Number Theory

SGColin

August 11, 2019

The Shiyan School Attached to Shijiazhuang NO.2 Middle School

Self Introduction

我叫高义雄，负责这两天给大家讲 NOIP 范围内的基础数论。

二中南校区，2017 级。NOIP 2018 省一，APIO 2019 Cu。

我的 Blog 是 https://blog.gyx.me ，课件可以在这里下载。

Praface

NOIP 中的数论部分重在思考，上课有问题随时提问。

可以简单记一些强调的公式性质，课件在课后自己下载或下发。

讲的太快/慢了，有不懂的都提醒我一下。

Contents

约数相关

约数与倍数

对于整数 a, b，若存在整数 c 使得 $b = a \times c$ ：

则称 b 为 a 的倍数，a 为 b 的约数。

两数的最大公约数称为 GCD(Greatest common divisor)

两数的最小公倍数称为 LCM(Least common multiple)

举个例子？

素数与合数

若大于 1 的正整数 P ，其约数只有 1 和 P 本身，称其为素数 (质数)。

若其有超过两个约数，则称其为合数。

若两个数 A, B 其最大公约数为 1 ，则称 A, B 互质。

~~小学老师应该都讲过吧？~~

算术基本定理

任何一个自然数 N ，如果 N 不为质数，那么 N 可以唯一分解成有限个质数的乘积

$$N = p_1^{a_1} \times p_2^{a_2} \times p_3^{a_3} \times \cdots \times p_n^{a_n}$$

其中 $p_1 < p_2 < p_3 < \cdots < p_n$ 均为质数，指数 a_i 均为正整数。

这样的分解称为 N 的标准分解式。

举个例子？

素数无限定理

内容：正整数集中包含无限个素数

证明：构造反证法

假设素数有限，为 $p_1, p_2, p_3, \cdots, p_n$，构造

$$S = 1 + \prod_{i=1}^{n} p_i$$

若 S 为素数，与假设矛盾。

若 S 为合数，则 $p_1, p_2, p_3, \cdots, p_n$ 都与 S 互质，与算术基本矛盾。

Quiz

Q_1：给定一个正整数，如何计算其全部约数？

线性暴力：从小到大枚举数 a 是否是当前 n 的约数即可。

Q_2：给定一个正整数，如何计算其标准分解？

线性暴力：从小到大枚举数 a 是否是当前 n 的约数，若是则将 n 一直除 a 直到 a 不是 n 的约数为止。

Quiz - Solution

Q_1：给定一个不超过 10^{14} 的正整数，如何计算其全部约数？

根号统计：发现若 p 是 n 的约数，则 n/p 也是 n 的约数 (约数成对出现)，故只需知道小于等于根号 n 的全部约数对即可。

复杂度为 $O(\sqrt{n})$ ，有没有什么细节需要注意？

Q_2：给定一个不超过 10^{14} 的正整数，如何计算其标准分解？

根号分解：若枚举的 $a > \sqrt{n}$ 显然无意义，故只算 $a \leq \sqrt{n}$ 的，最终剩下的 n 若不是 1 则也是一个素数。

复杂度为 $O(\sqrt{n})$ 。

Quiz

Q_1：给出一个不超过 10^{14} 的数，求其约数个数？

线性暴力：从小到大枚举数 a 是否是当前 n 的约数即可。

Q_2：给出一个不超过 10^{14} 的数，求其约数和？

线性暴力：从小到大枚举数 a 是否是当前 n 的约数即可。

Quiz - Solution

Q_1 : 给出一个不超过 10^{14} 的数，求其约数个数？

$O(\sqrt{n})$ 计算出其标准分解，多集合的基础计数问题。

$$ans = \prod_{i=1}^{n}(a_i + 1)$$

Q_2 : 给出一个不超过 10^{14} 的数，求其约数和？

$O(\sqrt{n})$ 计算出其标准分解，多集合的基础计数问题。

$$ans = \prod_{i=1}^{n}(\sum_{j=0}^{a_i} p_i^j)$$

最大公约数

(1) 若 GCD(a,b)=1, 那么 a，b 两数互质。

(2)GCD(a,2a)=GCD(a,a)=GCD(a,0)=a;

(3)LCM(a,b)GCD(a,b)=ab;（证明：集合的交并）

(4)GCD(n,n+1)=1;

证明：反证法。

假设他们不是互素的，有大于 1 的公因子 q

n = p1 * q,n + 1 = p2 * q；n+1 - n = q(p2 - p1)

则 q(p2-p1) = 1；其中 p2,p1 均为整数，q >=2, 可证不等，与假设相悖。

GCD 与 LCM 的集合含义

Q_1：两个很大的数 A, B ，以标准分解形式给出，求其 gcd ？

Q_2：两个很大的数 A, B ，以标准分解形式给出，求其 lcm ？

$$A = p_1^{a_1} \times p_2^{a_2} \times p_3^{a_3} \times \cdots \times p_n^{a_n}$$

$$B = p_1^{b_1} \times p_2^{b_2} \times p_3^{b_3} \times \cdots \times p_n^{b_n}$$

Solution

Q_1：两个很大的数，以标准分解形式给出，求其 gcd ？

$$ans = \prod_{i=1}^{n} p_i^{\min(a_i, b_i)}$$

Q_2：两个很大的数，以标准分解形式给出，求其 lcm ？

$$ans = \prod_{i=1}^{n} p_i^{\max(a_i, b_i)}$$

更相减损术

《九章算术》中古人的智慧。

Step:

(1)gcd(a,b)=gcd(a,a-b)

(2)gcd(2a,2b)=2gcd(a,b)

(3)gcd(2a,b)=gcd(a,b)

证明：设 gcd(a,b)=g，g 整除 a 也整除 b，那么 g 整除 a-b

用途：高精 gcd [SDOI 2009] SuperGCD

欧几里得算法

更优秀的解法，又名辗转相除法。

NOIP 数学部分的重点考察算法之一。

大家知道 $\%$ 运算吗？

若正整数 a, b 满足 $a > b$，则 a 可表示为 $a = kb + c$，则 $a\%b = c$.

有没有注意到取模运算就是多次的减法（大数减小数）？

欧几里得算法：当 $a > b$ 时，$gcd(a, b) = gcd(b, a\%b)$。

欧几里得算法 - cont'd

算法过程

由 $gcd(a, b) = gcd(b, a\%b)$，令 $a' = b, b' = a\%b$

递归调用 $gcd(a', b')$，返回 $gcd(a, b) = gcd(a', b')$。

递归边界:

若较小的数 $b = 0$，由性质 $gcd(a, 0) = a$，得到当前的结果为 a

正确性证明

只需证明 $x|a, x|b \Rightarrow x|a - b$，然后可以得到等式

$$gcd(a, b) = gcd(a, a\%b) = gcd(b, a\%b);$$

欧几里得算法 - cont'd

时间复杂度分析

暴力的复杂度最差是计算 $gcd(n,1)$，复杂度是 $O(n)$ 的。

欧几里得算法复杂度为 $O(\log_2 n)$ ，非常优秀。

因为我们可以证明 $a > b$ 时取模操作满足，$a\%b < \frac{a}{2}$:

(1) 若 $b > \frac{a}{2}$，则 $a\%b = a - b < a - \frac{a}{2} = \frac{a}{2}$

(2) 若 $b \leq \frac{a}{2}$，则 $a\%b < b \leq \frac{a}{2}$

当 $a < b$ 时 $(b, a\%b) = (b, a)$，相当于交换 a, b 此时必定满足前者大于后者, 回到上一情况。

因此每 2 次递归必定会使较大值缩小到原来一半以下。

进行 $\log_2 \max(a, b)$ 次递归后必定有一个数为 0，递归结束。

Luogu 1372

老师想要挑出默契程度最大的 k 个人参与毕业晚会彩排。可是如何挑呢？老师列出全班同学的号数 1，2，……，n，并且相信 k 个人的默契程度便是他们号数的最大公约数。

给出 n, k，求最大的默契程度。$(k \le n \le 10^{18})$

Luogu 1372 - Solution

$$answer = \frac{n}{k}$$

果园有 $M \times N$ 棵树，组成一个 M 行 N 列的矩阵，水平或垂直相邻的两棵树的距离为 1。

兔八哥在第 x_1 行第 y_1 列的果树下, 猎人爬上第 x_2 行第 y_2 列的果树，准备杀死兔八哥。

如果猎人与兔八哥之间没有其它的果树，猎人就可以看到兔八哥，兔子就不安全。

给出 x_1, x_2, y_1, y_2，安全输出 yes 否则输出 no。
$(testcase \leq 10^7, x_1, x_2, y_1, y_2 \leq 10^{18})$

问题实质为：判断两整点确定的直线上，两点间是否还存在另一整点。

以兔子的坐标为原点，设原坐标系兔子 (x_1, y_1) ，猎人 (x_2, y_2) ，那么新坐标系下猎人的坐标为 $(x_2 - x_1, y_2 - y_1)$ ；

猎人能看见原点当且仅当其横纵坐标互质。

现在给出一个表达式，形如 a1/a2/a3/.../an ，直接计算就是逐个除过去，比如 1/2/1/4=1/8。

看到分数很不爽，希望你通过添加一些括号使分式变成一个整数。

例子中一种可行的添加括号的办法是 (1/2)/(1/4)=2。

现在给出 $a_1, a_2, \cdots, a_n$ ，问是否可以通过添加一些括号改变运算顺序使其成为一个整数。

数据范围：$n \leq 10^7, a_1, a_2, \cdots, a_n \leq 10^{18}$

为了使其结果尽可能为整数，我们应使分母最大，分子最小；

找规律发现，a2 无论如何都是在分母上的，那么这样添加括号即可：

$$a_1/(a_2/a_3/.../a_n) = \frac{a_1 \times a_3 \times \cdots \times a_n}{a_2}$$

进行约分，数太大，不能乘起来，怎么办？

对每一个分子都和分母求一次 GCD，然后令分母除以 GCD。

到最后一项时若分母 =1，则结果可以为整数，否则不可能。

输入 2 个正整数 x_0, y_0 ，求满足以 x_0 为 gcd, 以 y_0 为 lcm 的有序正整数对 (P, Q) 的个数。

数据范围：$x_0, y_0 \le 10^7$

由最大公约数的定义我们得到：

存在 $k1, k2 \in R$，使 $P = k_1 x_0, Q = k_2 x_0$

由 $LCM(a, b)GCD(a, b) = ab$ 可以得到：

$x_0 y_0 = PQ = k_1 k_2 x_0^2$, 即 $k_1 \times k_2 = y_0 / x_0$;

不妨设 $P < Q$, 即 $k_1 < k_2$, 从 1 到 $\lfloor \sqrt{\frac{y0}{x0}} \rfloor$ 枚举 k_1 ，计算出 k_2

若 k_1, k_2 互质，则为合法数对，计数。

因为是有序数对，交换 P, Q 为另一答案，答案乘二。

Quiz

Q_1：如何求多个数的最大公约数？

Q_2：如何求多个数的最小公倍数？

Q_3：给出两数的 GCD 和 LCM ，求合法的两数之差的绝对值最小值 $(GCD \times LCM \leq 10^{18})$。

Q3 - solution

Q_3：给出两数的 GCD 和 LCM ，求合法的两数之差的绝对值最小值 $(GCD \times LCM \leq 10^{18})$。

解法一：

求出 $GCD \times LCM$，这个就等于两数之积，考虑枚举其中的一个数。

枚举的数一定是 GCD 的倍数，所以直接枚举 GCD 的倍数，只需要处理枚举的数小于另一个数的情况，最后将所有算出来的答案取 min 即可，复杂度 $O(\sqrt{LCM})$。

Q3 - solution - cont'd

Q_3：给出两数的 GCD 和 LCM ，求合法的两数之差的绝对值最小值 $(GCD \times LCM \le 10^{18})$。

解法二：$\frac{LCM}{GCD} = \frac{A}{GCD} \times \frac{B}{GCD}$ 枚举第二个式子左半部分，乘上更新答案。复杂度 $O(\sqrt{\frac{LCM}{GCD}})$

解法三：还是上面的式子。考虑当 $\frac{A}{GCD}$ 和 $\frac{B}{GCD}$ 最接近的时候产生的差值最小所以直接从 $\sqrt{\frac{LCM}{GCD}}$ 处开始枚举第一个遇见的答案一定是最优秀的。

Bézout's lemma

常称作裴蜀定理或贝祖定理。

定理内容：设 a, b 是不全为零的整数，则存在整数 x, y ，使得 $ax + by = \gcd(a, b)$.

特殊形式：a, b 互质时，存在整数 x, y，使得 $ax + by = 1$

证明：参考 OI-wiki 上的证明：Link

应用：对于整数 a, b，其线性组合不可能组合出 x，使得 $\gcd(a, b) \nmid x$

扩展欧几里得

已知整数 a, b，求方程 $ax + by = \gcd(a, b)$ 的一组整数解。

算法原理：将求解 x, y 的过程放入到求解 $\gcd$ 的过程中。

对于取模运算，有 $a\%b = a - \lfloor \frac{a}{b} \rfloor \times b$

根据 $\gcd$ 性质 $ax + by = \gcd(a, b) = \gcd(b, a\%b)$

$$b \times x' + a\%b \times y' = b \times x' + \left(a - \lfloor \frac{a}{b} \rfloor \times b\right) \times y' = y' \times a + \left(x' - \lfloor \frac{a}{b} \rfloor \times y'\right) \times b$$

所以 $x = y', y' = x' - \lfloor \frac{a}{b} \rfloor \times y'$

递归边界：当 $b = 0$ 时，$ax + by = a$ 的解显然是 $x = 1, y = 0.$

扩展欧几里得 - 通解

已知方程 $ax + by = \gcd(a, b)$ 的一组整数解 x_0, y_0。

则通解为 $x = x_0 + kb, y = y_0 - ka(k \in \mathbb{Z})$，正确性可以理解吗？

$\Delta = kab$

同余方程

已知整数 a, b，求方程 $ax + by = z$ 的一组整数解。

有解条件：$\gcd(a, b)|z$ （裴蜀定理）

原方程的解即为 $ax + by = \gcd(a, b)$ 的解乘上 $\frac{z}{gcd(a,b)}$。

除法分块

求以 N 为被除数，在 $[0, N]$ 的范围内，将所得的商向下取整相同的所有除数区间。

$N \in [0, 10^9]$

这个问题有 $O(\sqrt{N})$ 的解决方案，即除法分块。

我们先给出做法，在证明正确性和复杂度。

除法分块 - 做法

维护两个变量 L, R，代表当前除数区间为闭区间 $[L, R]$，L 初始值为 1。

然后在 $L \le N$ 时循环进行下面的过程：

1. 设 $t = \lfloor \frac{N}{L} \rfloor$
2. 当前答案区间的右端点 $R = \lfloor \frac{N}{t} \rfloor$
3. $L = R + 1$

具体写法参考代码。

开始时左端点是 1 显然是没有问题的，而以后的每一次操作 $L = R + 1$，因此，我们只需要证明每次的 R 都为正确的即可。

首先 $\lfloor \frac{N}{t} \rfloor$ 一定是属于该除数区间的，所以我们只需要证明该数为区间上界。

反证法。设 $X = \lfloor \frac{N}{t} \rfloor$ 不是我们想要得到的 R，那么至少有 $X + 1$ 属于答案区间。

于是有 $\lfloor \frac{N}{X+1} \rfloor = t$，因为是下取整，于是有 $N \geq t \times (X + 1)$，于是有 $\lfloor \frac{N}{t} \rfloor \geq \left(\lfloor \frac{t \times (X+1)}{t} \rfloor = X + 1 \right)$

而根据定义有 $X = \lfloor \frac{N}{t} \rfloor$，于是有 $X \geq X + 1$，与事实相悖。

除法分块 - 复杂度证明

分情况讨论。

当所选除数 $\leq \sqrt{N}$ 时，显然这一部分的除数区间不会超过 $\sqrt{N}$ 个。

当所选除数 $\geq \sqrt{N}$ 时，得到的商 $\leq \sqrt{N}$，商不超过 $\sqrt{N}$ 种，所以除数区间也不会超过 $\sqrt{N}$ 个。

于是总时间复杂度 $O(\sqrt{N})$。

求和式

分情况讨论。

当所选除数 $\leq \sqrt{N}$ 时，显然这一部分的除数区间不会超过 $\sqrt{N}$ 个。

当所选除数 $\geq \sqrt{N}$ 时，得到的商 $\leq \sqrt{N}$，商不超过 $\sqrt{N}$ 种，所以除数区间也不会超过 $\sqrt{N}$ 个。

于是总时间复杂度 $O(\sqrt{N})$。

素数相关

素数的性质

若大于 1 的正整数 P ，其约数只有 1 和 P 本身，称其为素数 (质数)。

由此可以知道，p 与 $1, 2, \cdots, p-1$ 都互质，即与 $(p-1)!$ 互质。

Eraosthens 素数筛法

求小于 n 的所有正整数中的质数集合。

设置一 $1, 2, \cdots, n$ 的数表，从 2 开始若该数没有被划掉，则其为一个素数，将 $\leq n$ 的其所有倍数划掉。

优化：

(1) 如果当前枚举到的数是合数，那么它的倍数也一定是合数，之前肯定被当前数的因数划掉过。

(2) 若当前 i 为质数，则 2 到 $i-1$ 内的质数倍数都已经被划掉了，因此从 i^2 开始划掉合数即可。

优化后复杂度为 $O(n \log\ \log n)$，证明过于繁琐再次不再叙述。

Euler 素数筛法

求小于 n 的所有正整数中的质数集合。

维护每个数的最小素因子 mindiv，从 2 开始，若其 mindiv 未知，则为素数，将其小于本身的素数倍的 mindiv 设置成素数。

看代码理解一下过程。

每个数只会被其最小素因子筛一次，因此复杂度为 $O(n)$。

这种筛法不止可以用来筛素数，几乎是万能的。

所有积性函数的计算都可以用这个筛法线性筛出，很重要。

网上的版本很多，这里放一个比较好理解的。

复杂度证明即为证明每个数只会被最小的素因子筛一次。

prime 数组中的素数是递增的, 当 i 能整除 prime[j]，那么 i*prime[j+1] 这个合数肯定被 prime[j] 乘以某个数筛掉。

因为 i 中含有 prime[j],prime[j] 比 prime[j+1] 小，即 i=k*prime[j]

则 i*prime[j+1]=(k*prime[j])*prime[j+1]=k'*prime[j]，后面素数同理。

所以不用筛下去了。因此，在满足 $i\%prime[j] == 0$ 这个条件之前以及第一次满足改条件时,prime[j] 必定是 prime[j]*i 的最小因子。

同余相关

取模运算与同余号

对于整数 a, b 若 $a \div b = c \cdots d$

则称 a 整除 b 得 c ，余数为 d。又称 $a \mod b = d$;

若对于三个数 a, b, p ，有 $a \mod p = b \mod p$

则称 a, b 关于 p 同余，表示为 $a \equiv b \pmod p$ 。

存在整数 k 使得 $a = b + k \times p$ 。

模运算性质

(1) 自反性：$a \equiv a \pmod d$

(2) 交换性：$a \equiv b \pmod d \to b \equiv a \pmod d$

(3) 传递性：$a \equiv b \pmod d, b \equiv c \pmod d \to a \equiv c \pmod d$

(4) 同幂性：$a \equiv b \pmod d \to a^n \equiv b^n \pmod d$

(5) $a \equiv b \pmod d$ 则 $d|a-b$

如果 $a \equiv n \pmod d, b \equiv m \pmod d$，则

(6) 加法：$a + b \equiv n + m \pmod d$

(7) 减法：$a - b \equiv n - m \pmod d$

(8) 乘法：$a \times b \equiv n \times m \pmod d$

剩余系

剩余系就是指对于某一个特定的正整数 p，一个整数集中的数模 p 所得的余数域。

如果一个剩余系中包含了这个正整数所有可能的余数，就称之为是模 p 的完全剩余系。(一般地，对于正整数 p 有 p 个余数 $0, 1, 2, \cdots, p-1$)

整数的所有运算限制在剩余系中各种性质仍成立。

快速幂

求 a^k 的值，绝大多数会在模意义下做。

(1) a 的奇数次幂等于 $a \times (a$ 的偶数次幂）：$a^{2k+1} = a \times a^{2k}$

(2) a 的偶数次幂等于底数平方，指数折半 $a^{2k} = (a^2)^k$

时间复杂度：每两次运算必定会使指数减半，复杂度 $O(\log_2 n)$

乘法逆元

$ab \equiv ba \equiv 1 \pmod p$ 称 b 为 a 在模 p 意义下的乘法逆元 (inv)

定义了剩余系中的除法：$\frac{a}{b} \equiv a \times inv_p(b) \pmod p$

求法：扩展欧几里得或费马小定理。

扩欧解法：给定 a, p 计算 $a \times b \equiv 1 \pmod p$，等价于解方程 $ax + py = 1 \pmod p$ （x, y 为整数），其中 x 即为 a 的逆元。

根据裴蜀定理，方程有解的充要条件是 $gcd(a, p) = 1$，即 a 在模 p 意义下有逆元的充要条件是 a, p 互质。

费马小定理 - 引理

若 A, B 互质，即 $gcd(A, B) = 1$，则此时 $k \times A(0 \leq k < B)$ 会遍历整个 $\bmod B$ 剩余系。

一般化：若 $gcd(A, B) = g$，则此时 $k \times A(0 \leq k < B)$ 只能遍历 $\bmod B$ 剩余系中 g 的倍数部分。

证明（互质部分）采用反证法。

假设若不能遍历，则至少存在 k_1 k_2，使得

$$k_1 \neq k_2, k_1 \times a = k_2 \times a \pmod p$$

则 $(k_1 - k_2) \times a \equiv 0 \pmod p$

又因为 a, p 互素，所以 a 在模 p 剩余系意义下有逆元

所以 $k_1 - k_2 \equiv \frac{0}{a} = 0 \pmod p$，所以 $k_1 = k_2$，矛盾，证毕。

后者（不互质部分）证明类似。

费马小定理

若 p 为质数，且 $gcd(a, p) = 1$ ，那么 $a^{p-1} \equiv 1 \pmod p$

证明：构造集合

$$S_1 = \{1, 2, 3, \cdots, p-1\}, S_2 = \{a, 2a, 3a, \cdots, (p-1)a\}$$

由引理易知模意义下 $S_1 = S_2$。

因此将两个集合内所有元素乘起来，在模意义下依然相等

$$(p-1)! \equiv a^{p-1} \times (p-1)! \pmod p$$

由于 $(p-1)!$ 与 p 互质，所以 $(p-1)!$ 在模 p 意义下存在乘法逆元，两侧可以同除 $(p-1)!$，即 $a^{p-1} \equiv 1 \pmod p$，证毕。

费马小定理求乘法逆元

由费马小定理 $a^{p-1} \equiv 1 \pmod{p}$：

两侧同除 a，即得到 a 的逆元：

$$inv_p(a) \equiv a^{p-2} \pmod{p}$$

快速幂计算即可，复杂度 $O(\log_2 p)$

~~好些好调，建议求逆元不要写扩欧，写快速幂~~

欧拉函数

欧拉函数

定义：$\varphi(x)$ 表示 $[1, x]$ 里的所有整数中，与 x 互质的数的个数。

若 P 为质数，则 $\varphi(P) = P - 1$

若 P 为质数 p 的 n 次幂，则 $\varphi(P) = (p - 1) \times p^{n-1}$

若 P 可以写成两个互质的数 a, b 的积，则 $\varphi(P) = \varphi(a) \times \varphi(b)$

欧拉函数 - 求法

公式法：单点复杂度 $\sqrt{n}$ ，常用于少量求函数值

将 n 质因数分解为 $n = p_1^{k_1} \times p_2^{k_2} \times ... \times p_m^{k_m}$。

那么有 $\varphi(n) = n \times \frac{p_1 - 1}{p_1} \times \frac{p_2 - 1}{p_2} \times ... \times \frac{p_m - 1}{p_m}$ ，复杂度显然是质因数分解复杂度。

注意复杂度分析的时候不能直接是个数 $\times \sqrt{n}$ ，因为往往我们求的数并不全都是卡上限的。

欧拉函数 - 求法

线性筛，复杂度线性，用于求一个不大的数域内全部的函数值。

原理见代码。

我们再来练习另外几个线性筛积行函数。

[SDOI 2008] 仪仗队

给出一个 n ，求

$$\sum_{i=1}^{n}\sum_{j=1}^{n}[(i,j)=1]$$

$n \le 4 \times 10^4.$

[SDOI 2008] 仪仗队 - Solution

还记得前面那个兔子题吗？这是求一个 $n \times n$ 的矩阵内，横纵坐标互质的点的个数。

先考虑纵坐标小于横坐标的情况，那么相当于求每一个横坐标有多少个小于其且与其互质的纵坐标，有

$$\sum_{i=1}^{n}\sum_{j=1}^{i}[(i,j)=1]=\sum_{i=1}^{n}\varphi(i)$$

剩余的部分显然是纵坐标大于横坐标的点，考虑将横纵坐标交换，有转化成了刚才的式子。

此时我们对角线上的点都被重算了一次，但是除了 $(1,1)$ 点以外所有对角线上的点显然横纵坐标并不互质

$$ans=\left(\sum_{i=1}^{n}\varphi(i)\right)\times 2-1$$

[BZOJ 2818] GCD

给出一个 n ，求

$$\sum_{i=1}^{n}\sum_{j=1}^{n}[(i,j)\ is\ prime]$$

$n \le 10^7.$

先枚举 gcd 的值，式子变成

$$\sum_{d=1,\ d\ is\ prime}^{n}\sum_{i=1}^{n}\sum_{j=1}^{n}[(i,j)=d]=\sum_{d}\sum_{i=1}^{\lfloor\frac{n}{d}\rfloor}\sum_{j=1}^{\lfloor\frac{n}{d}\rfloor}[(i,j)=1]$$

发现后面的两个求和号就变成了上一题。

线性处理欧拉函数，线性求前缀和，再枚举 n 以内的质数，累加上其对应的答案就好。

[Luogu 2398] GCD SUM

给出一个 n ，求

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

$n \leq 10^5$.

按照套路我们枚举 (i,j) 的值，放到式子的最前面，有

$$\sum_{d=1}^{n} d \times \sum_{i=1}^{n}\sum_{j=1}^{n}[(i,j)=d] = \sum_{d=1}^{n} d \times \sum_{i=1}^{\lfloor \frac{n}{d} \rfloor}\sum_{j=1}^{\lfloor \frac{n}{d} \rfloor}[(i,j)=1]$$

然后后面的就是仪仗队这个题了，最后线性扫几遍就能得到答案。

[Luogu 3601] 签到题

定义函数 $f(x)$ 为小于等于 x 的数中与 x 不互质的数的个数。

给出 l, r ，求

$$\sum_{i=l}^{r} f(i) \% 66623333$$

$0 \le l \le r \le 10^{12}, r - l \le 10^6.$

[Luogu 3601] 签到题 - Solution

显然 $f(x) = x - \varphi(x)$ 然后就是两个求和减一下，前面是等差数列，我们只关心后一个。

$$\sum_{i=l}^{r} \varphi(i)$$

显然线性筛不能筛这么大数据范围，所以需要单点求欧拉函数值。

考虑对每一个数质因数分解复杂度还是过高，所以考虑每一个因数的影响。

显然区间里的 x 的倍数只有 $\frac{len}{x}$ 个，所以复杂度调和级数，枚举倍数然后更新一下就好了。

最后判断一下区间里的每一个数是否变成 1 了，若没有就再算一次即可。

Questions?

Thanks for listening.

QQ: 2679864609

Email : 2679864609@qq.com

Blog : blog.gyx.me

Made by LaTeX