题目大意

给定一个大小为K的环R。

环是一类包含两种运算（乘法$\otimes$和加法$\oplus$）的代数系统，满足

- $\forall a,b,c \in R, (a \oplus b) \oplus c = a \oplus (b \oplus c)$（加法结合律）
- $\forall a,b \in R, a \oplus b = b \oplus a$（加法交换律）
- $\exists 0 \in R$，$\forall a \in R, a \oplus 0 = a$（加法单位元）
- $\forall a \in R, \exists (-a) \in R, a \oplus (-a) = 0$（加法逆元）
- $\forall a,b,c \in R, (a \otimes b) \otimes c = a \otimes (b \otimes c)$（乘法结合律）
- $\exists 1 \in R$，$\forall a \in R, 1 \otimes a = a \otimes 1 = a$（乘法单位元）
- $\forall a,b,c \in R, a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c), (b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a)$（分配律）

考虑所有N维向量$\boldsymbol{u} = (u_1, u_2, \ldots, u_N)$（这里$\boldsymbol{u}$的每一维都是$R$中的元素），定义向量加法

$$\boldsymbol{u} + \boldsymbol{v} = (u_1 \oplus v_1, u_2 \oplus v_2, \ldots, u_N \oplus v_N)$$

以及数量乘法

$$a \cdot \boldsymbol{u} = (a \otimes u_1, a \otimes u_2, \ldots, a \otimes u_N)$$

（这里$a \in R$）。

对于一个向量集合$S = \{\boldsymbol{s_1}, \boldsymbol{s_2}, \ldots, \boldsymbol{s_n}\}$，我们称其能够表示$\boldsymbol{u}$当且仅当$\exists a_1, a_2, \ldots, a_n \in R, \sum_{i=1}^{n} a_i \boldsymbol{s_i} = \boldsymbol{u}$。

称一个N维向量集合S是一个完全表示，当且仅当它能够表示所有N维向量。

求所有N维完全表示的大小的M次方和对164511353（一个质数）取模的结果。

输入格式

第一行输入三个数N, K, M。

第二行输入一个数tp。

我们认为R中的每个元素唯一对应$[0, K)$中的一个整数。特别地，保证加法单位元对应0，乘法单位元对应1。

如果$tp = 1$，则$\forall i, j \in R, i \oplus j = (i + j) \mod K, i \otimes j = (i * j) \mod K$。

如果$tp = 2$，接下来输入$2K$行每行K个数。

对于前K行，第$i+1$行的第$j+1$个元素表示$i \oplus j$。

对于后K行，第$i+1$行的第$j+1$个元素表示$i \otimes j$。

输出格式

输出一行一个数，表示答案对164511353取模的结果。

数据范围

对于所有数据，$1 \le N \le 100000, 2 \le K \le 100000, 0 \le M \le 1000, \forall i,j \in R, i \oplus j, i \otimes j \in [0,K)$，保证输入是一个合法的环。

子任务编号	N	K	M	tp	特殊性质	分值
1	-	-	-	1	$K^N \le 20$	10
2	≤ 20	$\in \mathbb{P}$	$=0$	1	-	15
3	≤ 1000	$\in \mathbb{P}$	$=0$	1	-	5
4	-	$\in \mathbb{P}$	$=0$	1	-	5
5	-	≤ 100	$=0$	1	-	15
6	-	-	$=0$	1	-	5
7	≤ 100	-	≤ 100	1	-	15
8	-	-	-	1	-	15
9	-	≤ 20	-	2	-	15

解题过程

子任务1

直接暴力枚举集合，判断是不是完全表示。

复杂度$O(2^{K^N}(K^N)^2K + K^N\log M)$。

子任务2

不妨考虑dp。

令$f_{i,j}$表示i维完全表示中大小为j的个数。

对于一个i维向量集合T，令$trans(T)$为一个$i-1$维向量集合，使得

$$trans(T) = \{(u_1, u_2, \ldots, u_{i-1}) | \mathbf{u} \in T\}$$

直观地说，可以认为是T中的每个向量都删去了第i维，然后去重得到的结果。

显然如果T是完全表示，则$trans(T)$也必须是完全表示。于是对于i维完全表示T，我们认为其是由$trans(T)$转移而来的。

不妨考虑容斥：即$i-1$维完全表示转移到的所有集合-转移到的非完全表示。

前者是平凡的。主要难点在于转移到的非完全表示数。

如果$trans(T)$是完全表示，则T是完全表示当且仅当T能够表示$(\mathbf{0}_{i-1},1)$，且如果T能够表示$(\mathbf{u},x)(\mathbf{u},y)(x \neq y, \mathbf{u}\text{是}i-1\text{维向量})$，就也能够表示$(\mathbf{0}_{i-1}, x-y)$，进而能够表示$(\mathbf{0}_{i-1},1)$。

那么对于任意$i-1$维向量$\mathbf{u}$以及数a，称$\mathbf{u}$“对应”a当且仅当T能够表示$(\mathbf{u},a)$。则在T中，每个$i-1$维向量$\mathbf{u}$必须“对应”恰好一个数a。

定义$i-1$维的“基”向量为$(1,0,\ldots,0),(0,1,\ldots,0),\ldots,(0,0,\ldots,1)$。

钦定T能够表示$(1,0,\ldots,0,a_1),(0,1,\ldots,0,a_2),\ldots,(0,0,\ldots,1,a_{i-1})$。

则一个$i-1$维向量$\mathbf{u}$就会“对应”$\sum_{j=1}^{i-1}a_ju_j$。容易验证这样得到的确实是一个非完全表示。

那么我们有

$$f_{i,j}=(\sum_{l=0}^{j}([x^j]((x+1)^K-1)^l)f_{i-1,l})-K^{i-1}f_{i-1,j}$$

不妨写成生成函数的形式：

$$\begin{gathered}F_0(x)=x+1\\F_i(x)=\sum f_{i,j}x^j\\=F_{i-1}((x+1)^K-1)-K^{i-1}F_{i-1}(x)\\\therefore F_i(x-1)=F_{i-1}(x^K-1)-K^{i-1}F_{i-1}(x-1)\end{gathered}$$

令$G_i(x)=F_i(x-1)$则有

$$\begin{gathered}G_0(x)=x\\G_i(x)=G_{i-1}(x^K)-K^{i-1}G_{i-1}(x)\end{gathered}$$

那么答案就是

$$\begin{gathered}\sum_i[x^i]F_N(x)\\=F_N(1)\\=G_N(2)\end{gathered}$$

暴力求$G_N(x)$，复杂度$O(2^N)$。

子任务3

仔细观察一下$G(x)$的形式，可以发现x总是转移到x或x^K，且$G_0(x)=x$。于是$G(x)$必然只包含形如x^{K^i}的项，且$0\le i\le N$。

不妨定义未定元y，满足$y^i\cdot y^j=y^{ij}$。

定义$C(y)$满足

$$\begin{gathered}C_0(y)=y\\C_i(y)=(y^K-K^{i-1})C_{i-1}(y)=\prod_{j=0}^{i-1}(y^K-K^j)\end{gathered}$$

则

$$[x^j]G_i(x)=[y^j]C_i(y)$$

所以答案就是

$$\sum_j 2^j[y^j]C_N(y)$$

$C_N(y)$可以$O(N^2)$求出。复杂度$O(N^2)$。

子任务4

164511353是一个奇怪的数。那么它有什么用呢？

我们发现在模164511353的意义下，$2^{41}\equiv 1$。

那么对于y^i，我们可以认为它和$y^{i \bmod 41}$是等价的。

于是复杂度变成$O(N \cdot 41)$（实际上子任务4可以做到线性，但与后续做法关系不大）。

子任务5

现在考虑非质数的情况。

我们考虑枚举$d|K$，计数从某个$i-1$维完全表示转移而来的T，满足若T能表示$(\mathbf{0}_{i-1}, x)$，则$d|x$。

这也就是说，每个$i-1$维向量可以“对应”若干数，它们在模d意义下同余。

与质数类似地，我们首先确定基向量模d的值，然后$trans(T)$中每个元素可以“对应”$\frac{K}{d}$个数中的任意≥ 1个。

最后我们可以容斥出完全表示的个数：

$$G_0(x) = x$$
$$G_i(x) = \sum_{d|K} \mu(d) d^{i-1} G_{i-1}(x^{\frac{K}{d}})$$

和子任务3一样定义$C_i(y)$，则

$$C_i(y) = \sum_{d|K} \mu(d) d^{i-1} y^{\frac{K}{d}} C_{i-1}(y)$$

（可以发现K是质数的时候正是原来的式子）

应用子任务4的观察，复杂度可以做到$O(N \cdot 2^{K\text{的质因子个数}} \cdot 41)$。

子任务6

我们发现在上式中，不同的质因子是相对独立的。

形式化地说（设K质因数分解后得到$K = p_1^{a_1} p_2^{a_2} \dots p_l^{a_l}$）：

$$C_i(y) = \sum_{d|K} \mu(d) d^{i-1} y^{\frac{K}{d}} C_{i-1}(y)$$
$$= (\prod_{j=1}^{l} (y^{p_j^{a_j}} - p_j^{i-1} y^{p_j^{a_j - 1}})) C_{i-1}(y)$$

复杂度$O(N \cdot (K\text{的质因子个数}) \cdot 41)$。

子任务7

对于M次方和，我们还是考虑在$C_i(y)$上作文章。

令$C_{i,m}(y)$表示$\sum_j j^m y^j ([y^j] C_i(y))$。

可以发现对于任意m，

$$C_{i,m}(y) = (\prod_{j=1}^{l} ((p_j^{a_j})^m y^{p_j^{a_j}} - p_j^{i-1} (p_j^{a_j - 1})^m y^{p_j^{a_j - 1}})) C_{i-1,m}(y)$$

这样我们可以求出$\sum_i i^m 2^i ([x^i] G_n(x))$，不妨记为$h_m$。

于是

$$
\begin{aligned}
&\sum_i i^M [x^i] F_N(x) \\
&= \sum_i i^M [x^i] G_N(x+1) \\
&= \sum_i ([x^i] G_N(x)) \sum_j \binom{i}{j} j^M \\
&= \sum_i ([x^i] G_N(x)) \sum_j \binom{i}{j} \sum_k \left\{ M \atop k \right\} \binom{j}{k} k! \\
&= \sum_k \left\{ M \atop k \right\} \sum_i ([x^i] G_N(x)) i^{\underline{k}} 2^{i-k} \\
&= \sum_k \left\{ M \atop k \right\} G_N^{(k)}(2) \\
&= \sum_k \left\{ M \atop k \right\} 2^{-k} \sum_j \begin{bmatrix} k \\ j \end{bmatrix} h_j
\end{aligned}
$$

这里$\begin{bmatrix} \\ \end{bmatrix}$和$\left\{ \right\}$分别表示有符号的第一类斯特林数和第二类斯特林数。

于是总复杂度为$O(M \cdot N \cdot (K\text{的质因子个数}) \cdot 41 + M^2)$。

子任务8

仔细观察式子。

我们发现

$$
\begin{aligned}
C_{N,m}(y) &= \prod_{i=0}^{N-1} \prod_{j=1}^{l} ((p_j^{a_j})^m y^{p_j^{a_j}} - p_j^i (p_j^{a_j-1})^m y^{p_j^{a_j-1}}) \\
&= \prod_{j=1}^{l} (p^{a_j m N}) y^{p_j^{(a_j-1)N}} \prod_{i=0}^{N-1} (y^{p_j} - p_j^{i-m}) \\
&= (\prod_{j=1}^{l} (p^{a_j m N}) y^{p_j^{(a_j-1)N}}) \prod_{i=-m}^{N-m-1} \prod_{j=1}^{l} (y^{p_j} - p_j^i)
\end{aligned}
$$

前面的乘积是容易的。对于后面部分，我们考虑分治。

令$solve(l, r, D(y))$表示：现在有$D(y) = \prod_{i=-l}^{N-r-1} \prod_{j=1}^{l} (y^{p_j} - p_j^i)$（$-l > N - r - 1$时$D(y) = 1$），求解$h_l, \ldots, h_r$。

每次递归下去时维护$D(y)$。

这样总复杂度就是$O((N + M \log M) \cdot (K\text{的质因子个数}) \cdot 41 + M^2)$。

子任务9

我们考虑更一般的情况。

对于i维向量集合T和$i-1$维向量$\mathbf{u}$，令$I(\mathbf{u}, T) = \{a \in R | T\text{能表示}(\mathbf{u}, a)\}$。

可以发现$I(\mathbf{0}_{i-1}, T)$满足：

- $0 \in I$
- $\forall a \in I, b \in R, ba \in I$
- $\forall a_1 \in I, a_2 \in R, a_1 + a_2 \in I$

我们称这样的集合为R的一个左理想。

现在我们枚举每个左理想I_0，考虑$I(\mathbf{0}_{i-1},T)=I_0$的$T$。

对于任意$i-1$维的向量$\mathbf{u}$，观察$I(\mathbf{u},T)$（简记为I'）：

首先从子任务2的观察扩展，可以发现$\forall a_1,a_2\in I',a_1-a_2\in I_0$。

更一般地，如果存在函数$f:I'\to R$，使得$\sum_{a\in I'}f(a)=0$，则$\sum_{a\in I'}f(a)\cdot a\in I_0$（令$g(f)=\sum_{a\in I'}f(a)\cdot a$）。

我们发现这两个限制实际上是等价的。

> 必要性：
>
> $\forall a_1,a_2\in I'$，令$f(a_1)=1,f(a_2)=-1$，其他位置均为0。则$a_1-a_2\in I_0$。
>
> 充分性：
>
> 考虑归纳证明。
>
> 如果f处处为0，则$0\in I_0$。
>
> 否则f至少有两个位置不为0。不妨令其分别为a_1,a_2，则令$f'(a_1)=f(a_1)+f(a_2)$，$f'(a_2)=0$，其他位置$f'(a)=f(a)$。这样0的个数变多了。
>
> 通过归纳假设，$g(f')\in I_0$，那么$g(f)=g(f')+f(a_2)(a_2-a_1)\in I_0$。

任取一个$a\in I'$。

则$\forall a_0\in I',a-a_0\in I_0$且互不相同，于是$|I'|\le|I_0|$。

又有$\forall b\in I_0,a+b\in I'$且互不相同，于是$|I_0|\le|I'|$。

所以$|I_0|=|I'|$。

任取$a\in I'$，则I'可以表示为$\{a+b|b\in I_0\}$。

我们称这样的I'是群$(R,+)$的子群$(I_0,+)$的一个陪集，记为$a+I_0$。

陪集有一些有趣的性质：

- I_0的任意两个陪集要么不交，要么相等

证明：$\forall a_1,a_2\in R$，若a_1+I_0与a_2+I_0有交（设$a_1+i_1=a_2+i_2$），那么$\forall i_3\in I_0$，

$$a_2+i_3\in a_2+I_0$$
$$a_2+i_3=a_1+i_1-i_2+i_3\in a_1+I_0$$

- 群中的每个元素恰好在一个陪集中

证明：$a\in a+I_0$，且如果a在两个陪集中，则这两个陪集相等。

- 对于两个陪集，任取其中两个元素相加，和所在的陪集是确定的。

证明：$a_1+i_1+a_2+i_2\in(a_1+a_2)+I_0$。

（这里我们还可以得到一个推论，即$|I_0|$是$|R|$的因数。这可以略微降低复杂度）

那么我们可以先枚举每个基向量$\mathbf{base}$，讨论$I(\mathbf{base},T)$是I_0的哪一个陪集。基向量确定以后，其他的向量对应的陪集也就确定了：从每个基向量对应的陪集中选出一个，则可以求出该向量对应的陪集中的一个元素，进而可以确定这个陪集。

接下来考虑T的形态：每个$trans(T)$中的向量可以对应$|I_0|$个元素中的任意≥ 1个。

注意这里有可能算到$I(\mathbf{0}_{i-1},T)\subset I_0$的情况，所以需要容斥掉。

我们最后要求是$I(\mathbf{0}_{i-1},T)=R$。于是容斥系数$\alpha:\{I\subseteq R|I\text{是}R\text{的左理想}\}\to\mathbb{R}$需要满足

$$\sum_{I\subseteq I_1}\alpha(I_1)=[I=R]$$

枚举每个子集，判断其是不是左理想。然后可以快速莫比乌斯变换计算容斥系数。

实际上，可以发现$K\le 20$时R的加法群的子群个数是很少的（oeis），从而理想个数也很少。直接暴力计算容斥系数也可以。

最后式子形如

$$C_i(y)=(\sum_{I\text{是}R\text{的左理想}}\alpha(I)(|I|)^M(\frac{K}{|I|})^{i-1}y^{|I|})C_{i-1}(y)$$

后面的做法跟子任务8相同。

复杂度$O(2^KK^2+(N+M\log M)\cdot(K\text{的因子个数})\cdot 41+M^2)$。

参考资料

https://en.wikipedia.org/wiki/Ring_(mathematics)

https://en.wikipedia.org/wiki/Ideal_(ring_theory)

https://oeis.org/A061034