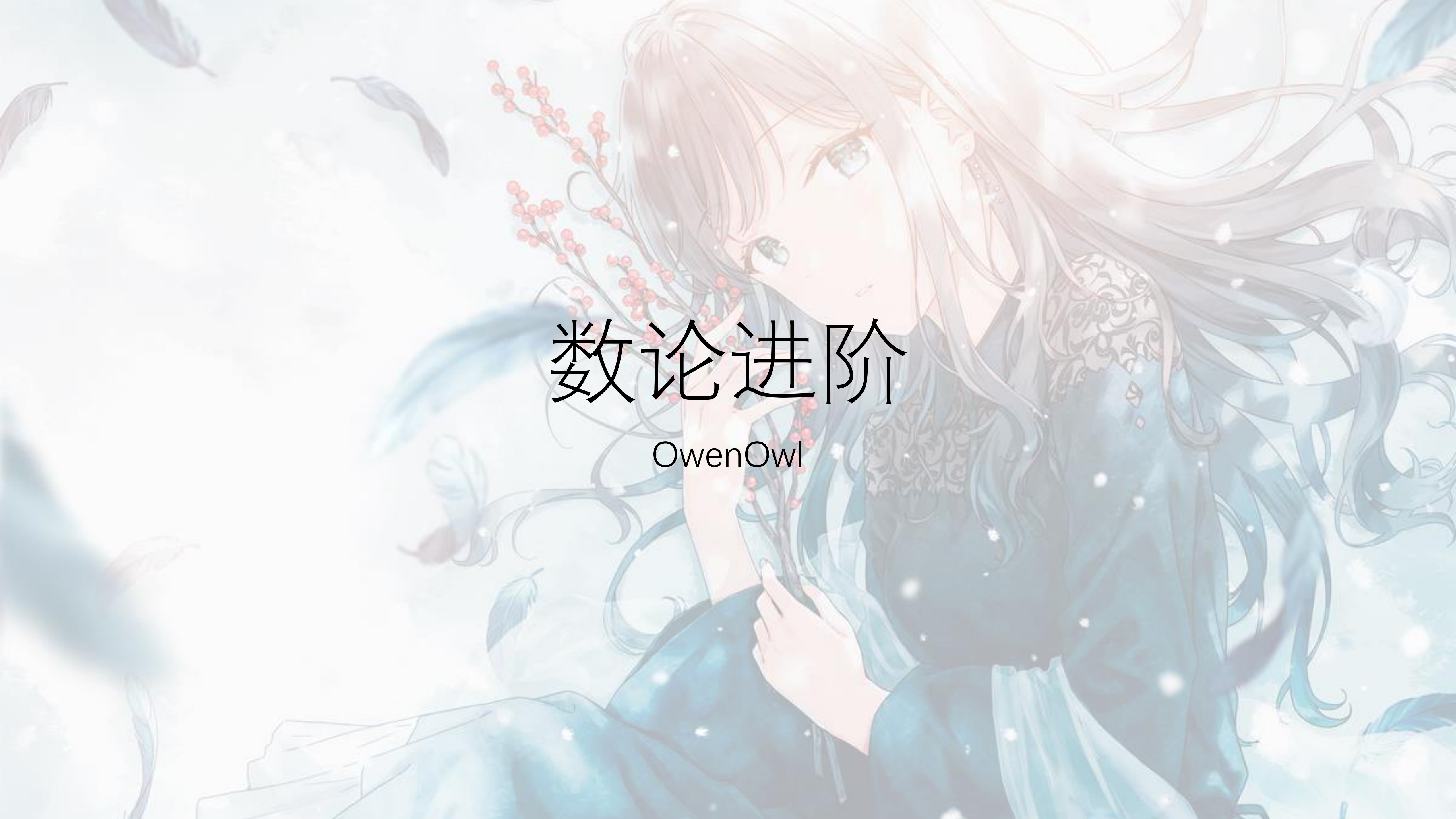
数论进阶

OwenOwl



莫比乌斯函数

$$\mu(n)=\begin{cases}0 & \exists p, p^2 \mid n\\(-1)^r & n=p_1p_2\dots p_r\end{cases}$$

- 即有平方因子时为 0，否则奇数个质因子为 -1，偶数个质因子为 1。

莫比乌斯函数

- 莫比乌斯函数可用于约数相关的容斥，下面用一道例题说明。

完全平方数

- 求 1 到 n 有多少个数无平方因子。
- $n \le 10^{14}$。

完全平方数

- 容斥原理，用总的，减去有一个质数的平方的，加上有两个质数的平方的，再减去有三个质数的平方的……

$$n-\sum_{p\in\mathbb{P}}\left\lfloor\frac{n}{p^2}\right\rfloor+\sum_{p_1,p_2\in\mathbb{P}}\left\lfloor\frac{n}{p_1^2p_2^2}\right\rfloor-\cdots$$

- 即

$$\sum_{x\geq 1}\mu(x)\left\lfloor\frac{n}{x^2}\right\rfloor$$

- 复杂度 $O(\sqrt{n})$。

莫比乌斯函数

- 也可以使用线性筛求 1 到 n 的值。
- 对于质数 p，$\mu(p) = -1$；
- 对于 $px, p \nmid x$，$\mu(px) = -\mu(x)$；
- 对于 $px, p \mid x$，$\mu(px) = 0$。

数论函数

- 定义域为正整数的函数称为数论函数。
- 对于数论函数 f，若任意互质的 p,q 都有 $f(pq)=f(p)f(q)$，则称 f 是积性函数。
- 对于数论函数 f，若任意 p,q 都有 $f(pq)=f(p)f(q)$，则称 f 是完全积性函数。

数论函数

- 常见积性函数：
- 除数函数 $\sigma_k(n)$： n 的所有约数的 k 次方和；
- 欧拉函数 $\varphi(n)$：不超过 n 的与 n 互质的数的个数；
- 莫比乌斯函数 $\mu(n)$。

数论函数

- 常见完全积性函数：
- 1 函数 $1(n) = 1$；
- 元函数 $\varepsilon(n) = [n = 1]$；
- 幂函数 $I^k(n) = n^k$。

欧拉筛

- 欧拉筛可以用于处理 $i = 1 \sim n$ 的所有 $f(i)$ 的值。
- 显然当 $p \nmid x$ 时，$f(px) = f(p)f(x)$。
- 而当 $p \mid x$ 时，有可能不像 φ, μ 那样有简洁的式子，因此可以假设 $px = p^r y \, (p \nmid y)$，这样 $f(px) = f(p^r)f(y)$。
- 但是当 $y = 1$ 的时候也不能这样求，也就是说此种情形下所有 $f(p^r)$ 都需要用定义直接求值。

欧拉筛

- 例如可以欧拉筛预处理 $I^k(n)$ 在 $1 \sim n$ 的值。
- 非质数处可以使用 $f(px) = f(p)f(x)$ 求值。
- 质数处直接使用快速幂求值。
- 由于 n 以内质数大约 $O\left(\frac{n}{\ln n}\right)$ 个，因此复杂度是 $O\left(n + \frac{n \log k}{\ln n}\right)$，一般情况下可以近似认为是 $O(n)$。

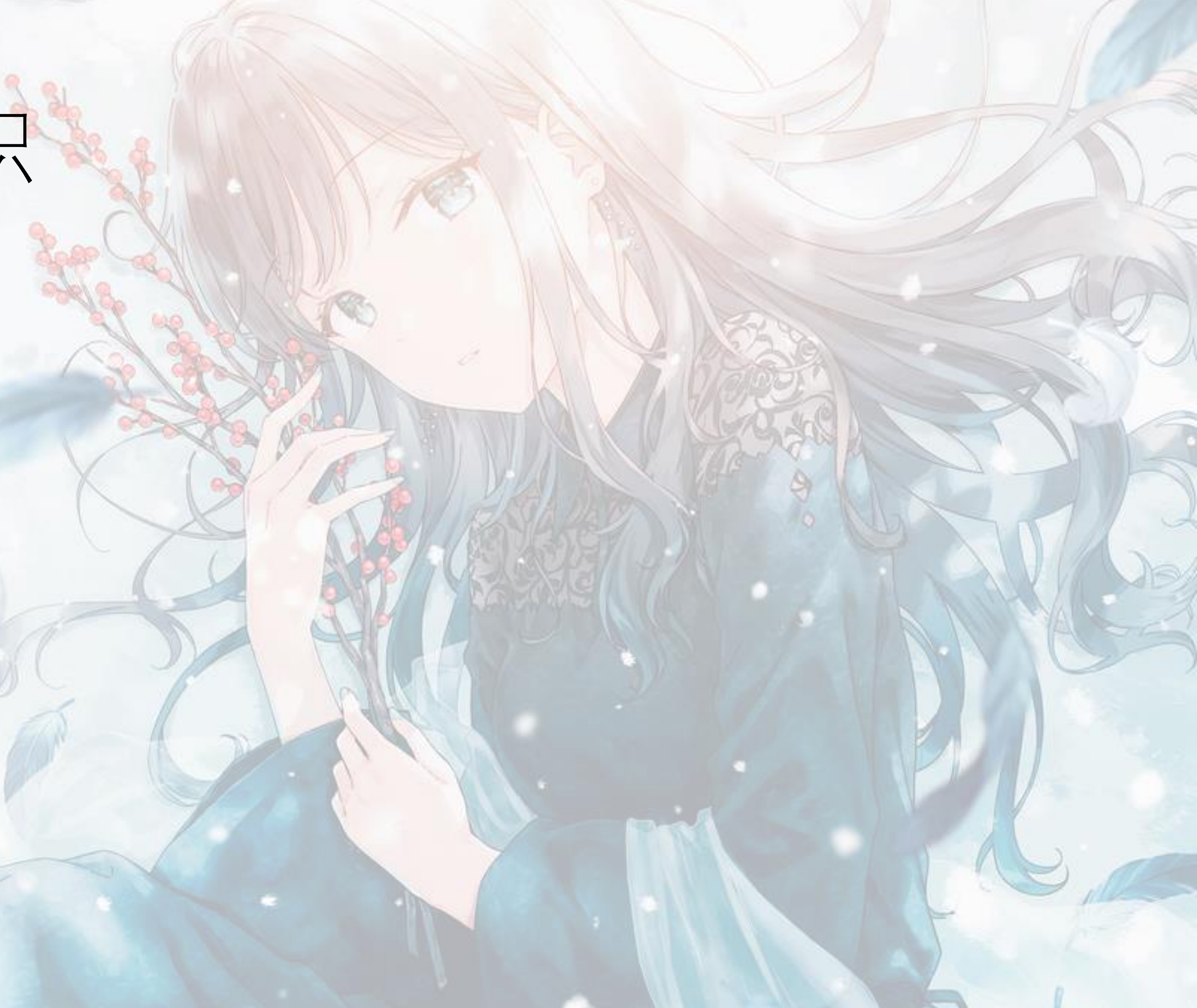
狄利克雷卷积

$$h(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

- 记作 $h = f \otimes g$。
- 若 f,g 是积性函数，则 h 也是积性函数。

狄利克雷卷积

- 常见卷积恒等式:
- $\mu \otimes 1 = \varepsilon$
- $\varphi \otimes 1 = I$
- $\mu \otimes I = \varphi$
- $1 \otimes 1 = \sigma_0$
- $1 \otimes I^k = \sigma_k$



狄利克雷卷积

- 对于上面的积性函数，可以表达为狄利克雷生成函数的形式，能更直观地解释一些积性函数之间的关系。有兴趣的同学可以自行搜索学习。

莫比乌斯反演

- 对于给定的数论函数 f, g

$$f(n) = \sum_{d|n} g(d) \Leftrightarrow g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$$

- 即

$$f = g \otimes 1 \Leftrightarrow g = f \otimes \mu$$

莫比乌斯反演

- 子集反演也可以得到莫比乌斯反演。
- 把正整数的质因子看做多重集合，不仅可以得到上式，还可以通过超集形式得到一组倍数求和的形式。

$$f(i)=\sum_{i|j}^{n} g(j) \Leftrightarrow g(i)=\sum_{i|j}^{n} \mu\left(\frac{j}{i}\right) f(j)$$

字符串计数

- 求字符集为 m，长为 n 且不存在小于 n 的循环节的字符串个数。
- $m,n \leq 10^9$。

字符串计数

- 设长为 i 的答案为 f_i。由于一个串一定是由一个没有循环节的子串循环得来的，所以

$$m^n = \sum_{d|n} f_d$$

- 反演就得到

$$f_n = \sum_{d|n} \mu\left(\frac{n}{d}\right) m^d$$

莫比乌斯反演

- 一般与积性函数和相关的题目被称为反演题，但反演题不一定用到反演。
- 这类题目特征明显，熟练掌握套路应用下面这两个公式即可。
- $\sum_{d|n}\varphi(d)=n$
- $\sum_{d|n}\mu(d)=[n=1]$
- 下面几个例题。

最大公约数求和

- T 次给出 m,n，求

$$\sum_{i=1}^{m}\sum_{j=1}^{n}\gcd(i,j)$$

- $T \le 10^4$，$m,n \le 10^6$。

最大公约数求和

- 代入 $\sum_{d|n} \varphi(d) = n$ 把 $\gcd(i,j)$ 替换掉，得到
- $\sum_{i=1}^{m} \sum_{j=1}^{n} \sum_{d|\gcd(i,j)} \varphi(d)$
- $= \sum_{d} \varphi(d) \sum_{d|i}^{m} \sum_{d|j}^{n} 1$
- $= \sum_{d} \varphi(d) \left\lfloor \frac{m}{d} \right\rfloor \left\lfloor \frac{n}{d} \right\rfloor$
- 这样单词询问就是 $O(n)$ 的。

最大公约数求和

- 接下来应用到另一个结论：$\left\lfloor \frac{n}{d} \right\rfloor$ 只有 $O(\sqrt{n})$ 种取值。
- 因此可以求 φ 的前缀和后，对 $\left\lfloor \frac{n}{d} \right\rfloor$ 相同的一段一并处理。
- 已知 l，如何找到与 $\left\lfloor \frac{n}{l} \right\rfloor$ 相同的一段的右端点 r?
- $\left\lfloor \frac{n}{l} \right\rfloor = \left\lfloor \frac{n}{r} \right\rfloor \le \frac{n}{r}$
- 因此有 $r \le \frac{n}{\left\lfloor \frac{n}{l} \right\rfloor}$，即 $r = \left\lfloor \frac{n}{\left\lfloor \frac{n}{l} \right\rfloor} \right\rfloor$。
- 该做法称作“整除分块”。

最大公约数计数

- T 组询问，每次给出 m,n,k，求
$$\sum_{i=1}^{m}\sum_{j=1}^{n}[\gcd(i,j)=k]$$
- $T \le 10^4$，$m,n,k \le 10^6$。

最大公约数计数

- 考虑到是 $[n=1]$ 的形式，代入 $\sum_{d|n}\mu(d)=[n=1]$ 替换 $\left[\frac{\gcd(i,j)}{k}=1\right]$。
- $\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{d|\frac{\gcd(i,j)}{k}}\mu(d)$
- $\sum_{d}\mu(d)\sum_{kd|i}^{m}\sum_{kd|j}^{n}1$
- $\sum_{d}\mu(d)\left\lfloor\frac{m}{kd}\right\rfloor\left\lfloor\frac{n}{kd}\right\rfloor$
- 注意到 $\left\lfloor\frac{m}{kd}\right\rfloor=\left\lfloor\frac{\left\lfloor\frac{m}{k}\right\rfloor}{d}\right\rfloor$，因此和上题一样做法。

JZPTAB

- T 次给出 m,n 求

$$\sum_{i=1}^{m}\sum_{j=1}^{n}\operatorname{lcm}(i,j)$$

- $T \le 10^4$， $m,n \le 10^6$。

JZPTAB

- $\operatorname{lcm}(i,j)=\frac{ij}{k}[\gcd(i,j)=k]$ 用这个进行替换
- $\sum_k \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{ij}{k} \sum_{d\mid\frac{\gcd(i,j)}{k}} \mu(d)$
- $=\sum_k \sum_d \mu(d) \sum_{kd\mid i}^{m} \sum_{kd\mid j}^{n} \frac{ij}{k}$
- $=\sum_k k \sum_d d^2 \mu(d) \sum_{i=1}^{\left\lfloor\frac{m}{kd}\right\rfloor} i \sum_{j=1}^{\left\lfloor\frac{n}{kd}\right\rfloor} j$

JZPTAB

- 替换一下参数，设 $t = kd$，原式变成
- $\sum_t t \sum_{d|t} d\mu(d) \sum_{i=1}^{\left\lfloor\frac{m}{t}\right\rfloor} i \sum_{j=1}^{\left\lfloor\frac{m}{t}\right\rfloor} j$
- 其中，$t \sum_{d|t} d\mu(d)$ 是积性函数（积性函数的点积和狄利克雷卷积都是积性函数），线性筛预处理。
- 后面是关于 $\left\lfloor\frac{m}{t}\right\rfloor$ 的等差数列求和，因此也照搬前几题套路即可。

SDOI 2014：数表

- T 次给出 m, n, a 求

$$\sum_{i=1}^{m}\sum_{j=1}^{n}\sigma_1(\gcd(i,j))[\sigma_1(\gcd(i,j)) \le a]$$

- $T \le 2 \times 10^4$，$m, n \le 10^5$，$a \le 10^9$。

SDOI 2014：数表

- 先不考虑 $\le a$ 的限制，枚举 $\gcd(i,j)=k$ 继续套。
- $\sum_k \sigma_1(k) \sum_{i=1}^{m} \sum_{j=1}^{n} [\gcd(i,j)=k]$
- $= \sum_d \mu(d) \sum_k \sigma_1(k) \sum_{kd|i}^{m} \sum_{kd|j}^{n} 1$
- $= \sum_t \sum_{d|t} \mu(d) \sigma_1\left(\frac{t}{d}\right) \left\lfloor\frac{m}{t}\right\rfloor \left\lfloor\frac{n}{t}\right\rfloor$
- 后面部分套路处理。现在有了 a 的限制，因此考虑离线把 σ_1 从小到大加进去。观察式子发现加入 $\sigma_1(i)$ 的时候，所有 i 的倍数的函数值都要修改。而查询因为要查区间和，可以树状数组维护。
- 复杂度 $O(T\sqrt{n}\lg n + n\ln n\lg n)$。

BZOJ 3309： DZY Loves Math

- 定义 $f(n)$ 表示 n 所含因子的最大幂指数，例如
- $f(2^3 \times 5 \times 7^2) = 3$，$f(1) = 0$。
- T 次询问，每次给定 m, n，求

$$\sum_{i=1}^{m} \sum_{j=1}^{n} f(\gcd(i, j))$$

- $T \le 10^4$，$m, n \le 10^7$。

BZOJ 3309： DZY Loves Math

- 还是大力枚举 $\gcd(i,j)$ 然后展开。
- $\sum_t \left\lfloor\frac{m}{t}\right\rfloor \left\lfloor\frac{n}{t}\right\rfloor \sum_{d|t} f(d)\mu\left(\frac{t}{d}\right)$
- 令 $g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right)$，现在的问题就是快速预处理这个。

BZOJ 3309：DZY Loves Math

- 只需要考虑 $\mu\left(\frac{n}{d}\right)$ 不为 0 的项，这样 $f(d)$ 里每个质因子最多被拿走一个幂次。假设 $n=\sum_{i=1}^{l} p_i^{r_i}$，其中最大的 r_i 是 r_0。
- 如果存在 $r_j \neq r_0$，那么一对 $f(d)$ 和 $f\left(\frac{d}{p_j}\right)$ 一定相同都为 r_0 或者 r_0-1。而对应的 μ 一定恰为 ± 1，因此总和就为 0。
- 而如果所以 r 相等，那么除了所有质因子都被拿走一个幂次之外其余的 f 均为 r，为 $r-1$ 处的系数是 $(-1)^l$。因此总和就是 $(-1)^{l+1}$。

BZOJ 3601：一个人的数论

- 给定 n,k，求小于等于 n 的所有与 n 互质的数的 k 次方和。
- n 以 $\sum_{i=1}^{m} p_i^{r_i}$ 的形式给出。
- $m \leq 1000$，$p_i, r_i \leq 10^9$，$k \leq 100$。

BZOJ 3601：一个人的数论

- 容斥原理，答案是 $\sum_{d|n}\mu(d)d^k\sum_{i=1}^{\frac{n}{d}} i^k$。
- 幂和是 $k+1$ 次多项式，插值求出其系数 $\sum_{i=1}^{n} i^k=\sum_{i=0}^{k+1} a_i n^i$。
- 原式就转化为 $\sum_{i=0}^{k+1} a_i \sum_{d|n}\mu(d)d^k\left(\frac{n}{d}\right)^i$。
- 后半部分是积性函数的狄利克雷卷积，还是积性函数，因此每个质数单独算就行了。

51Nod 1222：最小公倍数计数

- 求

$$\sum_{i\le j}[\mathrm{lcm}(i,j)\le n]$$

- $n \le 10^{11}$

51Nod 1222：最小公倍数计数

- 去掉 $i \le j$ 的条件最后处理。
- $\sum_{i=1}^{n}\sum_{j=1}^{n}\left[\frac{ij}{\gcd(i,j)} \le n\right]$
- $= \sum_{d^2 \le n}\mu(d)\sum_{i,j,k \le \frac{n}{d^2}}\left[ijk \le \frac{n}{d^2}\right]$
- 关键在于后一个求和怎么处理。对于 $ijk \le n$ 不妨假设 $i < j < k$，因此 $i \le n^{\frac{1}{3}}$，$j \le \sqrt{\frac{n}{i}}$，k 的方案数可以直接计算。最后答案再乘上排列数就行了。注意谨慎处理有等号的情况。

51Nod 1222：最小公倍数计数

- 复杂度用积分近似（可略去不看）：
- $T(n)=\int_1^{\sqrt{n}}\mathrm{d}x\int_1^{\left(\frac{n}{x^2}\right)^{\frac{1}{3}}}\sqrt{\frac{n}{x^2y}}\,\mathrm{d}y=\mathrm{O}\left(n^{\frac{2}{3}}\right)$

杜教筛

- 设有数论函数 f,g,h，其中 $h=f\otimes g$，如果要求 f 的前缀和 F，而 g,h 的前缀和 G,H 简单好求，可以使用杜教筛。

杜教筛

- $H(n)=\sum_{i=1}^{n}\sum_{j|i}f(j)g\left(\frac{i}{j}\right)$
- $=\sum_{i=1}^{n}g(i)\sum_{j=1}^{\left\lfloor\frac{n}{i}\right\rfloor}f(j)$
- $=\sum_{i=1}^{n}g(i)F\left(\left\lfloor\frac{n}{i}\right\rfloor\right)$
- $=g(1)F(n)+\sum_{i=2}^{n}g(i)F\left(\left\lfloor\frac{n}{i}\right\rfloor\right)$
- 把 $F(n)$ 移到一边就可以得到表达式
- $F(n)=\frac{H(n)-\sum_{i=2}^{n}g(i)F\left(\left\lfloor\frac{n}{i}\right\rfloor\right)}{g(1)}$

杜教筛

- 这个式子每次需要花费 $O(\sqrt{n})$ 的时间整除分块，而且需要递归计算到所有的 $F\left(\left\lfloor\frac{n}{i}\right\rfloor\right)$，总复杂度也可近似积分
- $O\left(\int_1^{\sqrt{n}}\sqrt{i}+\sqrt{\frac{n}{i}}\mathrm{d}i\right)=O\left(n^{\frac{3}{4}}\right)$
- 如果使用线性筛，预处理 F 的前 $n^{\frac{2}{3}}$ 项，复杂度就降为了 $O\left(n^{\frac{2}{3}}\right)$。具体预处理多少项需要根据具体问题和代码的常数分析。

梅滕斯函数

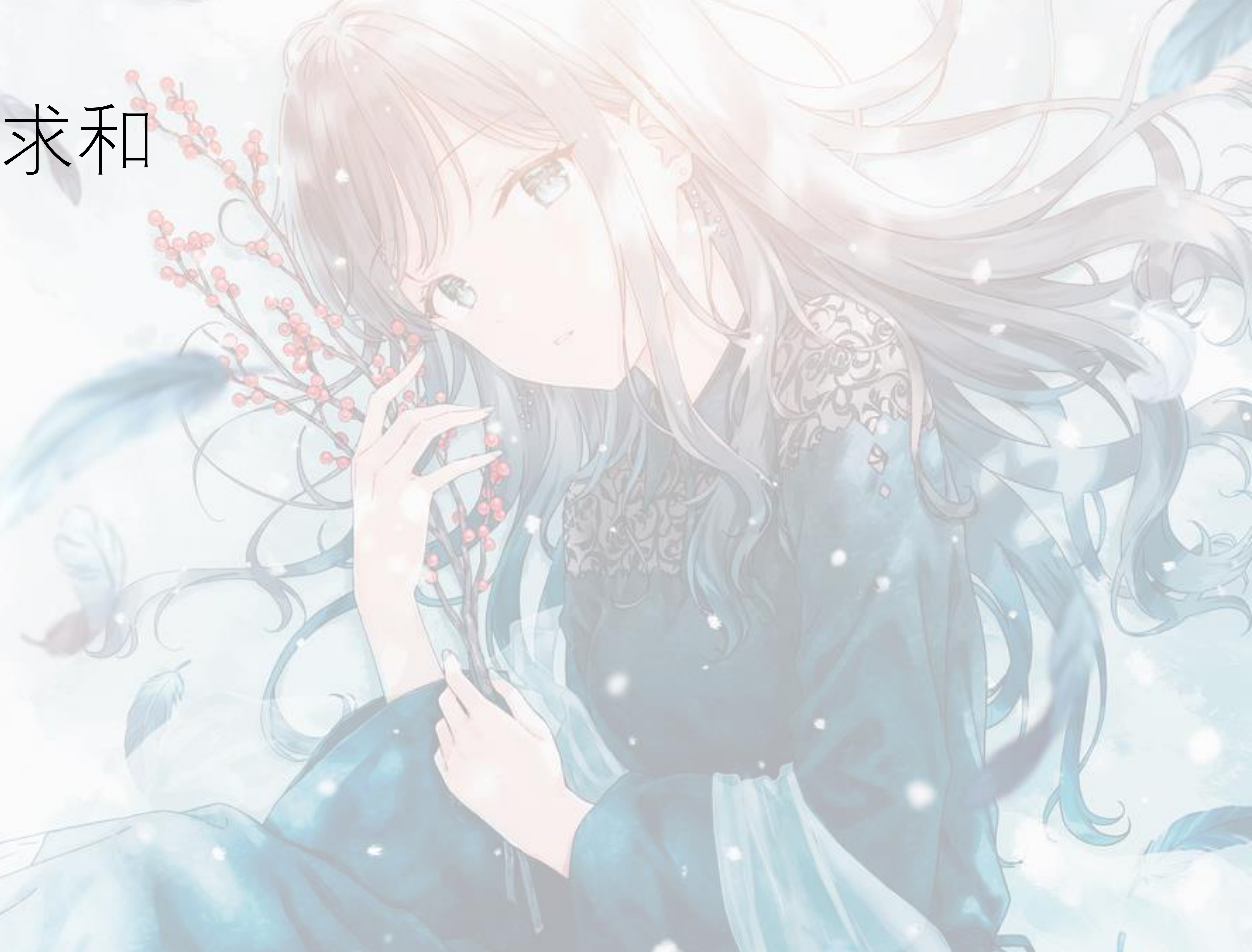
- 求 $\mathrm{M}(n)=\sum_{i=1}^{n}\mu(i)$
- $n\le 10^{10}$

梅滕斯函数

- 如果令 $f=\mu$，取 $g=1$，那么 $h=f\otimes g=\varepsilon$。
- 代入杜教筛式子可得
- $\mathrm{M}(n)=\mathrm{E}(n)-\sum_{i=2}^{n}\mathrm{M}\left(\left\lfloor\frac{n}{i}\right\rfloor\right)=1-\sum_{i=2}^{n}\mathrm{M}\left(\left\lfloor\frac{n}{i}\right\rfloor\right)$
- $\mathrm{O}\left(n^{\frac{2}{3}}\right)$

欧拉函数求和

- 求 $\sum_{i=1}^{n} i\varphi(i)$
- $n \leq 10^{10}$

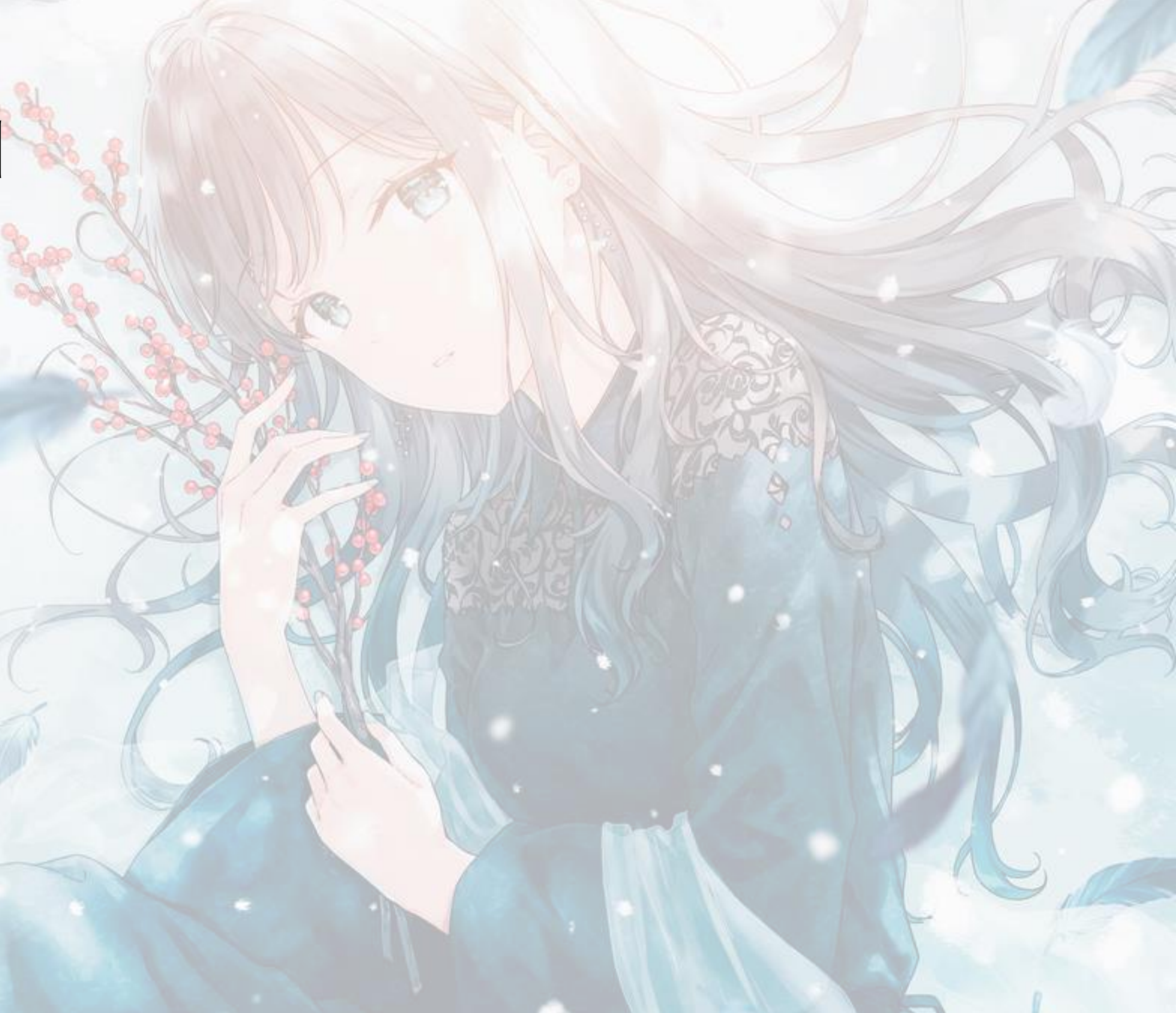


欧拉函数求和

- $I\varphi \otimes I = I^2$
- 剩下的留作练习。

约数函数求和

- 求 $\sum_{i=1}^{n} \sigma_1(n)$
- $n \le 10^{14}$



约数函数求和

- 有时候直接卷积不易，需要一些转化。
- 问题是求每个数的约数和，考虑转而求每个数是多少数的约数。
- 答案变为 $\sum_{i=1}^{n} i \left\lfloor \frac{n}{i} \right\rfloor$，整除分块，复杂度 $O(\sqrt{n})$。

素因子次幂

- 设 $\omega(n)$ 是 n 的不同质因子个数。
- 求 $\sum_{i=1}^{n} 2^{\omega(n)}$
- $n \le 10^{12}$

素因子次幂

- $2^{\omega(n)}$ 相当于每个质数要么取，要么不取，即假设有 $pq = n$，原式即 $\gcd(p,q) = 1$ 的对数。
- 不妨设 $p \le q$，则 $p \le \sqrt{n}$。枚举 p。
- $1 + 2\sum_{i=1}^{\sqrt{n}} \sum_{j=i+1}^{\left\lfloor \frac{n}{i} \right\rfloor} [\gcd(i,j) = 1]$
- $= 1 + 2\sum_{d} \mu(d) \sum_{d|i}^{\sqrt{n}} \left\lfloor \frac{n}{id} \right\rfloor - \frac{i}{d}$
- 直接枚举，复杂度 $\mathrm{O}(\sqrt{n}\ln n)$

And More

- 上面可以发现，杜教筛的使用有一定的局限性，能否找到一种适用范围更广的算法呢？
- 这就是洲阁筛，其原理比较复杂，这里不讲，详见 2016 年任之洲集训队论文。

And More

- 上面可以发现，杜教筛的使用有一定的局限性，能否找到一种适用范围更广的算法呢？
- ~~这就是洲阁筛，其原理比较复杂，这里不讲，详见 2016 年任之洲集训队论文。~~
- 这就是 Min_25 筛，其原理也不复杂，这里不讲，详见 Min_25 博客或网络搜索 Min_25 筛。

And More

- 上面可以发现，杜教筛的使用有一定的局限性，能否找到一种适用范围更广的算法呢？
- ~~这就是洲阁筛，其原理比较复杂，这里不讲，详见 2016 年任之洲集训队论文。~~
- ~~这就是 Min_25 筛，其原理也不复杂，这里不讲，详见 Min_25 博客或网络搜索 Min_25 筛。~~
- 这就是新版 Min_25 筛（亦称 Min_26 筛），详见知乎专栏 60378354。