

推论 1 若 \mathbb{Z}_n 中含有一个无所不在的元素, 则用 r -电路计算 \mathbb{Z}_n 中的加法至少需要 $\lceil \log_r(2 \lceil \log_2 n \rceil) \rceil$ 个时间单位.

推论 2 若 \mathbb{Z}_n 中不存在无所不在的元素, H 是 \mathbb{Z}_n 的子群, H 中存在一个无所不在的元素, 则用 r -电路计算 \mathbb{Z}_n 中的加法至少需要 $\lceil \log_r(2 \lceil \log_2 |H| \rceil) \rceil$ 个时间单位.

定理 17.44 (1) $n = p^i$, p 为素数, i 为正整数, 则用 r -电路计算 \mathbb{Z}_n 中的加法至少需要 $\lceil \log_r(2 \lceil \log_2 n \rceil) \rceil$ 个时间单位.

(2) $n = p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k}$, 是 n 的素因子分解式, 则用 r -电路计算 \mathbb{Z}_n 中的加法至少需要 $\lceil \log_r(2 \lceil \log_2 t(n) \rceil) \rceil$ 个时间单位, 其中 $t(n) = \max\{p_1^{i_1}, p_2^{i_2}, \cdots, p_k^{i_k}\}$.