不定方程与积性函数

讲师：PinkRabbit　时间：20210629　地点：福建师范大学附属中学

Example.1 Chef and Prime Divisors (CHAPD)

题意：

> 对于正整数 n，设 n 的质因数分解为 $n=\prod_{i=1}^{s}p_i^{a_i}$ ，定义根数 $\operatorname{rad}(n)=\prod_{i=1}^{s}p_i$。
>
> T 组询问，每组给出 A，B，回答 $\operatorname{rad}(B)\mid A$ 是否成立
>
> $T\le 10^4$，$A,B\le 10^{18}$，1s，512MB。

题解：

因为 A 有 B 的每一个质因数，所以 $B\mid A^{+\infty}$，直接暴力判断就行了，每次把 A 平方一下，复杂度是 $O(\log\log n)$。

Example.2 失控的未来交通工具

题意：

> n 个点的带边权无向图，一开始没有边，另给定模数 m。
>
> 修改 (u,v,w)：加一条长度为 w 的边 (u,v)。
>
> 询问 (u,v,x,b,c)：求在 $x,x+b,\ldots,x+(c-1)b$ 中，有多少个数存在一条长度与之模 m 同余的、从 u 到 v 的（不必简单）路径
>
> $n\le 10^6,m\le 10^9$，1.2s，512MB。

题解：

参考线性基的套路，我们建出原图的一个生成树，并尝试找到所有的自由元。

首先，每个环是一个自由元，因为只要在去环的路上绕一绕，绕上 $2m$ 次，贡献就只剩环了。然后，每条边的两倍也是一个自由元，因为每条双向边可以看作一个环。设 a_i 为所有的自由元，于是有：

$$x+tb=L+\sum_{i=1}^{s}k_ia_i+km \tag{1}$$

根据多元裴蜀定理，得：

$$x-L+tb\equiv 0 \pmod{\gcd(m,a_1,a_2,\cdots,a_s)} \tag{2}$$

直接 `exgcd` 求解这个二元一次不定方程即可。

Example.3 Falsyta in Tina Town

题意：

> 给出随机数生成器 $x_{n+1}=kx_n+b \bmod m$ 的参数 x_0， m， k， b。
>
> 求最小的**正整数** n 使得 $x_n=x_0$，或者说明这样的 n 不存在。
>
> $T\le 100$ 组数据，$1\le m\le 10^9+9$，1s，128MB

题解：

显然有：

$$x_n=k^nx_0+\frac{1-k^n}{1-k}b\equiv x_0 \pmod m \tag{3}$$

视 $s=k^n$ 为未知数，则：

$$(k-1)x_0s+bx\equiv(k-1)x_0+b \pmod m \tag{4}$$

设 $A=(k-1)x_0$ 得：

$$As\equiv A \pmod m \tag{5}$$

于是：

$$As=A+ym\Rightarrow s=1+\frac{m}{\gcd(m,A)}y\Rightarrow k^n\equiv 1 \pmod{\frac{m}{\gcd(m,A)}} \tag{6}$$

设 $B=\frac{m}{\gcd(m,A)}$，则我们要求的是 $\lambda_B(k)$。

众所周知，若 $\gcd(k,B)\ne 1,$ 则阶不存在；否则的话，有 $\lambda|\varphi(m)$，直接扫描其因数就行了。

Example.4 猜数游戏

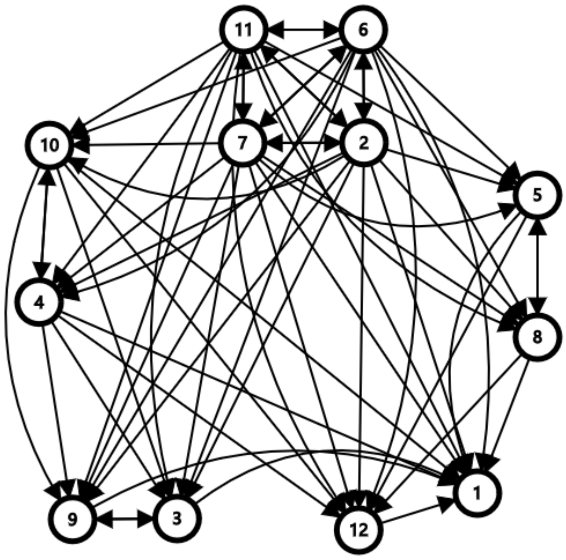
题意：

> 游戏在模 $m=p^\alpha$ 意义下进行，p 是奇素数。
>
> 给出 n 个互不相同的整数 $a_1,a_2,\dots,a_n$，值均在 $[1,m)$ 内。黑箱生成一个上述 n 个数的非空子集。
>
> 猜数规则：向黑箱询问一个 a_i，如果 a_i 不属于子集，回答空集；否则回答子集中所有形如 ${a_i}^k \bmod m$ 的数
>
> 求对于所有非空子集，（运气最好情况下）最小猜数次数的和，模 998244353。

> $n \le 5000$，$3 \le m \le 10^8$，2s，128MB。

题解：

我们建出图来找一找规律。先建出 $m=p$ 的图：



我们有以下猜想：

1. 如果图按照强连通分量缩点，则每个点对应一个 λ；λ 相同的所有点会构成一个团。
2. $x \to y \quad \Leftrightarrow \quad \lambda_p(y) | \lambda_p(x)$。
3. 这张图的任何一张导出子图缩点后都是原图缩点后的图的导出子图。

引理：$\lambda_p(x)$ 相同的点，它们的出边的可达集合相同。

> 因为 p 是质数，所以 $\gcd(x,p)=1$；又因为 $x=g^{\log_g x}$。
>
> $$\lambda_p(x)=\frac{\varphi(p)}{\gcd(\log_g x, \varphi(p)-1)} \tag{7}$$
>
> 设上式中的左右两式分别为 $g_x=\gcd(\log_g x,\varphi(p)-1)$, 设 $T=\varphi(p)$，于是可以表示 $x=g_x \cdot x' \ \ (\gcd(\frac{T}{g_x},x'=1))$。显然 g^{g_x} 的可达集合大小为 $\frac{T}{g_x}$，覆盖了每个 g_x 的倍数。
>
> 注意到 x 的可达集合可以表示为 $\{r\cdot g_x\cdot x'\}$；而 $g_x | r\cdot g_x \cdot x'$，所以 x 的可达集合包含于 g_x 的可达集合。
>
> 又注意到，$\lambda_p(x)=\lambda_p(g_x)$，所以两个集合大小相同；综上这是两个相同的集合。

猜想 1：

> g_x 的可达集合包含了所有 g_x 的倍数包含了所有 λ 相同的点。根据引理，每个 λ 与 g_x 相同的点都可以到达这些点，也就可以到达所有 λ 相同的点，因此这些点构成一个团。

猜想 2：

$\lambda_p(y)|\lambda_p(x)$ 等价于

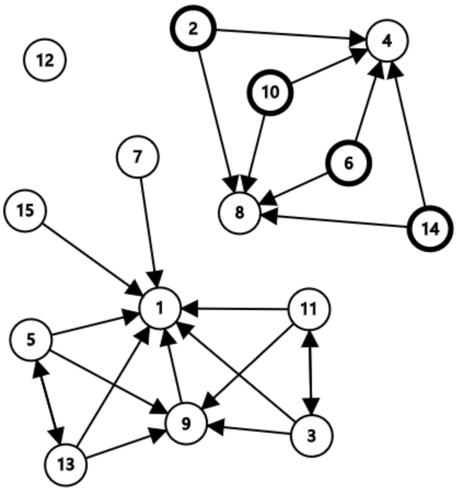
$$gcd(\log_g y, \varphi(p)-1) | \gcd(\log_g x, \varphi(p)-1) \tag{8}$$

于是 $g_y|g_x$；所以 g_y 可达 g_x；结合引理，x 可达 y。

猜想 3 显然。

因此我们在这一部分就可以分开统计每一个联通块的贡献，贡献条件是，它的上游全不选且它自己里面至少选一个。答案贡献可以表示为 $\sum(2^{\text{size}}-1)\cdot 2^{cnt}$ 的形式。

接下来考虑 $m=p^\alpha$ 次方的情况：



易见，图分成 $p|x$ 和 $p\nmid x$ 两部分；（图中忽略了第一部分通向 0 的边）。

对于第二部分，我们发现它和 $m=p$ 的情况有着相同的结论；对于第一部分，因为含有 p 作为因数，所以至多 α 次方就会通向 0，我们暴力连边的复杂度是对的；并且第一部分的图是一张 `DAG`，因为每个点只会连向拥有 p 的因子比自己更多的那些点。

Example.5

题意：

> 给出二阶线性递推数列 $f(0)=a$，$f(1)=b$，$f(n)=3f(n-1)-f(n-2)$。
>
> 求 $f^k(n) \bmod m$，其中 f^k 表示 f 迭代 k 次。$T\le 1000$ 组询问。
>
> $1\le n$，$m\le 10^9$，$1\le k\le 100$，1s，512MB。

题解：

做法当然是一层层找到循环节，设 $f(x) \bmod m$ 的循环节是 p_1，则 $f(f(x)) \bmod m$ 的循环节就是 $f(x) \bmod p_1$ 的循环节，依次类推。

考虑如何找到一个模数下的循环节。

`zc_li` 法：随机 $\sqrt{6m}$ 个点，矩阵快速幂计算出它的权值。根据生日悖论，则期望上会出现一对相同的二元组，这就是答案。

更优秀的做法：把 m 分解成 $\prod p^c$，答案就是这些的循环节的最小公倍数。如何找到 p 的循环节？如果 $p \bmod 10$ 等于 1 或 9，则其最大循环节是 $p-1$；否则是 $p+1$。而 p^c 的循环节就是 p 的循环节乘以 p^{c-1}。

Example.7 圆上的整点

题意：

> 求原点为圆心、R 为半径的圆周上的整点个数。$R \le 2 \times 10^9$。

题解：

易得：

$$(x+yi)(x-yi) = R \tag{9}$$

我们实际上就是求 R^2 的高斯素数分解的方案。设 $R^2 = \prod p_i^{c_i}$，则分解方案数为：

$$4\prod\left(\sum_{j=0}^{c_i}\chi(p_i^j)\right) \tag{10}$$

其中 $\chi(x) = 1, 0, -1, 0, 1, 0, -1, 0, \cdots$。这个可以用来求出一个 π 的表达式。

Example.8 Porter-Tele-Porter

题意：

https://www.luogu.com.cn/problem/AT190（课件中的题意写的不是很清楚）。

题解：

把图的坐标当作复数，那么这张图的坐标可以对 $E+si$ 取模（其他几个相当于 $(E+si)i$ 等）。、

设使用了传送器 (A_i, B_i)，最终位置为 $(A+Bi)(C+Di)$，则使用次数就是 $|C|+|D|$。

解一个复数意义下的 `exgcd` 即可；高斯整数的除法定义为除法完后两维分别四舍五入。

Example.9 GCD Counting

题意：

> 给定 n 个点的树，每个点 i 有一个权值 a_i，为 m 以内正整数。
>
> 定义 $g(x,y)$ 为 x,y 间简单路径的权值最大公约数
>
> 对于所有可能的 k，分别求有多少对 $x,y(x\le y)$ 使得 $g(x,y)=k$。
>
> $n,m\le 2\times 10^5$，4.5s，256MB。

题解：

询问 $g(x,y)=k$ 这样的条件，不妨先做 $k|g$，最后在反演回来。

于是图被分成了若干个连通块，每个连通块的贡献是 $\frac{sze^2+sze}{2}$；枚举 k，每次都直接对于满足条件的点做一次并查集的过程。复杂度 $O(n\cdot\max \mathrm{d}\cdot\alpha(n))$。

Example.10

题意：

> 一个 R×C 的矩形房间，四壁都是镜面
>
> 从一角沿角平分线方向发射一束光，不断反射。抵达角落则被传感器吸收
>
> 被吸收前反射次数记为 $f_{R,C}$，给出 $M,N\le 10^7$，求 $\sum_{i=1}^M\sum_{j=1}^N f(i,j)$。
>
> 答案对 10^9+7 取模，T 组询问，$T\le 10000$，4s，256MB

题解：

每反射一次，就把这个矩形往反射的方向翻折一次，易得：

$$f_{R,C}=\frac{\mathrm{lcm}(R,C)}{R}+\frac{\mathrm{lcm}(R,C)}{C}-2=\frac{R+C}{\gcd(R,C)}-2 \tag{11}$$

直接莫反就行了。

Example.11

题意：

> 给定正整数 n,m（$n\le 10^8$，$m\le 2\times 10^5$）。
>
> 考虑所有长度为 n，每个元素为前 m 个正整数的序列 $a=a_1,a_2,\dots,a_n$。
>
> 对于所有这样的序列，求 $(\mathrm{lcm}_{i=1}^n a_i)^{\gcd_{i=1}^n a_i}$ 之积，对 P=998244353 取模。

题解：

一种朴素的想法是枚举 gcd，但是这还是太复杂；我们决定将 gcd 欧拉反演掉，得：

$$\mathrm{Ans} = \prod_{a \subseteq [m]^n} (\mathrm{lcm}_{i=1}^n a_i)^{\sum_{d|a_i} \varphi(d)} \tag{12}$$

变换求和顺序并提取公因数：

$$\mathrm{Ans} = \prod_{d=1}^{m} \left(d^{\lfloor \frac{m}{d} \rfloor^n} \prod_{a \subseteq [\lfloor \frac{m}{d} \rfloor]^n} \mathrm{lcm}_{i=1}^n a_i \right)^{\varphi(d)} \tag{13}$$

考虑里面的这个 prod 怎么求，我们分开考虑每个素数的贡献：

$$\mathrm{Ans}_d = \prod_{p \in \mathbb{P}} \exp_p \left(\sum_{a \subseteq [m']^n} \max k : \exists i, p^k \mid a_i \right) \tag{14}$$

将 max 用小于号代替掉：

$$\mathrm{Ans}_d = \prod_{p \in \mathbb{P}} \exp_p \left([log_p m'] m'^n - \sum_{k=1}^{[log_p m']} \sum_{a \subseteq [m']^n} [\nexists i, p^k \mid a_i] \right) \tag{15}$$

仔细思考一下：

$$\mathrm{Ans}_d = \prod_{p \in \mathbb{P}} \exp_p \left([log_p m'] m'^n - \sum_{k=1}^{[log_p m']} \left(m' - \frac{m'}{p^k} \right)^n \right) \tag{16}$$

经过计算，这么做的复杂度是 $O(m \log_2 n)$ 的。

Example.12 循环之美

咕咕咕

Example.13

题意：

> 设 $g(x)$ 为 x 的可重质因子数目
>
> 例如 $g(2^3) = g(2 \times 3 \times 5) = g(2 \times 3^2) = 3, g(1) = 0$。
>
> 设 $f(x) = 2^{g(x)}$，你需要求出 $\sum_{i=1}^n f(i)$，对输入的质数 p 取模。
>
> $n \le 10^14$，$9 \times 10^8 < p < 10^9$，6s，1GB。

题解：

首先讲一下我想到的一种杜教筛做法（不能通过，但是很妙）。令 f 自卷，设 $H=f*f$，则：

$$H_n=\sum_{ab=n}2^{g(a)}\cdot 2^{g(b)}=\sum_{ab=n}2^{g(ab=n)}=f(n)\cdot d(n) \tag{17}$$

于是有：

$$f*f=f\cdot d \tag{18}$$

我们将其带入杜教筛的那个式子：

$$f(1)S(n)=\sum_{i=1}^{n}f(i)\cdot d(i)-\sum_{i=2}^{n}f(i)S\left(\left\lfloor\frac{n}{i}\right\rfloor\right) \tag{19}$$

考虑怎么求右式左边的那段：

$$\sum_{i=1}^{n}f(i)\cdot d(i)=\sum_{j=1}^{n}\sum_{j|i}f(i)=\sum_{j=1}^{n}f(j)S\left(\left\lfloor\frac{n}{j}\right\rfloor\right) \tag{20}$$

卧槽，假了 `f**k`！ 不想删了，请自动忽略上面的这段。

我们考虑 f 的 Bell 级数 $\sum_{i=0}^{+\infty}2^ix^i$，将其差分两次后发现 x^1 次项为 0。即 $f*\mu*\mu$ 只有在 `powerful number` 处有非零的值。那么这个函数是可以很快求得的。（μ 相当于差分）。

设 $h(n)=2^{g(n)-2}$ $(h[0]=1,h[1]=0)$，于是有

$$h=f*\mu*\mu \quad\Rightarrow\quad f=h*1*1=h*d \tag{21}$$

我们求和一下并变换求和顺序：

$$\sum_{i=1}^{n}f(i)=\sum_{i=1}^{n}\sum_{j|i}h(j)\cdot d\left(\frac{i}{j}\right)=\sum_{j=1}^{n}\sum_{i=1}^{\lfloor\frac{n}{j}\rfloor}h(i) \tag{22}$$

而 h 的前缀和可以在 $O(\sqrt{n})$ 时间内计算（只需考虑 `powerfull number`）。