仿射密码的应用——记一次失败的解题经历

2025-09-25 原文链接

网站版本 1c934d989f84 · 文章 ID h_f0662722f45619ac

前几天，在群里看到一道题：

> n 位数里，19 的倍数，每位都不含 1 4 7 的数量，和不含 4 5 6 的数量一样多，这个怎么证?

第一想法就是构造双射，但当时没细想，忙别的事去了。今晚申强老师来问我，有没有看他的做法（只有 8 个字“了解一下仿射密码”）。

这里简单介绍一下仿射密码的概念，其实本质就是一种双射，和我的第一想法是一样的。

> **仿射密码**是一种替换密码。它是一个字母对一个字母的。它的加密函数是 $e(x) = ax + b \pmod{m}$，其中a和m互质，m是字母的数目。解码函数是 $d(x) = a^{-1}(x - b) \pmod{m}$，其中$a^{-1}$是a在$\mathbb{Z}_m$群的乘法逆元。[1]

顺着这个思路我开始思考以下几个问题：

1. 怎样的双射 f:x→ax+b，能将 {4,5,6} 映射到 {1,4,7}?

2. 这样的双射如何保证将 19 的倍数仍映射到 19 的倍数?

第一个问题比较好解决，f(x)=3x+3 就可以（这个系数 3 是容易得到的），但构造出的双射无法满足第二个要求，思路陷入了困境。

大强提示我可以构造从 {0,1,2,3,7,8,9} 到 {0,2,3,5,6,8,9} 的双射（本质似乎是一样的，原因是此时我还没意识到真正的问题所在）。

再次尝试未果，大强又给出了提示：映射就是 f(x)=3x，并问我应该模什么?

我立马顿悟了。要满足第二个要求，显然不能模 10，而应该模 19，并且构造的双射也应该是 f(x)=ax 的形式。

所以，是什么让我（以及没反应过来的读者们）在一开始就默认应该模 10 呢?

最后，放一道类似的能用仿射密码做的竞赛题（2021 年百年老校数学竞赛第 6 题）。

设质数 $p \geq 5$. 称 $1, 2, \cdots, p$ 的排列 $a_1, a_2, \cdots, a_p$ 为"好排列", 如果对 $1 \leq k \leq p$ 均有 $a_k \neq k$, 且 $a_1 + 2a_2 + \cdots + pa_p$ 是 p 的倍数. 求好排列的个数除以 $p^2 - p$ 的余数.