数论进阶

2024 年 7 月

feecle8146

QQ：3576754855，有问题欢迎课后提问。

回顾

回顾

昨天我们学习了：

1. 唯一分解定理。
2. 许多常用的数论函数，及求出它们的方法：线性筛。
3. 不定方程的解法：exgcd，以及由此引出的逆元。
4. 合并同余方程：excrt。
5. Lucas 定理处理组合数模小质数。

这些基础知识在今天仍然会大量用到。除这些外，我们还将

1. 简单的“式子处理”，这就涉及到整除分块。
2. 学习模意义下指数相关问题的解法，这就涉及到原根。

整除分块

整除分块

约数和 P2424

给定 X,Y，求 $\sum_{X\le i\le Y} d(i)$。$Y \le 2\times 10^9$

只需求出前缀和 $\sum_{i\le n} d(i)$，再相减。

尝试化简上式？提示：将 d 拆成一个求和号，再交换。

$$\sum_{i\le n} d(i) = \sum_{i\le n}\sum_{j|i} 1$$

$$= \sum_{j\le n}\sum_{j|i} 1 = \sum_{j\le n} floor\left(\frac{n}{j}\right)$$

整除分块

整除分块

整除分块的用途就是求 $\sum_{j\le n} floor\left(\frac{n}{j}\right)$ 这样的式子的值。为了简便，我们以后都省略 floor。事实上，它可以求任何 $\sum_{j\le n} g(j)\times f\left(\frac{n}{j}\right)$，其中 f 是好算的函数，而 $g(j)$ 的前缀和好算。

$\frac{n}{j}$ 可以有几种取值？提示：根号分治。

当 $j\le\sqrt{n}$ 时，j 只有 $\sqrt{n}$ 个；
当 $j>\sqrt{n}$ 时，$\frac{n}{j}\le\sqrt{n}$，只有 $\sqrt{n}$ 个。

因此，只有 $\le 2\sqrt{n}$ 种取值；换句话说，我们只需计算 $O(\sqrt{n})$ 种 $f(x)$，然后把每种 $f(x)$ 累加对应的次数。

整除分块

整除分块

有两种实现方法：

1. 直接实现根号分治的代码，讨论 $x \le \sqrt{n}, x > \sqrt{n}$，并分别算出这个 x 对应几个 j。由于较为繁琐，在此不提。
2. 仍然枚举 j，但是注意到 $\frac{n}{j}$ 是分段相等且单调递减的，因此可以一次枚举一段。

我们（以及主流 OI 界）将采用第二种实现。这就需要知道，当我们枚举到 j 时，下一步应当跳到哪里，也就是最大的 k 使得 $\frac{n}{k} = \frac{n}{j}$。

试着自己推出 k 的表达式？

$$\frac{n}{floor\left(\frac{n}{j}\right)}$$

整除分块

整除分块

枚举 j，但是注意到 $\frac{n}{j}$ 是分段相等且单调递减的，因此可以一次枚举一段。

当我们枚举到 j 时，下一步应当跳到哪里，也就是最大的 k 使得 $\frac{n}{k}=\frac{n}{j}$。

$$k=\frac{n}{floor\left(\frac{n}{j}\right)}$$

```
for (int i = 1, j; i <= n; i = j + 1) {
    j = n / (n / i);
    ans += (j - i + 1) * f(n / i);
}
```

试看看！

余数求和 P2261

求 $\sum_{i\le n}(k \bmod i)$，其中 $n,k \le 10^9$。

首先把 $k \bmod i$ 写成 $k-\frac{k}{i}\times i$，然后

$$ans = nk - \sum_{i\le n} i \times \frac{k}{i}$$

细节：

1. 代码里的 j 要和 n 取 min。
2. 当 $\frac{k}{i}=0$ 时，j 的真实值为无穷大，但在这里应该设为 n。

整除分块相关练习题：CF1706D2

试看看！

模积和 P2260

求 $\sum_{i\le n,j\le m,i\neq j}(n \bmod i)(m \bmod j)$，其中 $n,m \le 10^9$。

不妨假设 $n \le m$，则可以写成：所有 i,j，减去 $i=j$ 的。（这样有什么好处？）

拆式子的过程同上题，最终会出现同时含有 $\frac{n}{i},\frac{m}{i}$ 的表达式。如何处理？

提示：分界点的个数乘 2 后还是 $O(\sqrt{n})$ 的。

```
for (int i = 1, j; i <= n && i <= m; i = j + 1)
{
    j = min(n / (n / i), m / (m / i));
    ans += ... * f(n / i, m / i);
}
```

原根 阶

阶

使得 $x^n \equiv 1 \pmod p$ 的最小正整数 n 称为 x 模 n 的阶，记作 $|x|$。

显然，阶存在的充要条件是 $\gcd(x,p)=1$。

所有 $x^n \equiv 1 \pmod p$ 的 n 都是阶的倍数。这是因为阶也满足“辗转相除法”的性质。

结合拓展欧拉定理，可得 $|x| \mid \varphi(p)$。

阶是 x 的幂模 p 的最小循环节。由此可以推出，$\left|x^k\right| = \frac{|x|}{\gcd(k,|x|)}$。

（可以画图理解）

原根

原根

结合拓展欧拉定理，可得 $|x| \mid \varphi(p)$。

若 $|x| = \varphi(p)$，就说 x 是模 p 的一个原根。此时，$x^0, \ldots, x^{\varphi(p)-1}$ 不重不漏地取遍了所有 $< p$ 的与 p 互质的数。

结论：有原根的数只有 $2, 4, p^k, 2p^k$。且如果存在原根，最小原根不会超过 $n^{1/4}$，所以求原根的方法就是从小到大枚举，并判断阶是否为 $\varphi(p)$。

如何快速判断？

根据阶的性质，只需求出 $\varphi(p)$ 的所有质因子 q，并判断 $x^{\frac{\varphi(p)}{q}}$ 是否是 1。已知 $p, \varphi(p)$ 前提下，单次判断时间复杂度 $O(\log p\, w(p))$。

原根

所有原根

根据 $\left|x^k\right| = \frac{|x|}{\gcd(k,|x|)}$ 以及原根的次幂取遍所有与 p 互质的数，可以推出：

若 g 是某个原根，则所有原根就是 g^k，其中 $k \perp \varphi(p)$。

这说明原根若存在，则有 $\varphi(\varphi(p))$ 个。

练习题：P6091

原根 阶

求阶

求 $|x|$ 的暴力方法就是枚举 $\varphi(p)$ 的因数看每个因数满不满足 $x^k = 1$，利用的性质太少了。

能不能利用 $|x|$ 的倍数都满足 $= 1$ 的性质？

可以使用“试除法”：依次试图除掉每个质因子，若除掉之后 x^k 不再是 1 了，说明不能除。

至多试除 $O(\log p)$ 次，在已知 $p, \varphi(p)$ 的前提下复杂度是 $O(\log^2 p)$。

一个没什么关系的例题：P8993

BSGS

BSGS

求解指数同余方程

上面的“求阶”，其实是求阶指数同余方程的特殊情况。

指数同余方程的一般形式为，求下面方程 x 最小正整数解：

$$a^x \equiv b \pmod{p}$$

我们先解决 $\gcd(a,p)=1$ 的情况。

BSGS 算法的思想就是 meet in the middle。取块长 B，设 $x=iB-j$，则 $a^x \equiv b$ 等价于 $(a^B)^i \equiv b \times a^j$。

将 $(a^B)^i$ 放入哈希表内（若有重复只保留 i 最小的），再依次查询 $b \times a^j$。

BSGS

BSGS

求解指数同余方程

将 $(a^B)^i$ 放入哈希表内（若有重复只保留 i 最小的），再依次查询 $b \times a^j$。

由于 $x \leq \varphi(p)$ 而 $\varphi(p) = O(p)$，所以取 $B = \sqrt{n}$ 可做到复杂度 $O(\sqrt{n})$。

特别地，如果固定 a, p 有多组 b，则只需要一次预处理（复杂度 $O\left(\frac{n}{B}\right)$），单次查询复杂度 $O(B)$，平衡复杂度后可做到总共 $O(\sqrt{nq})$。

由于在实数意义下，求 $a^x = b$ 的运算是“对数”，所以指数同余方程问题又称为离散对数问题。

BSGS

exBSGS

求解指数同余方程

上面我们解决了 $\gcd(a,p)=1$ 的情况，$\gcd(a,p)\neq 1$ 的情况呢？

此时，阶不存在，欧拉定理也不成立，所以 $a^i \bmod p$ 的值不再是“纯循环的”（圆形），而是先经过一段不循环的再循环（ρ 形）。

图：$p=495616, a=124$

思考：为什么会出现 ρ 的“尾巴”？
尾巴至多有多长？

BSGS

exBSGS

求解指数同余方程

出现“尾巴”的原因，可以通过分离互质部分和不互质部分看出。

假设 $a = cd$，其中 $c \perp p$。每次乘上 a 后，c, d 分别怎么变？

首先，c, d 的变化互不干扰。$c \to c^2$，$d \to d^2$。

其次，当 d 中包含的质因子幂次全部超过 p 对应的质因子幂次时，d 就不会变了。这也说明，ρ 的尾巴长度是 $\log$ 级别的。

（为了理解，可以模拟 $6^k \bmod 24$）

BSGS

exBSGS

求解指数同余方程

因此，可以用 $\gcd(a^k,p)=\gcd(a^{k+1},p)$ 是否成立，来判断是否进入了循环节；
假设已经进入了循环节，且进入位置为 $a^k\equiv u\pmod p$，则可以用 $\gcd(b,p)=\gcd(u,p)$ 是否成立，来判断 b 是在循环节内还是循环节外。

在循环节外：只有 $\log$ 个 b 有解，且解已在暴力过程中求出。

在循环节内：此时可以把 b,p 同除以 $\gcd(b,p)=g$，再把 a^x 分出一个 u，得

$$a^{x-k}\times\frac{u}{g}\equiv\frac{b}{g}\left(\mod\frac{p}{g}\right)$$

BSGS

exBSGS

求解指数同余方程

在循环节内：此时可以把 b,p 同除以 $\gcd(b,p)=g$，再把 a^x 分出一个 u，得

$$a^{x-k}\times\frac{u}{g}\equiv\frac{b}{g}\left(\mathrm{mod}\,\frac{p}{g}\right)$$

此时，$\frac{u}{g}$ 存在逆元，可以除过去；同时，根据之前的讨论，g 包含了所有 a,p 共有的质因子，所以 $\gcd\left(a,\frac{p}{g}\right)=1$。此时再套用 BSGS 即可。

注：对于“分开互质部分和不互质部分”的更多运用，可以参见[题解 P4588【[TJOI2018]数学计算】- 洛谷专栏 (luogu.com.cn)](#)。

BSGS

小结

小结

至此，我们已经完全解决了 $a^x \equiv b \pmod p$ 的问题：

1. $(a,p)=1$：BSGS 求特解 x，$x+|a|\times k$ 就是通解。
2. $(a,p)\neq 1$：先暴力找到循环节开头，判断方法是 $\gcd(a^k,p)=\gcd(a^{k+1},p)$。
   用 $\gcd(b,p)=\gcd(a^u,p)$ 来判断 b 在不在循环节内。

   不在：只有 log 个可能的 b，而且每个 b 只有一个解。

   在：设 $g=\gcd(b,p)$，把同余方程写成 $a^{x-k}\times\frac{u}{g}\equiv\frac{b}{g}\left(\mathrm{mod}\,\frac{p}{g}\right)$，此时所有数都有逆元，套用 BSGS 可以求出最小特解。

   而通解就是最小特解加上任意倍的 a 在模 $\frac{p}{g}$ 意义下的阶。

因此，所有离散对数问题要么等价于有下界的同余方程，要么只有 ≤ 1 个解。

试看看！

随机数生成器 P3306

给定 x_1, a, b, p，保证 p 是质数，$x_i = ax_{i-1} + b$。

求最小的 i 使得 $x_i \equiv b \pmod{p}$。

利用等比数列求和公式化简，再分离变量 a^i，就转化为 $a^i \equiv c \pmod{p}$ 了。

试看看！

快乐肥宅 P5345

已知 x 同时满足 n 个方程：$a_i^x \equiv b_i \pmod{p_i}$，其中 $p_i \leq 10^7$，$n \leq 1000$。

求出最小的符合条件的 x。若最小的 x 超过了 10^9，输出 -1。

根据前述结论，每个同余方程都等价于下面三者之一：

1. x 无解。
2. $x = x_0$。
3. $x = x_0 + k \times y_0$，其中 k 为正整数。

如果存在前两种，直接判断即可。否则，只需要 excrt 合并同余方程。

试看看！

快乐肥宅 P5345

已知 x 同时满足 n 个方程：$a_i^x \equiv b_i \pmod{p_i}$，其中 $p_i \leq 10^7$，$n \leq 1000$。

求出最小的符合条件的 x。若最小的 x 超过了 10^9，输出 -1。

细节：合并同余方程的时候 lcm 会很大，怎么办？

假设当前合并结果为 $x \equiv x_0 \pmod{P}$。当 $P > 10^9$ 时，x 只有一种可能，所以一旦 P 大了就不合并下去，直接判断当前的 x_0 是否合法。

试看看！

前缀离散对数 经典问题

给定 a,p，对于每个 $b=1,2,\dots,T$，求方程 $a^x \equiv b \pmod p$ 的最小解，保证 a,p 互质。

直接用刚才的做法是 $O(\sqrt{pT})$ 的。能不能利用 b 是前缀的性质，取得再优秀一点的复杂度？

提示：若 $a^{x_1} \equiv b_1, a^{x_2} \equiv b_2$，则 $a^{x_1+x_2} \equiv b_1 \times b_2$。

离散对数满足 $f(ab)=f(a)+f(b)$，可以线性筛！
只需知道质数处的值，就能筛出所有值（不一定最小）。

时间复杂度 $O(\sqrt{pT/\log T})$。当然，筛出的值不一定最小，所以还需要先算出 a 的阶，然后把答案对它取个模。

试看看！

心跳 Codechef CHEFMOD

固定 $P = 10^8 + 7$，给定 $1 \leq a < P$，定义无穷序列 $a_i = a^i \bmod p$。求 a_i 的所有前缀最小值之和。

有 T 次询问，$T \leq 500$。

先考虑一次询问怎么做。

提示：

1. “取模”和“比大小”两个操作看起来毫无关系。
2. i 第一次在序列中出现的位置就是 i 以 a 为底的离散对数。

可以认为模意义下的序列 a^i 几乎是随机的！

试看看！

心跳 Codechef CHEFMOD

固定 $P = 10^8 + 7$，给定 $1 \le a < P$，定义无穷序列 $a_i = a^i \bmod p$。求 a_i 的所有前缀最小值之和。

有 T 次询问，$T \le 500$。

由随机性（类比随机排列），我们可以认为经过足够多（不太多）次之后，前缀最小值已经很小了。

$O(i)$ 次后最小值大约是 $O\left(\frac{P}{i}\right)$，特别地，$O(\sqrt{P})$ 次后最小值就该 $\le 10^4$ 了。

这很难严谨证明。不过，穷举所有 $1 \le a < P$ 后可以发现是对的。

试看看！

心跳 Codechef CHEFMOD

固定 $P = 10^8 + 7$，给定 $1 \le a < P$，定义无穷序列 $a_i = a^i \bmod p$。求 a_i 的所有前缀最小值之和。

有 T 次询问，$T \le 500$。

暴力计算 $O(\sqrt{n})$ 项，后面只有 10^4 种不同的数。

用离散对数求出每种数 i 的出现位置，就能够回答询问了！这样，单次时间复杂度为 $\sqrt{10^4 P / \log 10^4}$。

如何拓展到所有 a？提示：取原根 g，设 $a = g^k$。

试看看！

心跳 Codechef CHEFMOD

固定 $P = 10^8 + 7$，给定 $1 \le a < P$，定义无穷序列 $a_i = a^i \bmod p$。求 a_i 的所有前缀最小值之和。

有 T 次询问，$T \le 500$。

取原根 g，设 $a = g^k$。

假设现在要求 i 在 $\{a^u\}$ 这一序列里出现的位置。先用 BSGS 预处理 i 在 g^k 序列里第一次出现位置 p，则其出现的所有位置就是 $p + j(P-1)$ $(j \in \mathrm{N})$；又因为 $a^u = g^{ku}$，所以只需求出最小的 j，使得 $k | p + j(P-1)$。

这就是二元不定方程，exgcd 即可，注意这里的 exgcd 可以做到 $O(1)$ 。

小结

“心跳”这道例题是原根处理指数问题的极好范例，我们将其中的思想总结如下：

1. 增长得很快的函数在模意义下的值可以认为是伪随机数。
2. 原根和阶两个概念使我们完全搞清楚了（有原根前提下）任何一个与 mod 互质的数 a 的所有次幂在模 mod 意义下的出现规律。

因此，我们得以将大部分与次幂的值相关的问题转化为关于指数的同余方程问题。

原根和群的同构 (*)

如果你了解过“群”的语言，你应当看出，原根的作用实际上是给出了模 p 缩系下的乘法群和模 $\varphi(p)$ 意义下的加法群的同构——这两个群都是元素个数为 $\varphi(p)$ 的循环群。

乘法群是我们不熟悉的，但循环群（可以想象为圆环上跳动）是我们熟悉的，而且有同余方程等各种工具来处理。例如，加法群的一个生成元是 1，乘法群的一个生成元是 g。换句话说，g 在乘法里的作用约等于 1 在加法里的作用。

知识总结

到此为止，我们的课程已经涵盖了联赛难度的所有数论知识。然而，在这些简单的知识基础上，仍然可以出出千变万化的难题、趣题。

用于求解同余方程的 exgcd 是基础。

当出现多个同余方程时，使用 excrt（本质就是 exgcd）来合并。

指数上的问题，如果还没有到要考虑阶的地步，（拓展）欧拉定理也可以将其转为同余问题。

与整除相关的求和，数论分块来计算。

指数上更难的问题，可以考虑原根，并合理利用阶的性质。

试看看！

幂塔方程（简单版） P8457

解方程 $x^x \equiv a \pmod{p}$，其中 p 是质数。只需求出任意一个 $\leq 10^{18}$ 的解或判断无解。

$$p \leq 10^9$$

提示：
固定底数，指数以 $p-1$ 为周期。
固定指数，底数以 p 为周期。

$(p, p-1) = 1$，所以可以……
同时固定底数和指数！

试看看！

求和 CF1717E

求 $\sum_{a+b+c=n} \operatorname{lcm}(c, \gcd(a,b))$，其中 $n \le 10^5$。

回忆处理求和号的思路：尽量让枚举的变量独立，转化为子问题。

你认为应该先处理哪个变量？

枚举 c，和式变为

$$\sum_{c \le n} \sum_{a+b=n-c} \operatorname{lcm}(c, \gcd(a,b))$$

你认为接下来应该枚举什么变量？

试看看！

求和 CF1717E

求 $\sum_{a+b+c=n} \operatorname{lcm}(c, \gcd(a,b))$，其中 $n \le 10^5$。

回忆处理求和号的思路：尽量将枚举的变量独立，转化为子问题。

$$\sum_{c \le n} \sum_{a+b=n-c} \operatorname{lcm}(c, \gcd(a,b))$$

直接枚举 $\gcd(a,b)=d$，要求 $d \mid n-c$：

$$\sum_{c \le n} \sum_{d \mid n-c} \operatorname{lcm}(c,d) f(d, n-c)$$

其中 $f(d)$ 表示：有多少对 $a+b=n$ 满足 $\gcd(a,b)=d$。怎么处理 f？

试看看！

求和 CF1717E

求 $\sum_{a+b+c=n} \operatorname{lcm}(c, \gcd(a,b))$，其中 $n \le 10^5$。

有多少对 $a+b=n$ 满足 $\gcd(a,b)=d$。

注意到 $\gcd(a,b)=\gcd(a,a+b)=\gcd(a,n)$，所以就是有多少个 $a<n$ 满足 $\gcd(a,n)=d$。

$\gcd(a,n)=d$，其实就是 $\gcd\left(\frac{a}{d},\frac{n}{d}\right)=1$！

所以，满足条件的 a 有 $\varphi\left(\frac{n}{d}\right)$ 个。

直接套前述公式计算，复杂度 $O(n\log n)$。

小结

前两题相对简单，但其中都蕴含了普适的思维方式：

1. p 是质数的话，底数和指数都有各自的循环节。如果都要控制（都出现了未知数），无非是合并一下同余方程。
2. 对于求和类问题，想清楚枚举什么变量能使问题最简单。

试看看！

我这个坏东西 AT_tenka1_2017_f

解方程 $a^x \equiv x \pmod{m}$。只需求出任意一个 $\leq 2 \times 10^{18}$ 的解，或判断解不存在。

$a, m \leq 10^9$，≤ 100 组数据。

提示：类比第一题“幂塔方程”。

提示：底数、指数的同余性质我们了如指掌，可惜幂的值我们知之甚少。怎么办？

提示：那就假设我们知道幂的值 $a^x \equiv x \equiv T \pmod{m}$，此时 x 就可以 BSGS 了。当然，BSGS 不是重点（因为其实不知道 T），重点是……

试看看！

我这个坏东西 AT_tenka1_2017_f

解方程 $a^x \equiv x \pmod{m}$。只需求出任意一个 $\leq 2 \times 10^{18}$ 的解，或判断解不存在。

$a, m \leq 10^9$，≤ 100 组数据。

假设我们知道幂的值 $a^x \equiv x \equiv T \pmod{m}$，此时 x 就可以 BSGS 了。当然，BSGS 不是重点（因为其实不知道 T），重点是，它给出了 x 应该满足的（有下界的）同余方程：$x \equiv T' \left(mod\ \varphi(m)\right)$！

（当然，x 可能很小，还没进入循环节，但我们现在只是对问题进行思考，不必纠结于边界情况）

此时你能推出什么新东西？

试看看！

我这个坏东西 AT_tenka1_2017_f

解方程 $a^x \equiv x \pmod{m}$。只需求出任意一个 $\leq 2 \times 10^{18}$ 的解，或判断解不存在。

$a, m \leq 10^9$，≤ 100 组数据。

此时，我们就知道了两个关于 x 的方程同时满足！

$$\begin{cases} x \equiv T \pmod{m} \\ x \equiv T' \pmod{\varphi(m)} \end{cases}$$

这说明 $T \equiv T' \pmod{\gcd(m, \varphi(m))}$！再看看 T' 和 T 是什么？

T 就是 $a^{T'} \bmod m$，而 $\gcd(m, \varphi(m))$ 又是 m 的约数，所以……

试看看！

我这个坏东西 AT_tenka1_2017_f

解方程 $a^x \equiv x \pmod m$。只需求出任意一个 $\leq 2 \times 10^{18}$ 的解，或判断解不存在。

$a, m \leq 10^9$，≤ 100 组数据。

T 就是 $a^{T'} \bmod m$，而 $\gcd\big(m, \varphi(m)\big) = g$ 又是 m 的约数，所以

$$a^{T'} \equiv T \equiv T' \pmod g$$

换句话说，通过模 m 的解 x，我们能推出此时的 T' 是模 g 的解。
这个过程，能不能反过来？如果已知一个模 g 的解 T'，那……

想想 T' 是怎么定义来的？

试看看！

我这个坏东西 AT_tenka1_2017_f

解方程 $a^x \equiv x \pmod{m}$。只需求出任意一个 $\leq 2 \times 10^{18}$ 的解，或判断解不存在。

已知一个模 g 的解 T'，而 T' 的定义就是 $x \equiv T' \left(mod\ \varphi(m)\right)$，这说明 $T = a^x \bmod m$ 也随之确定了！

而已知 T', T，方程组 $\begin{cases} x \equiv T \pmod{m} \\ x \equiv T' \pmod{\varphi(m)} \end{cases}$ 也确定了，可以直接解出 x！

因此，算法流程就是不停递归 $m \to \gcd(m, \varphi(m))$，并通过上述方式回带出 x 的值。当然，为了保证扩展欧拉定理成立，需要解同余方程时取一个 $\geq 10^9$ 的解。代码：Submission

小结

本题是笔者非常喜爱的一道题。

其具有较高的难度，但它的难度既不是繁琐的讨论，也不是莫名其妙无厘头的结论，而是有迹可循的，能踏踏实实一步一步还原出思维链条。

1. 希望把问题化为“我们熟悉”的形式，也就是要么限制指数要么限制底数。那就设出幂的值和离散对数的值，强行构造一组同余方程。
2. 构造同余方程后，发现能推出一个更小的模数满足同一形式的式子。
3. 上述都是在“已知指数和底数”前提下从答案逆推；反过来，如果只知道这个同一形式的式子的解，其实也可以还原出来设出的幂值和离散对数值！
4. 做法豁然开朗。

诸君若有兴趣，则可细细品味，或是看看另一个类似的题：P8457。