09-C6

词典

排解冲突：双向平方试探

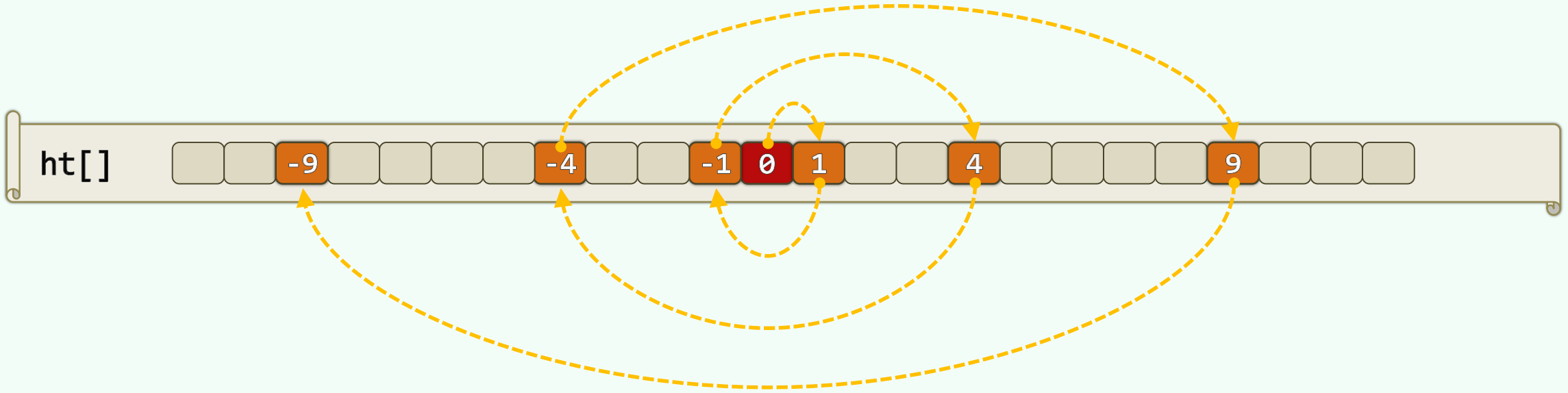
绕树三匝，何枝可依

伺候父亲躺下，我正准备离去，父亲拉住了我的手，轻轻地问我，丫儿，你知道什么是无枝可栖吗?

邓俊辉
deng@tsinghua.edu.cn

策略：交替地沿两个方向试探，均按平方确定距离

$$r_i(key) = (\ \mathrm{hash}(key) + (-1)^{i+1} \cdot (\lceil i/2 \rceil)^2\ ) \bmod \mathcal{M}, \quad i = 0, 1, 2, 3, \ldots$$



子试探链，彼此独立?

❖ 正向和反向的子试探链，各自包含 $\lceil \mathcal{M}/2 \rceil$ 个互异的桶

$$\underline{-\lfloor \mathcal{M}/2 \rfloor, \ldots, -3, -2, -1}, 0, \underline{1, 2, 3, \ldots, \lfloor \mathcal{M}/2 \rfloor}$$

$\pm i^2$		-36	-25	-16	-9	-4	-1	0	1	4	9	16	25	36
M	5					1	4	0	1	4				
	7				5	3	6	0	1	4	2			
	11		8	6	2	7	10	0	1	4	9	5	3	
	13	3	1	10	4	9	12	0	1	4	9	3	12	10

❖ 除了起点0，这两个序列是否还有...其它公共的桶?

4k + 3

❖ 两类素数：3 5 7 11 13 17 19 23 29 31

❖ 诀窍：表长取作素数 $\mathcal{M} = 4 \cdot k + 3$，即必然可以保证试探链的前 $\mathcal{M}$ 项均互异

± i²		-36	-25	-16	-9	-4	-1	0	1	4	9	16	25	36
M	5					1	4	0	1	4				
	7				5	3	6	0	1	4	2			
	11		8	6	2	7	10	0	1	4	9	5	3	
	13	3	1	10	4	9	12	0	1	4	9	3	12	10

❖ 反之，$\mathcal{M} = 4 \cdot k + 1$ 就...必然不能使用?

Two-Square Theorem of Fermat

❖ 素数 p 不能表示为一对整数的平方和，当且仅当

$$p \equiv 3 \pmod 4$$

❖ 只要注意到：

$$\begin{aligned}(\mathrm{u}^2+v^2)\cdot(s^2+t^2) &= (us+vt)^2+(ut-vs)^2\\ &= (us-vt)^2+(ut+vs)^2\end{aligned}$$

$$\begin{aligned}(2^2+3^2)\cdot(5^2+8^2) &= (10+24)^2+(16-15)^2\\ &= (10-24)^2+(16+15)^2\end{aligned}$$

❖ 就可以推知：

- 自然数 n 可表示为一对整数的平方和，当（且仅当）
- 它的每一 $\mathcal{M}=4\cdot k+3$ 类的素因子均为偶数次方

$$\begin{aligned}1 &= 1^2+0^2\\ 2 &= 1^2+1^2\\ 3 &=\\ 4 &= 2^2+0^2\\ 5 &= 2^2+1^2\\ 6 &=\\ 7 &=\\ 8 &= 2^2+2^2\\ 9 &= 3^2+\\ 10 &= 3^2+\\ 11 &=\\ &\vdots\end{aligned}$$