

- 书面作业讲解
 - TJ第7章练习3、7、9、12
 - TC第31.7节练习1、2
 - TC第31章问题2、3

TC第31.7节练习2

- $0 < d < \phi(n) \rightarrow 0 < ed < e\phi(n) = 3\phi(n) \rightarrow 0 < ed = k\phi(n) + 1 < 3\phi(n) \rightarrow k = 0, 1, 2 \rightarrow \phi(n)$ 至多有三个可能解
- $(p-1)(q-1) = \phi(n) \rightarrow pq - (p+q) + 1 = \phi(n) \rightarrow p+q = n+1 - \phi(n)$
- 再由 $pq = n \rightarrow p, q$ 是 $x^2 - (n+1 - \phi(n))x + n = 0$ 的两个根 \rightarrow 求根公式
(逐一尝试 $\phi(n)$ 的可能解, 直至找到 p, q 的整数可行解)
- 以上每一步都可在 n 的位数的多项式时间内完成

TC第31章问题2b

- $a = bq + r \rightarrow a \geq bq \rightarrow \lg a \geq \lg b + \lg q \rightarrow$
- $\mu(a, b) = (1 + \lg a)(1 + \lg b) \geq (1 + \lg b + \lg q)(1 + \lg b) \geq (1 + \lg b)^2 + \lg q(1 + \lg b) \rightarrow \lg q(1 + \lg b) \leq \mu(a, b) - (1 + \lg b)^2 \leq \mu(a, b) - (1 + \lg b)(1 + \lg r) = \mu(a, b) - \mu(b, r) = \mu(a, b) - \mu(b, a \bmod b)$
- 还需证明 $O(\lg q(1 + \lg b)) \subseteq O(\lg b(1 + \lg q))$
 - 实际上, $\lg q(1 + \lg b), \lg b(1 + \lg q) \in \Theta(\lg b \lg q)$

TC第31章问题3d

- 加法 $\Theta(\beta)$, 乘法 $\Theta(\beta^2)$
 - 方法1: 2^n 次加法
 - 方法2: n 次加法
 - 方法3: $\lg n$ 次（矩阵）乘法 + $\lg n$ 次（矩阵）加法

- 教材讨论
 - TJ第12、13、14章

问题1: general linear group

- 什么是general linear group?
 - all $n \times n$ invertible matrices, matrix multiplication
- 从线性空间的角度解释呢?
 - invertible linear transformations, composition
- 它为什么是一个群?

问题2: special linear group

- 什么是special linear group?
 - general linear group & determinant=1
- 它为什么是一个群?
- 它在二维空间上的几何意义是什么?
 - 保持面积不变
- 请你构造一个determinant=-1的矩阵, 试试看它是不是也能保持面积不变
- 你觉得determinant=1和determinant=-1在几何意义上有什么区别?
 - “方向”不同
- 你能不能在更简单的1维空间上解释这一区别?
- 在更复杂的三维空间上呢?

问题3: orthogonal group和isometry

- 什么是orthogonal group?
 - general linear group & $A^{-1}=A^t$
- 它为什么是一个群?
- 它的几何意义是什么?
 - 保持距离/长度/内积不变...
- isometry group的几何意义是什么?
 - 保持距离不变
- 那么orthogonal group和isometry group有什么区别?
 - 是否保持原点不变
- 在几何意义上, 你能举一个属于isometry group但不属于orthogonal group的变换吗?
 - translation

问题3: orthogonal group和isometry (续)

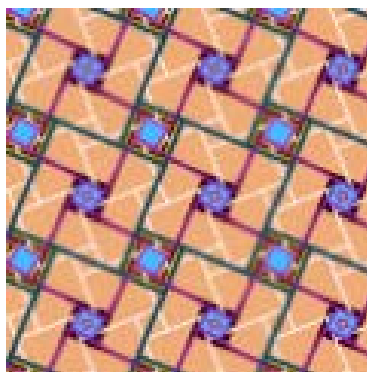
- 那么, 在几何意义上, orthogonal group中都是一些什么样的线性变换?
 - rotation (围绕原点)
 - reflection (对称轴过原点/原点对称)
- orthogonal group中的矩阵的行列式有什么特征?
 - determinant = ± 1
- 因此, 在几何意义上, orthogonal group和special linear group的交集special orthogonal group中都是一些什么样的线性变换?
 - rotation (围绕原点)
- 顺便问一下, 你能发现rotation和reflection之间的关系吗?
 - rotation = 两次reflection
- 现在你能抛开rotation, 只用reflection来解释orthogonal group和special orthogonal group吗?
 - reflection生成orthogonal group
 - 偶数次reflection生成special orthogonal group

问题4: symmetry group和wallpaper group

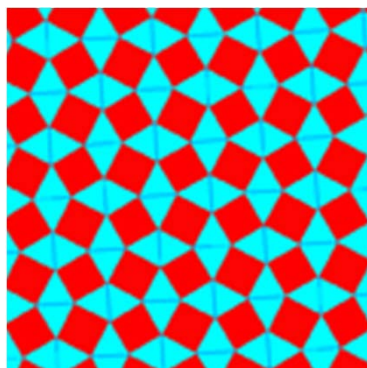
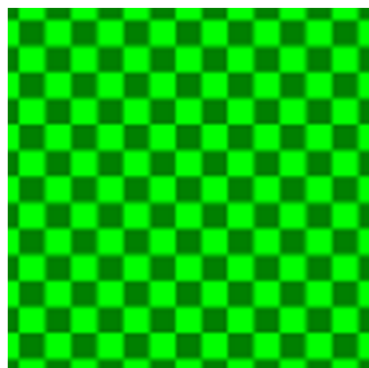
- 什么是symmetry group?
 - isometry group & some points fixed
- 刚才提到的这些群中，哪些是symmetry group?
 - general linear group
 - special linear group
 - orthogonal group
 - special orthogonal group
- 什么是wallpaper group? 它和symmetry group有什么关系?
 - 广义的symmetry group: some **objects** (e.g. points, **patterns**) fixed
- 两张wallpaper对应同一个wallpaper group, 是什么意思?

问题4: symmetry group和wallpaper group (续)

- 以下这些wallpaper对应同一个wallpaper group吗?



p4: 2种90度转点, 1种180度转点



p4m: 四向对称轴; 90度转点一定在对称轴上

p4g: 两向对称轴; 未必