính bằng tổng các Phi Ơ-le của tất cả các ước của n

Như vậy là **bổ đề 1** đã chứng minh hoàn tất !

- **Bổ đề 2:** $[n = 1] = \sum\limits_{d|n} \mu(d)$

Chứng minh:

- Với $n = 1$, theo (I) ta có: $[n = 1] = 1$ và $\sum\limits_{d|1} \mu(d) = \mu(1) = 1$ Do đó **bổ đề 2** hiển nhiên đúng vì cả vế trái và phải đều cùng bằng 1
- Với $n > 1$, ta có $[n = 1] = 0$, do đó ta chỉ cần đi chứng minh $\sum\limits_{d|n} \mu(d) = 0$ là bài toán được giải quyết !

Thật vậy: Ta có: $n = p_1^{a_1}.\, p_2^{a_2}.\, p_3^{a_3} \ldots p_r^{a_r}$ với p_i là các số nguyên tố.

Khi đó xét một ước z bất kì của n sẽ thuộc một trong hai dạng sau:

- **Dạng 1:** $z = p_\beta^\gamma.\, Q(Q \in \mathbb{N}^*)$ với $\beta \in \{1, 2, \ldots, r\}$ và $\gamma \geq 2$. Khi đó $\mu(z) = 0$ (theo định nghĩa của hàm Mobius)
- **Dạng 2:** z không thuộc **Dạng 1**, tức là z sẽ là ước của $n' = p_1 p_2 \ldots p_r$.

Khi đó, ta có:
$\sum\limits_{d|n} \mu(d) = \sum\limits_{d|n'} \mu(d) = \mu(1) + \sum\limits_{1 \leq i \leq r} \mu(p_i) + \sum\limits_{1 \leq i < j \leq r} \mu(p_i p_j) + \ldots + \mu(p_1 p_2 \ldots p_r) = \binom{r}{0} 1^r (-1)^0 + \binom{r}{1} 1^{r-1} (-1)^1 + \ldots + \binom{r}{r} 1^0 (-1)^r = (1-1)^0 = 0$
(Theo nhị thức Newton)

Như vậy việc chứng minh **bổ đề 2** của ta đã hoàn tất!

- **Bổ đề 3:** $\sum\limits_{d|n} d\mu(\frac{n}{d}) = \phi(n)$

Theo **bổ đề 1**, ta có: $n = \sum\limits_{d|n} \phi(d)$, nên áp dụng công thức nghịch đảo mobius, trong đó: $g(n) = n$ và $f(n) = \phi(n)$, ta có:

Vì: $g(n) = \sum\limits_{d|n} f(d) \implies f(n) = \sum\limits_{d|n} \mu(d) g(\frac{n}{d})$

Hay ta có: $\phi(n) = \sum\limits_{d|n} \mu(d).\, \frac{n}{d} = \sum\limits_{d|n} d\mu(\frac{n}{d})$

Như vậy là **bổ để 3** đã được chứng minh hoàn tất.

Chúng ta kết thúc phần 1, và chuyển sang phần 2. Sẽ còn nhiều phần hấp dẫn ở phần 2, các bạn tiếp tục đón xem nhé !

Phần 2: Giải quyết bài toán ban đầu.

Ta có: $S = \sum\limits_{i=1}^{n} gcd(\lfloor \sqrt[3]{i} \rfloor, i) = \sum\limits_{a=1}^{\lfloor \sqrt[3]{n} \rfloor} \sum\limits_{i=1}^{n} gcd(a, i).\, [\lfloor \sqrt[3]{i} \rfloor = a] \rightarrow (III)$

Ta có: $\lfloor \sqrt[3]{i} \rfloor = a \iff a \leq \sqrt[3]{i} < a + 1 \iff a^3 \leq i \leq (a+1)^3 - 1 \implies [\lfloor \sqrt[3]{i} \rfloor = a] = 1 \iff a^3 \leq i \leq (a+1)^3 - 1$

Do đó ta suy ra được: $\sum\limits_{i=1}^{n} gcd(a, i)[\lfloor \sqrt[3]{i} \rfloor = a] = \sum\limits_{i=a^3}^{min\left\{n, (a+1)^3 - 1\right\}} gcd(a, i)$

Đặt $r = \lfloor \sqrt[3]{n} \rfloor - 1$

Khi đó, từ (III) ta suy ra được: $S = \sum\limits_{a=1}^{\lfloor \sqrt[3]{n} \rfloor} \sum\limits_{i=a^3}^{min\left\{n, (a+1)^3 - 1\right\}} gcd(a, i) = S_1 + S_2$, trong đó:

- $S_1 = \sum_{a=1}^{r} \sum_{i=a^3}^{min\left\{n,(a+1)^3-1\right\}} gcd(a,i)$
- $S_2 = \sum_{a=\lfloor\sqrt[3]{n}\rfloor}^{\lfloor\sqrt[3]{n}\rfloor} \sum_{i=a^3}^{min\left\{n,(a+1)^3-1\right\}} gcd(a,i)$

Tiếp theo, ta có 2 nhận xét quan trọng sau:

- **Nhận xét 1:** $min\left\{n,(a+1)^3-1\right\} = (a+1)^3-1$ với mọi $1 \le a \le r$

(Vì $(a+1)^3-1 \le (r+1)^3-1 = (\lfloor\sqrt[3]{n}\rfloor-1+1)^3-1 = (\lfloor\sqrt[3]{n}\rfloor)^3-1 < n$)

- **Nhận xét 2:** $min\left\{n,(a+1)^3-1\right\} = n$ với mọi $a = \lfloor\sqrt[3]{n}\rfloor$

(Vì ta có: $(a+1)^3 = (\lfloor\sqrt[3]{n}\rfloor+1)^3 \ge n+1 \implies (a+1)^3-1 \ge n$)

Từ đây ta suy ra được:

- $S_1 = \sum_{a=1}^{r} \sum_{i=a^3}^{min\left\{n,(a+1)^3-1\right\}} gcd(a,i) = \sum_{a=1}^{r} \sum_{i=a^3}^{(a+1)^3-1} gcd(a,i)$
- $S_2 = \sum_{a=\lfloor\sqrt[3]{n}\rfloor}^{\lfloor\sqrt[3]{n}\rfloor} \sum_{i=a^3}^{n} gcd(a,i) = \sum_{i=(\lfloor\sqrt[3]{n}\rfloor)^3}^{n} gcd(\lfloor\sqrt[3]{n}\rfloor, i)$

Để tính được S_1, S_2, ta đi xét một bài toán sau, đó chính là tính: $Q = \sum_{i=1}^{n} gcd(a,i)$

Việc tính Q được thực hiện như sau:

- Ta có: $Q = \sum_{d} d \sum_{i=1}^{n} [gcd(a,i) = d] = \sum_{d} d \sum_{i=1}^{n} [gcd(\frac{a}{d}, \frac{i}{d}) = 1]$

Đến đây áp dụng **bổ đề 2** ở **phần 1** ta có: $Q = \sum_{d} d \sum_{i=1}^{n} \sum_{t|gcd(\frac{a}{d},\frac{i}{d})} \mu(t)$

Hay $Q = \sum_{d} d \sum_{i=1}^{n} \sum_{t|\frac{a}{d}, t|\frac{i}{d}} \mu(t)$ = $\sum_{T|a} \left\lfloor \frac{n}{T} \right\rfloor \sum_{d|T} d\mu(\frac{T}{d}) \to (IV)$

▶ **Để giúp các bạn dễ hình dung được, vì sao ta có được phép biến đổi (IV) này, mình sẽ lấy một ví dụ cụ thể như sau: (các bạn kích vào mũi tên)**

Đến đây, ta lại tiếp tục áp dụng **bổ đề 3** ở **phần 1** ta được:

$Q = \sum_{T|a} \left\lfloor \frac{n}{T} \right\rfloor \phi(T)$

Hay $Q = \sum_{i=1}^{n} gcd(a,i) = \sum_{T|a} \left\lfloor \frac{n}{T} \right\rfloor \phi(T) \to (V)$

Mình nghĩ đây là một kết quả quan trọng và áp dụng được vào trong nhiều bài tương tự, các bạn nhớ lưu tâm chỗ này nhé !

- Bây giờ ta sẽ áp dụng kết quả (V) này để tính S_1, S_2 . Các bạn tiếp tục đón xem nhé !

Việc tính toán S_2 hoàn toàn tương tự S_1, nên mình chỉ trình bày phần S_1 nhé, còn S_2 dành cho các bạn đọc nhé !

Phần tính toán S_1 như sau:

Ta có: $S_1 = \sum_{a=1}^{r} \sum_{a^3}^{(a+1)^3-1} gcd(a,i) = \sum_{a=1}^{r} \sum_{T|a} (\left\lfloor \frac{(a+1)^3-1}{T} \right\rfloor - \left\lfloor \frac{a^3-1}{T} \right\rfloor)\phi(T)$

Đặt $a = bT (b \in \mathbb{N}^*)$

$$\implies S_1 = \sum_{bT=1}^{r} \sum_{T|bT} (\left\lfloor \frac{(bT+1)^3-1}{T} \right\rfloor - \left\lfloor \frac{(bT)^3-1}{T} \right\rfloor)\phi(T)$$

$$= \sum_T \phi(T) \sum_{b=1}^{\left\lfloor \frac{r}{T} \right\rfloor} \left(\left\lfloor \frac{(bT+1)^3-1}{T} \right\rfloor - \left\lfloor \frac{(bT)^3-1}{T} \right\rfloor \right) \phi(T)$$

Để hiểu được vì sao có phép biến đổi này, các bạn cứ nháp từng ví dụ nhỏ ra là thấy nhé, phần này mình xin dành cho bạn đọc:

Mặt khác ta lại có: $\left\lfloor \frac{(bT+1)^3-1}{T} \right\rfloor - \left\lfloor \frac{(bT)^3-1}{T} \right\rfloor = \lfloor b^3T^2 + 3b^2T + 3b \rfloor - \lfloor b^3T^2 - \frac{1}{T} \rfloor$

$= (b^3T^2 + 3b^2T + 3b) - (b^3T^2 - 1) = 3b^2T + 3b + 1$

Nên từ đây ta suy ra được: $S_1 = \sum_{T=1}^{r} \phi(T)[(3T \sum_{b=1}^{\left\lfloor \frac{r}{T} \right\rfloor} b^2) + (3 \sum_{b=1}^{\left\lfloor \frac{r}{T} \right\rfloor} b) + \lfloor \frac{r}{T} \rfloor]$

Đến đây, ta áp dụng thêm 2 đẳng thức quen thuộc: $\sum_{i=1}^{q} i^2 = \frac{q(q+1)(2q+1)}{6}$ và $\sum_{i=1}^{q} i = \frac{q(q+1)}{2}$ nữa là S_1 đã được giải quyết hoàn tất.

Như vậy là bài toán đã giải quyết xong.

$\rightarrow$ **Tiếp theo là đến phần code**.

- Ta nhận thấy rằng, khi đã tìm được công thức, để phần code được tối ưu, chúng ta nên tính trước các giá trị của hàm Phi - Ơ le và biểu thức Q.
- Về phần xử lý mod, các bạn chú ý tính trước các giá trị $6^{-1}\%998244353$ và $2^{-1}\%998244353$ (Để tính được cái này các bạn dùng Inverse mod và luỹ thừa nhị phân nhé)
- Độ phức tạp của bài này là $O(r) \sim O(\sqrt[3]{n}) \sim 10^7$.

Như vậy là solution cho bài toán đã hoàn tất, mình hy vọng qua bài này, các bạn học thêm được một chút gì đó và rất cảm ơn tất cả các bạn đọc hết phần solution này !