线性递推*

张晴川
qzha536@aucklanduni.ac.nz

August 20, 2020

Random Number Generator [1]

大意

给定线性递推数列初值：$A_1, A_2, \dots, A_K$，转移关系 $A_i = \sum_{j=1}^{K} C_j A_{i-j}$。

求 $A_N \bmod 104857601$（NTT 模数）。

数据范围

- $1 \le N \le 10^{18}$
- $0 \le A_i, C_i < 104857601$

题解

设 $v_0 = [A_1, A_2, \dots, A_K]^T$

由于是线性递推，必定存在一个转移矩阵 M，满足：

$$M^n v_0 = [A_{n+1}, A_{n+2}, \dots, A_{n+K}]^T$$

于是我们的目标就是求 M^{N-1} 的最低项。

按定义可以得到：

$$M^K v_0 = [A_{K+1}, A_{K+2}, \dots, A_{K+K}]^T$$

考虑右边的最低项 A_{K+1}，根据递推关系，我们有：

$$\begin{aligned} A_{K+1} &= \sum_{i=1}^{K} C_1 A_{K+1-i} \\ &= C_1 A_K + C_2 A_{K-1} + \dots + C_K A_1 \end{aligned}$$

*更多内容请访问：https://github.com/SamZhangQingChuan/Editorials

[1] https://www.codechef.com/problems/RNG

同理可得 $A_{K+2}, A_{K+3}, \ldots, A_{K+K}$ 也有类似关系。

于是我们得到了：

$$M^K v_0 = C_1 M^{K-1} v_0 + C_2 M^{K-2} v_0 + \cdots + C_K M^0 v_0$$

即：

$$(M^K - C_1 M^{K-1} - C_2 M^{K-2} - \cdots - C_K M^0) v_0 = 0$$

由于 v_0 其实可以是任意向量，$M^K - C_1 M^{K-1} - C_2 M^{K-2} - \cdots - C_K M^0$ 其实就是零矩阵。

设 $f(x) = x^{N-1}, g(x) = x^K - C_1 x^{K-1} - C_2 x^{K-2} - \cdots - C_K x^0$

那么必然存在商 $q(x)$ 和余数 $r(x)$ 满足 $f(x) = q(x)g(x) + r(x)$，其中 r 的次数低于 g 的次数。

由于 $f(M) = q(M)g(M) + r(M) = q(M)0 + r(M) = r(M)$，我们只需计算 $r(x)$。这可以通过快速幂计算，中间过程可以暴力平方取模，或者使用多项式的技巧取模，复杂度分别为 $O(\log(N)K^2)$ 和 $O(\log(N)K\log(K))$。

假设计算完之后，得到 $r(x) = \sum_{i=0}^{K-1} c_i x^i$，那么 $f(M) = \sum_{i=0}^{K-1} c_i M^i$。在 $0 \le i < K$ 的时候，$M^i v_0$ 的最低项其实就是初值 A_{i+1}。于是最终答案就是 $\sum_{i=0}^{K-1} c_i A_{i+1}$。

复杂度

- 时间：$O(\log(N)K\log(K))$
- 空间：$O(K)$

代码

https://gist.github.com/42403551c8080416af4b8f2baeaf5016