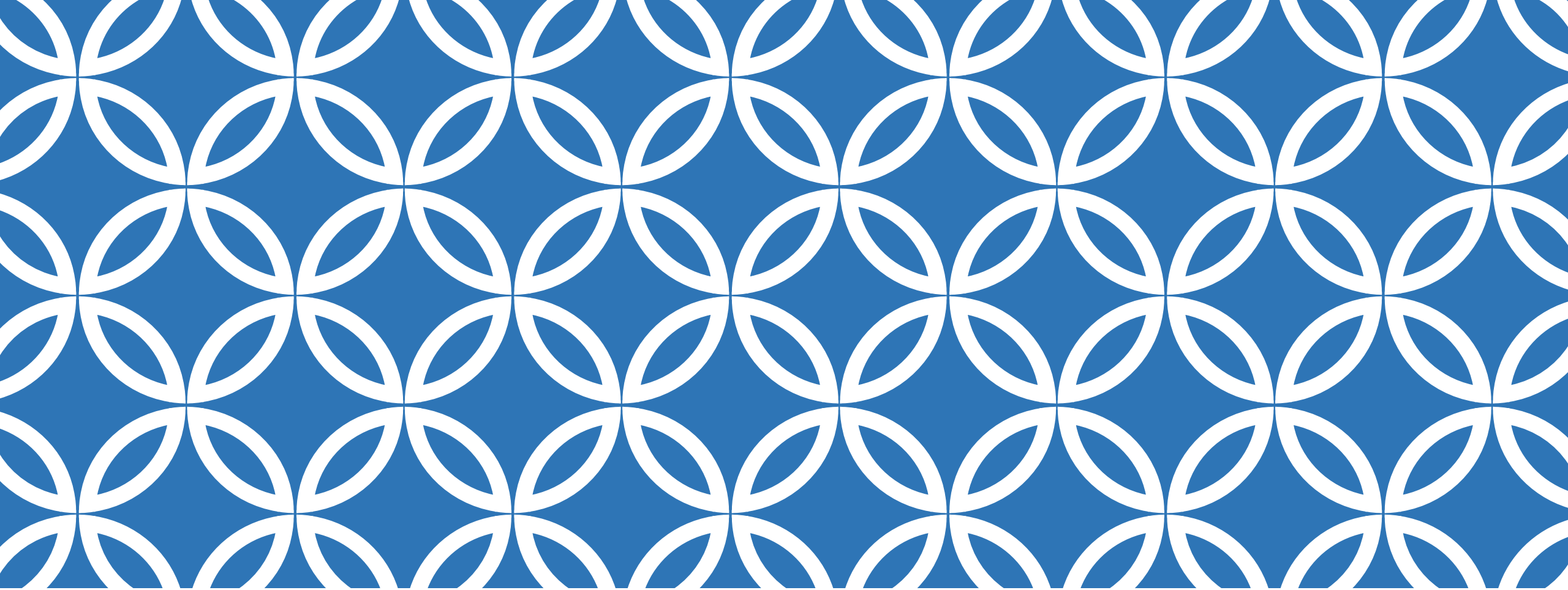


MEET IN THE MIDDLE

blue

问题

你有一个n个整数的集S.

问是否能从S中找到4个元素a, b, c, d，使得$a + b + c + d = 0$.

允许选取同一个元素多次。

$n \leq 1000$.

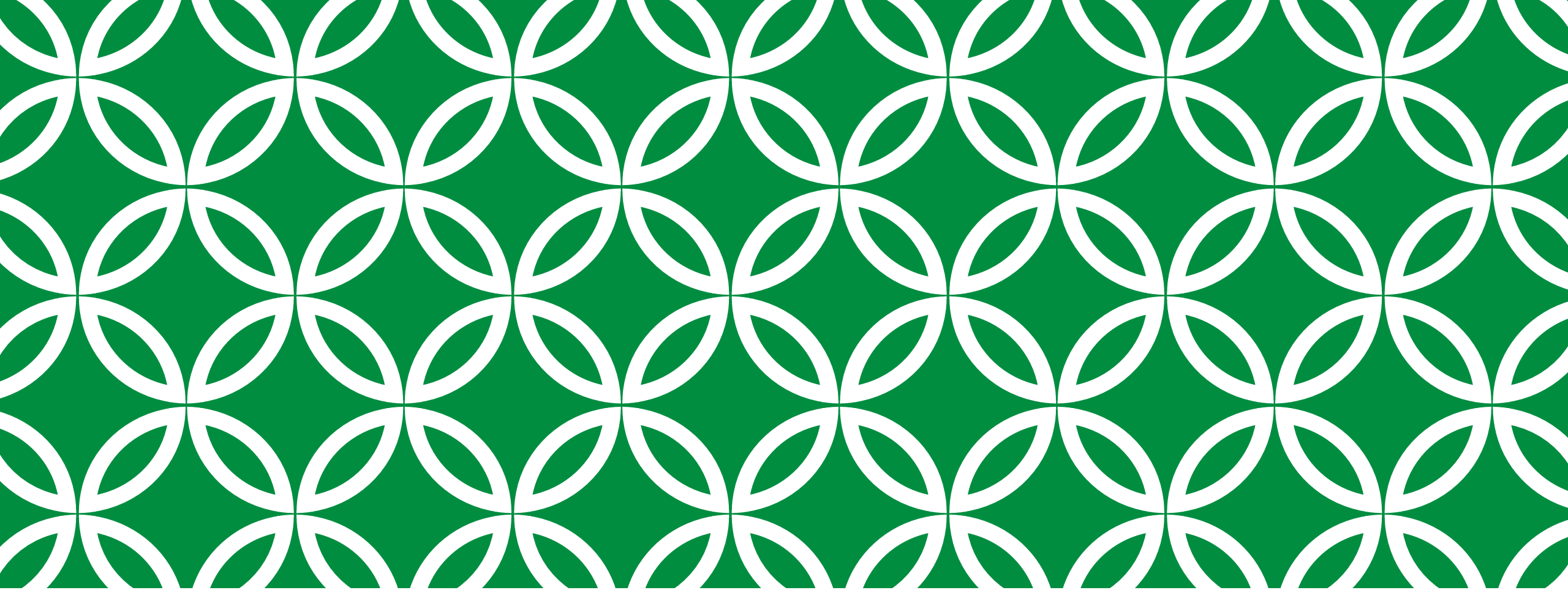
暴力

俗话说得好，想题先想暴力。

初级暴力：枚举a, b, c, d。复杂度$O(n^4)$.

高级暴力：枚举a, b, c，查询集合中是否存在$d = (-a) + (-b) + (-c)$

复杂度$O(n^3)$.



MITM

优化的暴力

正解

上面的问题正解是什么呢？

Step1. 枚举a,b，哈希存储$a+b$的结果。

代价$O(n^2)$.

Step2. 枚举a,b，查询上面的表中是否有$(-a)+(-b)$。

代价$O(n^2)$.

MITM

Meet-in-the-Middle.

就是个暴力。但是跑得比初级的暴力要快很多。

核心思想是分治。将大问题转化为两个小问题来暴力求解。

中间相遇。

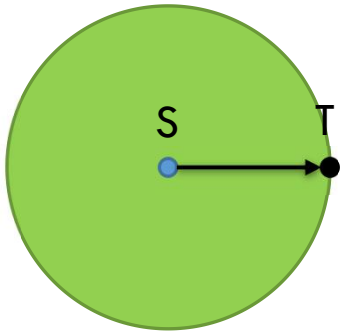
什么时候可以使用MITM?
问题可以“在中间相遇”的时候。

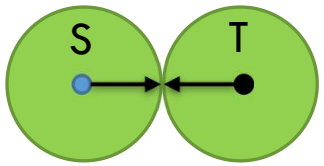
BFS

一般来说，广搜的搜索范围随着搜索层数递增。

那么，我们可以采用“双向广搜”的方式，来减少一些不必要的搜索过程。

单向



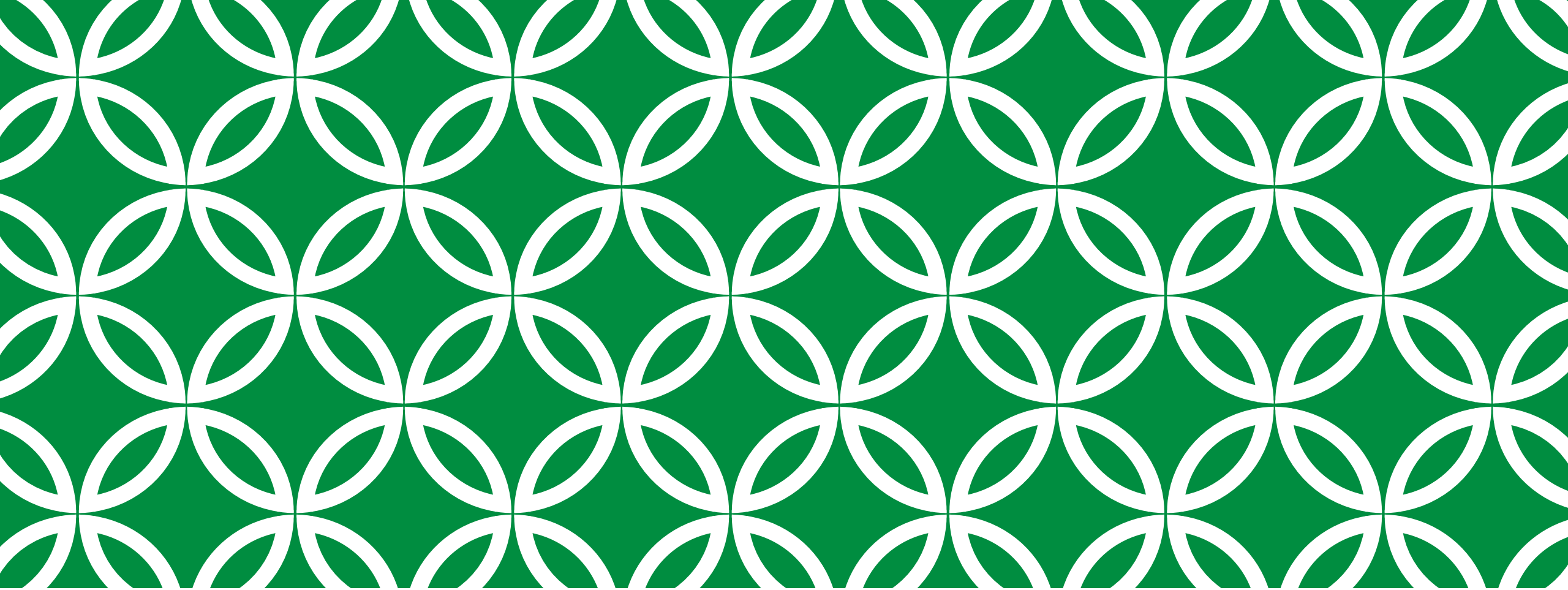


双向

MITM

双向广搜的思想，就是MITM。
现在是否明白了什么是“in the middle”？

将求解的东西分成两个部分。每部分都用暴力来解决。
例如最开始的题目，我们将a,b,c,d分成两组。



例题

切题时间到QAQ

你我只隔六步

给定一个社交网络（无向图）。

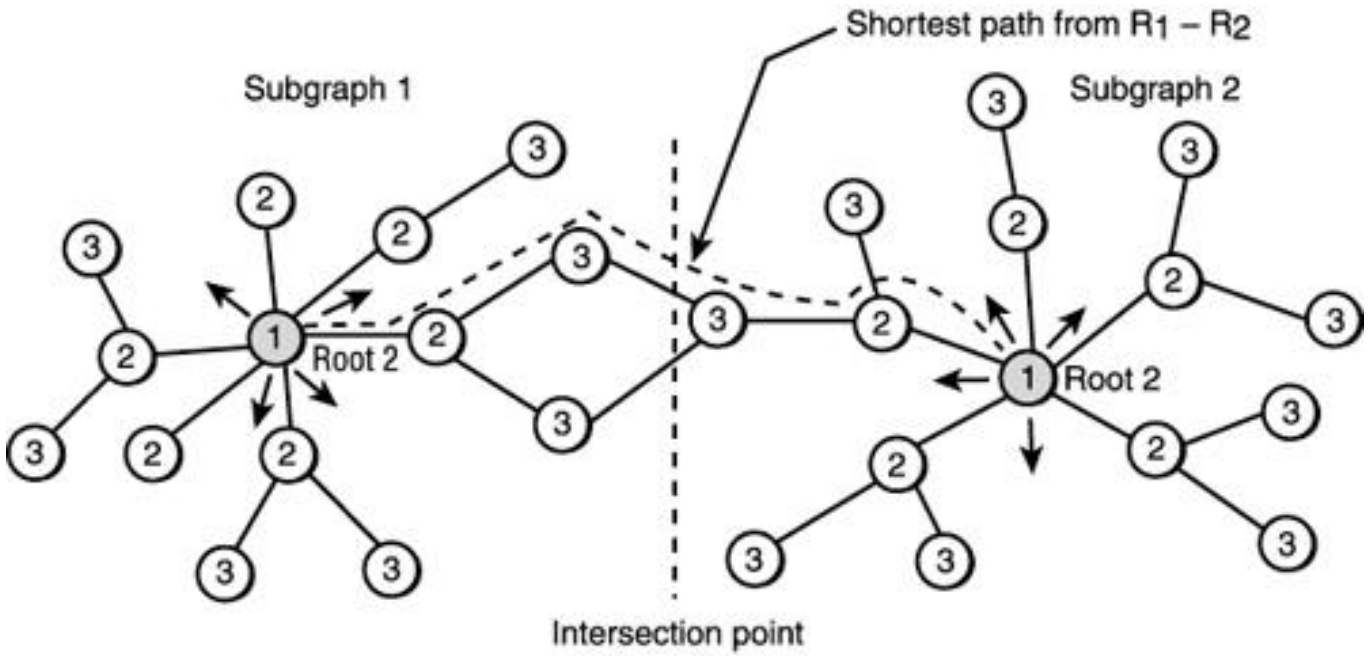
给出两个人的名字，回答这两个人是否最多相隔6个好友。

MITM

双向搜索。

在BFS的过程中，最多拓展3层。

搜索图


Shortest path from R1 – R2
Subgraph 1
Subgraph 2
Root 2
Root 2
Intersection point
Search 1 started from Root 1
Search 2 started from Root 2
Order of visitation: 1, 2, 3, . . .

分赃

你和blue合伙抢劫土豪Link，获得了40个金币，每个金币有相应的价值。

询问是否能把所有金币分成两堆，价值之和相同。

暴力

NP完全问题.现在人类没有找到多项式时间内的解法。

枚举每个硬币是放在A还是放在B。2^{40}次。

=1 099 511 627 776.

MITM

设总价值为$2w$，那么A堆的价值就是w.

如果A堆的价值是w,则B的价值也为w.

因此问题转变成：

从40个元素的集合中取出一些元素，使得价值和为w.

我们把序列随便分成两份，每份20个元素。

那么问题化为：

从A、B中各取若干个元素，使和为w.

对于集合A，枚举所有的元素和的取值，压进Hash表。
复杂度$O(2^{20})$.

对于集合B，枚举所有的元素和的取值K，
如果Hash表中有$(w-K)$，则判断有解。
复杂度$O(2^{20})$.

离散对数

弱化的离散对数问题：

给定质数n、正整数q，要求找出满足$p^k \equiv q\ (Mod\ n)$的正整数k.

为了弱化问题，只需要找到一个$1 \leq k \leq n$的解。

暴力

枚举k. 以$k-1$的状态推出k的状态.

复杂度$O(n)$.

MITM

考虑把k弄成两块，即$k = a\sqrt{n} + b$. 保证$0 \le a < \sqrt{n}, 0 \le b \le \sqrt{n}$.

原式化为：$p^{a\sqrt{n}} * p^b \equiv q\ (Mod\ n)$. 两边同除以$p^b$得：

$$p^{a\sqrt{n}} \equiv q * p^{-b}\ (Mod\ n)$$

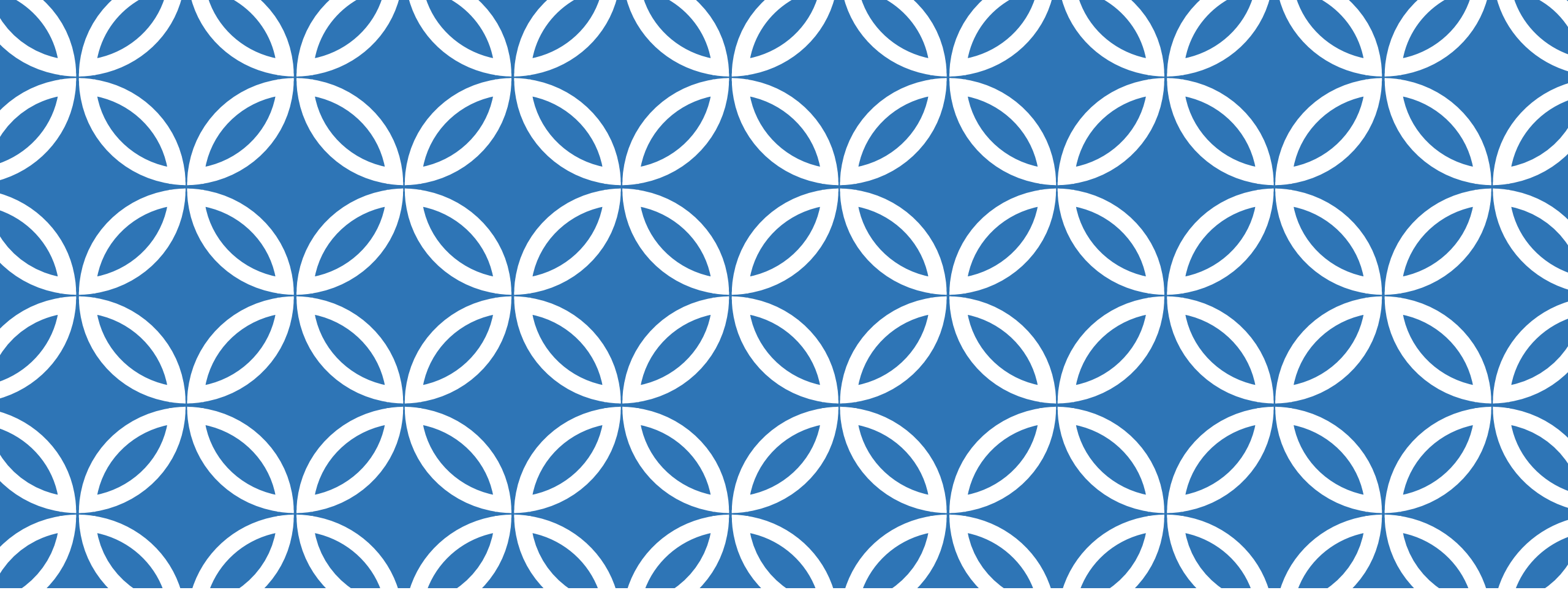
枚举a和b的值，就可以用$O(\sqrt{n})$的时间和空间复杂度解决问题。

负数次幂

如何计算$p^{-b}\ (Mod\ n)$?

$p^{-b} = (p^{-1})^b$,因此计算一次$p^{-1}\ (Mod\ n)$即可。
也就是求p在模n意义下的逆元。

扩展欧几里得算法。



END

blue