1 数据范围

$20\%:\ n \le 20, p \le 1000$
$40\%:\ n \le 50, p \le 10^6$
$100\%:\ n \le 50, p \le 10^9$

2 关键词

广义特征子空间，高斯消元，极小多项式，牛顿迭代法

3 题解与思路

$20\%:\ n \le 20, p \le 1000$:

这一部分分代码量较短．p 很小，可以通过枚举法，判断 $\det(\mathrm{kI}-\mathrm{A})$ 是否等于 0，来暴力求特征值．对每个特征值 λ，$(A-\lambda I)^n$ 的解空间就是它的广义特征子空间．由于要求的矩阵所代表的线性变换限制在每个特征字空间上都是纯量乘法，所以可以对每个广义特征子空间取一组基，共 n 个向量 $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \cdots, \boldsymbol{\alpha}_n$ 形成全空间的一组基．A_1 在这组基下的矩阵就是由特征值构成的对角矩阵，即 $A_1(\boldsymbol{\alpha}_1, \cdots, \boldsymbol{\alpha}_n) = (\boldsymbol{\alpha}_1, \cdots, \boldsymbol{\alpha}_n)\mathrm{diag}\{\cdots\}$

$40\%:\ n \le 50, p \le 10^6$:

这一部分分代码量更大．为了更快地求特征值，可以求特征多项式，再一一代入 $0, \cdots, p-1$．特征多项式的求解有两种常见方法：拉格朗日插值法，和海森堡矩阵法．更方便的做法是求解极小多项式：依次加入 $1, A, A^2, \cdots$，直到它们线性相关，可以通过高斯消元法求出相应的极小多项式（标准程序中有这一段代码）．

时间复杂度：$O(n^4 + pn)$．

$100\%:\ n \le 50, p \le 10^9$:

设 A 的最小多项式为 $f(x) = (x-\lambda_1)^{s_1} \cdots (x-\lambda_m)^{s_m}$，设 $f_i(x) = f(x)/(x-\lambda_i)^{s_i}$，那么 $f_i(A)$ 的像就是 λ_i 的广义特征子空间．多项式 $f_1(x), \cdots, f_m(x)$ 是互素的，因此存在 $g_1(x), \cdots, g_m(x)$，使得

$$1 = g_1(x)f_1(x) + \cdots + g_m(x)f_m(x) \tag{1}$$

$$\text{即对于任意 } \boldsymbol{\alpha} \in \mathbb{F}_p^n,\ \boldsymbol{\alpha} = g_1(A)f_1(A)\boldsymbol{\alpha} + \cdots + g_m(A)f_m(A)\boldsymbol{\alpha} \tag{2}$$

由上式看出，$g_i(A)f_i(A)$ 代表的线性变换就是投影到这个广义特征子空间的变换．A_1 代表的线性变换限制在每个广义特征子空间上都是纯量乘法，所以 A_1 就可以由下式计算：

$$A_1 = \lambda_1 g_1(A)f_1(A) + \cdots + \lambda_m g_m(A)f_m(A) \tag{3}$$

这告诉我们一个很有用的信息，A_1 可以用 A 的多项式表示，即 $A_1 = \xi(A) \in \mathbb{F}_p(A)$．那么同样，$A_2 = A - A_1 = A - \xi(A) = \eta(A) \in \mathbb{F}_p(A)$．剩下的只需求出 $\xi(A)$ 就可以了．由于 A_2 是幂零矩阵，$A_2^n = 0$，所以 $f(x) | \eta(x)^n$．令 $v(x) = (x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_m)$，那么 $v(x) | \eta(x)$．可以通过 $v(x) = f(x)/\gcd(\mathrm{f(x)}, \mathrm{f'(x)})$ 求解 $v(x)$．再看 $\xi(x)$，由于 $A_1 = \xi(A)$ 可对角化，它的极小多项式无重根，所以 $v(\xi(A)) = 0$，即 $f(x) | v(\xi(x))$．设 $\eta(x) = \theta(x)v(x)$，那么

$$f(x) | v(\xi(x)) = v(x - \theta(x)v(x)) \tag{4}$$

可以发现，满足上述条件的 $\xi(A)$ 一定是A_1．那么问题就转变为，根据上式求解 $\theta(x)$．不妨加强条件，让 $v(x)^t|v(\xi(x))$，其中 t 是 $f(t)$ 中重因式的最高次数．我们对 $v(x-\theta(x)v(x))$ 进行泰勒展开：

$$v^2(x)|v(x-\theta(x)v(x))=v(x)-v'(x)\theta(x)v(x)+(\cdots)v^2(x) \tag{5}$$

$$1-v'(x)\theta(x)\equiv 0\ (\mathrm{mod} v(x)) \tag{6}$$

由于 $v'(x)$ 与 $v(x)$ 互素，$\theta(x)\bmod v(x)$ 的值就求出来了．细心的读者可以发现，上面的过程就是牛顿迭代法，令 $x_0(x)=x$，每次迭代使 $x_{i+1}=x_i-v(x_i)/v'(x_i)$．经过至多 t 次迭代后就可以得到 $\eta(x)$，那么就求出 A_1 了．

一些注意事项：上述方法只能在 p 充分大的时候有效．因为在 p 较小的域中，虽然 $v(x)$ 无重根，但 $v'(x)$ 可能和 $v(x)$ 不互素．这时要采用部分分的暴力算法．

时间复杂度：$O(n^4)$．

另一些注意事项：实际上，如果“ A 的特征多项式在 $\mathbb{F}_p[x]$ 中可以分解为一次因式的乘积”不成立，仍可以定义Jordan 分解（扩张到代数闭包中），而且还可以证明，A_1 与 A_2 的元素仍属于原先的域．在这种情况下，仍可以采用上述方法．但这样的不平凡的数据是很难造的．