# 关于 xor 的 trick

黄知远, chatgpt

2025 年 10 月 21 日

## 目录



# 1 $[a,b]\oplus k$ 的结果形成 $O(\log n)$ 个区间

这个结论的证明以及代码实现需要用到 dyadic 分解.

## 1.1 dyadic 概念及性质

区间 $[a,b]$ 的 dyadic 分解是将其唯一地划分为若干个形如 $[x,x+2^t-1]$ 的子区间, 使得每个子区间的左端点 $x$ 满足 $2^t \mid x$.

对于任意非负整数 $t$ , 我们将区间 $[k2^t,(k+1)2^t-1]$ 定义为 $t$ 的一个对齐块. 定义函数 $F_p(k)$ , 表示将 $k$ 对应的对齐块中的元素与 $p$ 进行异或, 得到的数的集合.

**引理 1.** *$F_p(k)$ 一定是一个关于 $t$ 的对齐块.*

*证明.* 每一个对齐块一定包含前 $t$ 个二进制位的全排列, 因此在异或上某个数后, 前 $t$ 个二进制位会被映射成一个新的全排列, 而其余二进制位异或出的结果显然是相同的, 所以异或的结果任然是一个对齐块. □

**引理 2.** *dyadic 分解产生的区间有 $O(\log_2(b-a+1))$ 个.*

证明. 笔者不是数学专业的, 就写个感性证明了. 假设某一次删除了大小为 $2^t$ 的块, 那么下一次是可以选择大小为 $2^{t+1}$ 的块的, 因此选择的区间大小会不断翻倍, 那么大概只能选 $\log n$ 次. 但是有时 $b$ 的大小不允许我们选更大的块, 也就是说选择的块的大小开始下降了, 这一部分的操作次数和上升阶段是类似的, 所以最多也是只有 $\log n$ 次. 那么总的次数就是 $O(\log n)$ 次. □

**结论.** 由上述分析可知, 区间 $[a, b]$ 可被至多 $O(\log(b-a+1))$ 个 *dyadic* 块覆盖, 每个块都被异或操作映射到一个连续区间, 所以总共映射为 $O(\log(b-a+1))$ 个区间.

### 1.2 dyadic 分解的算法实现

假设当前有一个区间 $[a, b]$. 当 $a \le b$ 时, 执行以下步骤:

1. 找到最小的整数 $t$, 使得 $2^t \mid a$ 且 $a + 2^t - 1 \le b$;
2. 取出子区间 $[a,\ a + 2^t - 1]$;
3. 将 $a$ 更新为 $a + 2^t$, 继续上述过程, 直到 $a > b$.

$O((\log n)^2)$ 的做法是显然的.

## 2 $(kp+1)\oplus(p-1)$ 的单调性

**结论.** 对任意质数 $p$, 当 $k$ 取同一奇偶性时, $(kp+1)\oplus(p-1)$ 随 $k$ 严格单调增加.

证明. 令 $a = p-1$, $b_k = kp+1$, $A_k = b_k \,\&\, a$. 利用恒等式 $x \oplus y = x + y - 2(x \,\&\, y)$, 得

$$f(k) := b_k \oplus a = (kp+1) + (p-1) - 2A_k = (k+1)p - 2A_k.$$

若 $k_2 - k_1 = 2t$ 且 $t \ge 1$, 则

$$f(k_2) - f(k_1) = (k_2 - k_1)p - 2(A_{k_2} - A_{k_1}) = 2tp - 2\Delta A,$$

其中 $0 \le A_k \le p-1$, 故 $\Delta A \le p-1$. 因此

$$f(k_2) - f(k_1) \ge 2p - 2(p-1) = 2 > 0,$$

从而在相同奇偶性的 $k$ 上, $f(k)$ 严格递增. 对 $p = 2$ 的情形也成立. □