Number Theory

SGColin

August 11, 2019

The Shiyan School Attached to Shijiazhuang NO.2 Middle School

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？

GCD

数论的基础之一，今天的重点。

(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。

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 $O(\sqrt{n})$ ，代码实现大家会吗？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 $O(\sqrt{n})$，代码实现大家会吗？

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。

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

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

~~大家应该知道什么是时间复杂度吧？~~

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。

Luogu 2651

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：$n \le 10^7, a_1, a_2, \cdots, a_n \le 10^{18}$

Luogu 2651 - Solution

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。

Luogu 1029

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：$x_0, y_0 \leq 10^7$

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 $O(\sqrt{LCM})$。

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。

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 ？

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

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

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 ？

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

Questions?

Summary

Thanks for listening.

QQ: 2679864609

Email : 2679864609@qq.com

Blog : blog.gyx.me

Made by LaTeX