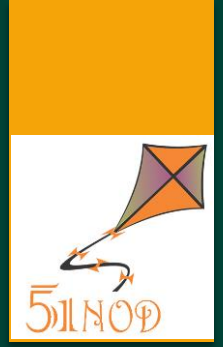




数论

最大公约数



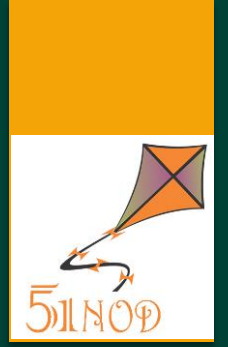
- ▶ 如果一个正整数 d 能被两个正整数 a 和 b 整除，那么 d 就是 a 和 b 的公约数。
- ▶ 最大的公约数就是最大公约数，我们称为gcd。

最大公约数



- ▶ 求解gcd是很容易的，我们可以迭代。
- ▶ $d|a, d|b \Leftrightarrow d|(a-b), d|b$
- ▶ $\text{gcd}(a,b)=\text{gcd}(a-b,b)=\text{gcd}(b,a\%b)$
- ▶ 复杂度为 $O(\log n)$

最大公约数



- ▶ 有意思的并不是gcd，而是求gcd的方法。

经典问题



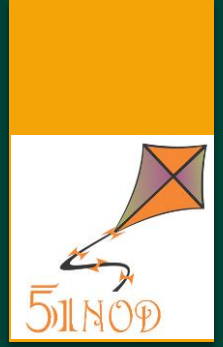
- ▶ 给定整数 a, b, c ，求两个整数 x 和 y 使得 $ax + by = c$ 。

经典问题



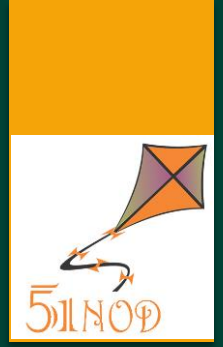
- ▶ 所谓exgcd。
- ▶ 由于 $a \% b = a - (a/b) * b$ ，那么求出 $bx' + (a \% b)y' = c$ 之后就能解出 $x = y'$, $y = x' - (a/b) * y'$

1187 寻找分数



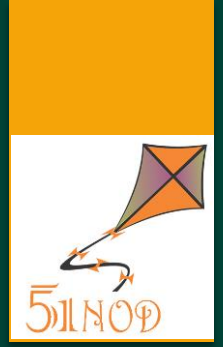
- ▶ 给出 a, b, c, d , 找一个分数 p/q , 使得 $a/b < p/q < c/d$, 并且 q 最小。(如果 q 相同, 输出 p 最小的)
- ▶ 其实 q 最小和 p 最小是没有区别的。

1187 寻找分数



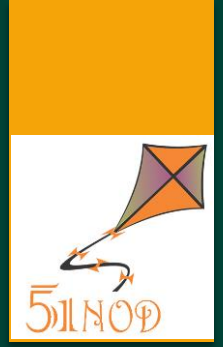
- ▶ 如果 $a/b=0$ ，很好办。
- ▶ 如果 a/b 和 c/d 的整数部分不相同，很好办。
- ▶ 于是可以去掉整数部分。

1187 寻找分数



- ▶ 假设 $a < b$, $c < d$, 尝试交换分子分母。
- ▶ $a/b < p/q < c/d \rightarrow d/c < q/p < b/a$
- ▶ 再次去掉整数部分 , 迭代下去。

1187 寻找分数



- ▶ 容易发现迭代等同于gcd，复杂度是 $O(\log n)$ 。

素数



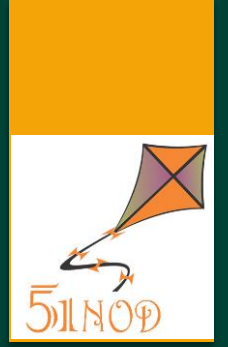
- ▶ 如果一个正整数除了1和它本身以外不再被别的正整数整除，那么它就是个素数。
- ▶ 判断一个数是不是素数，暴力可以做到 $O(n^{0.5})$

素因子分解



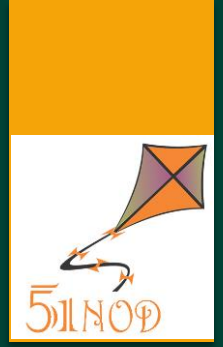
- ▶ 算术基本定理：任何一个大于1的自然数 n ，可以唯一分解为有限个素数的乘积。
- ▶ 暴力分解复杂度 $O(n^{0.5})$ 。
- ▶ 如何分解 $n!$ ？

素数个数



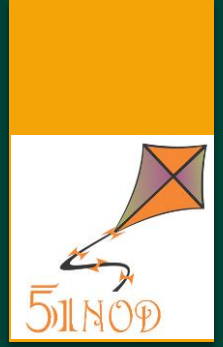
- ▶ 素数个数是无限多的。
- ▶ 小于 n 以内的素数个数大约为 $O(n/\log n)$ 。

筛法



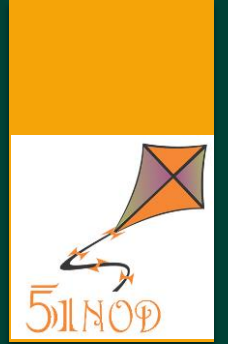
- ▶ 埃拉托斯特尼筛法 $O(n \log \log n)$
- ▶ 欧拉筛法 $O(n)$
- ▶ 可以求出1到n以内所有素数，也可以用来计算积性函数。

同余和逆元



- ▶ 对于整数 a, b, m ，如果 $a \% m = b \% m$ ，称 a 和 b 在模 m 下同余。
- ▶ 对于整数 x, y, m ，如果 $xy \% m = 1$ ，称 y 为 x 模 m 的逆元。

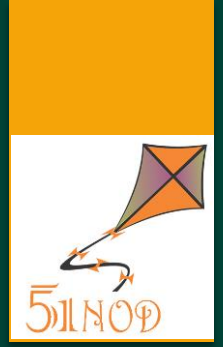
同余线性方程



▶ 解 $ax \% m = b$

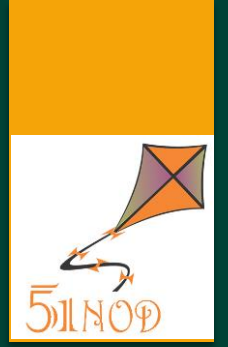
▶ `exgcd`

费马小定理



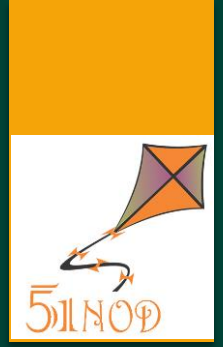
- ▶ 对于素数 p 和一个和 p 互质的数 x ，有 $x^{(p-1)} \% p = 1$ 。
- ▶ 欧拉定理：若 $\gcd(a, b) = 1$ ，有 $a^{\varphi(b)} \% b = 1$ 。

素数判定



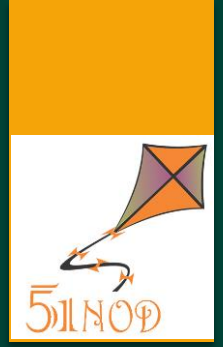
- ▶ 判定 p 是不是素数，随机几个 x ，看费马小定理是否成立。
- ▶ 但是有强伪素数，比如561。

素数判定



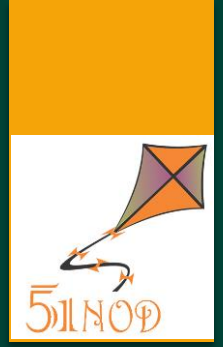
- ▶ 对于素数 p ， $x^2 \% p = 1$ 的 x 只有1和-1。
- ▶ 在验证费马小定理时，如果遇到平方，就可以同时检测。
- ▶ 对于 10^{18} 以内的数，选前9个素数测试即可。
- ▶ 这就是Miller-Rabin测试。

1186 质数检测 V2



- ▶ 直接Miller-Rabin测试即可。不过需要高精度。

欧拉函数



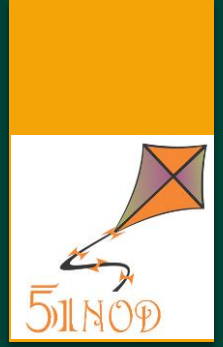
- ▶ 1到n以内和n互质的数字个数即为欧拉函数，记作 φ 。
- ▶ $\varphi(n) = n * (1 - 1/p_1) * (1 - 1/p_2) \dots * (1 - 1/p_k)$
- ▶ 欧拉函数显然积性，于是可以用欧拉筛法 $O(n)$ 求出所有的欧拉函数。

1060 最复杂的数



- ▶ 把一个数的约数个数定义为该数的复杂程度，给出一个 n ，求 $1-n$ 中复杂程度最高的那个数。

1060 最复杂的数



- ▶ 若 $n = p_1^{a_1} * p_2^{a_2} * \dots * p_k^{a_k}$ ，那么 n 的约数个数是 $(a_1+1)(a_2+1)\dots(a_k+1)$ 。
- ▶ 很显然，最复杂的数的质因子肯定是最小的一些，而且指数不增。
- ▶ 直接搜索。

1179 最大的最大公约数



- ▶ 给出N个正整数，找出N个数两两之间最大公约数的最大值。

1179 最大的最大公约数



- ▶ 其实就是求最大的公约数。
- ▶ 对于一个数 d ，如果有超过1个数是 d 的倍数，那就ok。

1179 最大的最大公约数



- ▶ 什么，怎么求有多少个数是 d 的倍数？
- ▶ 枚举 $d, 2d, 3d \dots$ 即可。
- ▶ $n/1 + n/2 + \dots + n/n = O(n \log n)$

1434 区间LCM



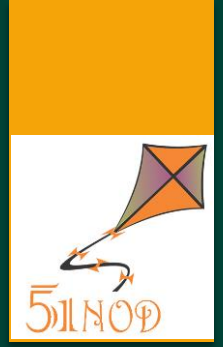
- ▶ 一个整数序列 S 的LCM（最小公倍数）是指最小的正整数 X 使得它是序列 S 中所有元素的倍数，那么 $\text{LCM}(S)=X$ 。
- ▶ 现在给定一个整数 N ，需要找到一个整数 M ，满足 $M>N$ ，同时 $\text{LCM}(1,2,3,4,\dots,N-1,N)$ 整除 $\text{LCM}(N+1,N+2,\dots,M-1,M)$ ，即 $\text{LCM}(N+1,N+2,\dots,M-1,M)$ 是 $\text{LCM}(1,2,3,4,\dots,N-1,N)$ 的倍数.求最小的 M 值。

1434 区间LCM



- ▶ 显然可以对于每个素数单独处理。
- ▶ 只要算出它在 n 内有多少次幂，若为 p^k ，那么 m 只要大于等于 $2p^k$ 即可。

1040 最大公约数之和



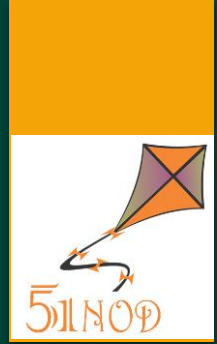
- ▶ 给出一个 n ，求 $1-n$ 这 n 个数，同 n 的最大公约数的和。

1040 最大公约数之和



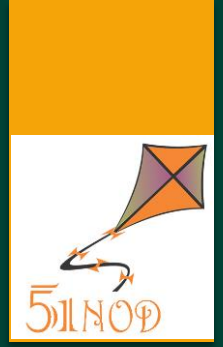
- ▶ 考虑枚举 n 的因子 d ，求出有多少个数和 n 的gcd为 d 。
- ▶ 容易发现有 $\phi(n/d)$ 个。

1217 Minimum Modular



- ▶ N 个不同的数 $a[1], a[2] \dots a[n]$ ，你可以从中去掉 K 个数，并且找到一个正整数 M ，使得剩下的 $N - K$ 个数， $\text{Mod } M$ 的结果各不相同，求 M 的最小值。

1217 Minimum Modular



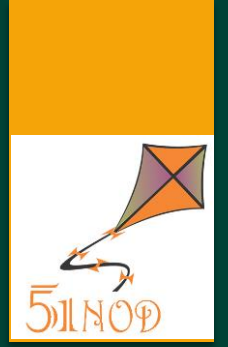
- ▶ 对于 $a[i]$ 和 $a[j]$ ，如果 $M \mid (a[i] - a[j])$ ，那么 M 会让 $a[i]$ 与 $a[j]$ 冲突。
- ▶ 容易算出每个 M 会产生多少对冲突。

1217 Minimum Modular



- ▶ 由于最多只能删 k 个，那么冲突对数不能超过 $(k+1)k/2$ 。
- ▶ 只要记录下这 k^2 对，并暴力判断即可。

1616 最小集合



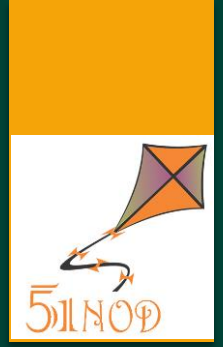
► 题面好长呀。

1616 最小集合



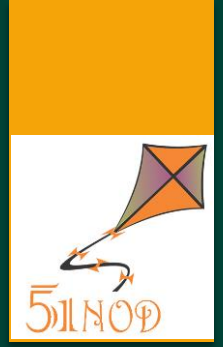
- ▶ 如果一个数字是原集合中某子集的gcd，那么它必须出现过。
- ▶ 否则就当它不存在。

1616 最小集合



- ▶ 用 $f[i]$ 表示有多少个数字是 i 的倍数。
- ▶ 如果 $f[d]$ 和 $f[id]$ ($i > 1$) 相同，那么 d 就可以不是最终集合中的数。否则就必须是。

1225 余数之和



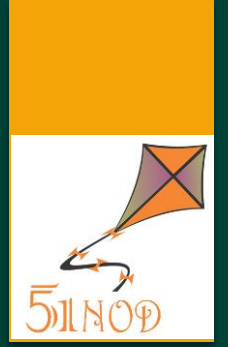
- ▶ $F(n) = (n \% 1) + (n \% 2) + (n \% 3) + \dots + (n \% n)$ 。
- ▶ 给出 n ，计算 $F(n)$ 。

1225 余数之和



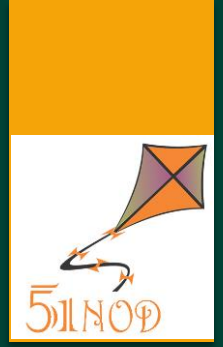
- ▶ $n \% i = n - (n / i) * i$
- ▶ n / i 的种类只有根号，枚举 n / i 等于多少，此时可行的 i 是一个区间，直接求和即可。

迪利克雷卷积



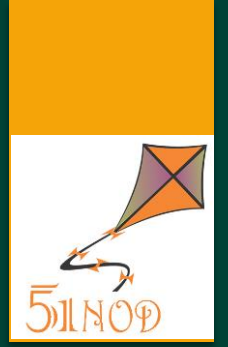
- ▶ 对于数论函数，下标加减意义不大，普通卷积不太有用。
- ▶ 于是就有了迪利克雷卷积：
- ▶ $(f * g)(n) = \sum f(d)g(n/d)$

迪利克雷卷积



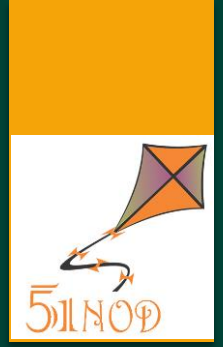
- ▶ 普通卷积需要快速傅里叶变换FFT，迪利克雷卷积直接算就是 $O(n \log n)$ 的。

莫比乌斯变换



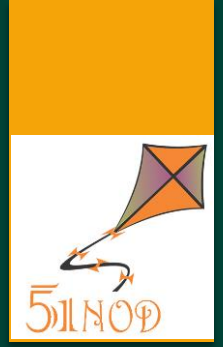
- ▶ 既然加减没有意义，那么前缀和就凉了。
- ▶ 但是前缀和是和全1数组的卷积，和全1数组的迪利克雷卷积称为莫比乌斯变换。
- ▶ $g=f*1$

莫比乌斯反演



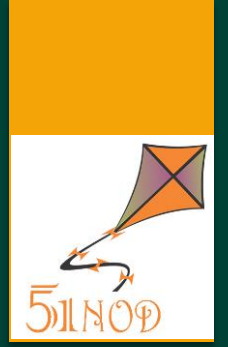
- ▶ 反过来，用g求f就是莫比乌斯反演，直接暴力就是 $O(n \log n)$ 的。
- ▶ 但是不够直观，能够用简单的式子表示吗？

莫比乌斯函数



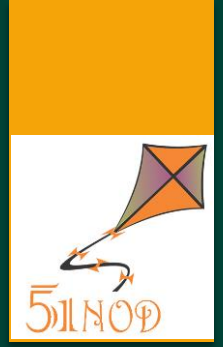
- ▶ 莫比乌斯函数 $\mu(n) = 0$ (n 有平方因子)
- ▶ $= 1$ (n 没有平方因子且有偶数个素因子，或者 $n=1$)
- ▶ $= -1$ (n 没有平方因子且有奇数个素因子)
- ▶ 显然莫比乌斯函数也积性。

莫比乌斯反演



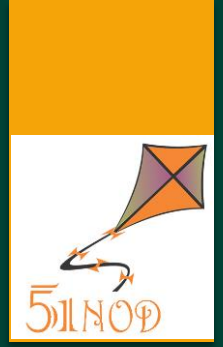
- ▶ 通过简单容斥，可以发现若 $g=f*1$ ，则 $f=g*\mu$ 。
- ▶ 这是我们平常见到的莫比乌斯反演。

1594 Gcd and Phi



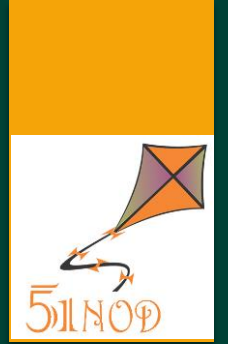
► 题目不太好打。

1594 Gcd and Phi



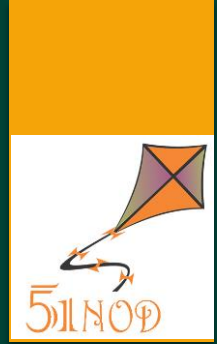
- ▶ 先求出所有的 ϕ 。
- ▶ 用 $f(i)$ 表示gcd为 i 的对数，这个是我们想求的。
- ▶ 用 $g(i)$ 表示gcd是 i 的倍数的对数，这个是我们容易求的。

1594 Gcd and Phi



- ▶ 看起来 f 和 g 并没有迪利克雷卷积的关系。
- ▶ 但是还是可以反演的。

总结



- ▶ 做好数论题，要求选手有较强的数学推导能力，掌握较多的数学知识和一些处理数论题的算法。
- ▶ 当然，对于更加难的数论题，技巧更加重要，需要有数学直觉和对数论题的较强的总结能力。