模 m 剩余类环的单位群 $(\mathbb{Z}/m\mathbb{Z})^\times$ 是循环群的充要条件证明

一、充分性证明：当 $m = 1, 2, 4, p^k, 2p^k$ 时，$(\mathbb{Z}/m\mathbb{Z})^\times$ 是循环群

1. $m = 1$

- **分析**：$\mathbb{Z}/1\mathbb{Z}$ 的剩余类仅含一个元素 0，其单位群 $(\mathbb{Z}/1\mathbb{Z})^\times$ 是平凡群。
- **结论**：平凡群是循环群。

2. $m = 2$ 或 $m = 4$

- $m = 2$:
  - $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$，阶为 1，是平凡循环群。
- $m = 4$:
  - $(\mathbb{Z}/4\mathbb{Z})^\times = \{1, 3\}$，阶为 2，同构于 $\mathbb{Z}/2\mathbb{Z}$，是循环群。

3. $m = p^k$（p 为奇素数，$k \geq 1$）

- **原根存在定理**：对奇素数 p，存在模 p 的原根 g，其阶为 $p-1$。
- **提升到 p^k**（Hensel 引理）：
  - 若 g 是模 p 的原根且 $g^{p-1} \not\equiv 1 \pmod{p^2}$，则 g 是模 p^k 的原根。
  - 否则取 $g + p$ 作为模 p^k 的原根。
- **结论**：$(\mathbb{Z}/p^k\mathbb{Z})^\times$ 是循环群，生成元为原根 g。

4. $m = 2p^k$（p 为奇素数，$k \geq 1$）

- **中国剩余定理**：因 2 与 p^k 互质，有环同构：

$$\mathbb{Z}/2p^k\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p^k\mathbb{Z}.$$

- **单位群结构**：

$$(\mathbb{Z}/2p^k\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/p^k\mathbb{Z})^\times.$$

  - $(\mathbb{Z}/2\mathbb{Z})^\times$ 是平凡群（阶 1）。
  - $(\mathbb{Z}/p^k\mathbb{Z})^\times$ 是循环群（阶 $\varphi(p^k) = p^{k-1}(p-1)$）。
- **直积的循环性**：
  - 平凡群与循环群的直积仍为循环群。
  - 生成元为 $(1, g)$，其中 g 是 $(\mathbb{Z}/p^k\mathbb{Z})^\times$ 的原根。

二、必要性证明：若 $(\mathbb{Z}/m\mathbb{Z})^\times$ 是循环群，则 m 必为 $1, 2, 4, p^k, 2p^k$

1. 分解 m 为标准形式

设 $m = 2^k \cdot p_1^{k_1} \cdots p_n^{k_n}$，其中 $p_1, \ldots, p_n$ 为奇素数。
由 **中国剩余定理**，单位群分解为：

$$(\mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/2^k\mathbb{Z})^\times \times \prod_{i=1}^{n} (\mathbb{Z}/p_i^{k_i}\mathbb{Z})^\times.$$

2. 分析各因子群的循环性

- **条件**：循环群的直积仍为循环群 **当且仅当** 每个因子群是循环群，且它们的阶两两互质。

3. 排除非允许的因子

- **情形 1：存在两个不同的奇素数因子（$n \geq 2$）**
  - 若 m 含两个不同奇素数 p 和 q，则 $(\mathbb{Z}/p^k\mathbb{Z})^\times$ 和 $(\mathbb{Z}/q^l\mathbb{Z})^\times$ 的阶分别为 $\varphi(p^k)$ 和 $\varphi(q^l)$。
  - 由于 $\varphi(p^k) = p^{k-1}(p-1)$ 和 $\varphi(q^l) = q^{l-1}(q-1)$ 均为偶数，必不互质。
  - 直积非循环群，矛盾。
- **情形 2：m 含 2^k 且 $k \geq 3$**
  - $(\mathbb{Z}/2^k\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$（当 $k \geq 3$ 时）。
  - 这是两个非平凡循环群的直积，且它们的阶 2 和 2^{k-2} 不互质，故直积非循环群。
  - 因此 $k \leq 2$，即 m 中 2 的幂次至多为 2。
- **情形 3：m 仅含单个奇素数因子 p 和可能的因子 2**
  - 若 $m = 2p^k$，则分解为 $(\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/p^k\mathbb{Z})^\times$，前者为平凡群，后者为循环群。
  - 若 $m = p^k$，直接为循环群。
  - 若 $m = 4$，已验证为循环群。

模 m 剩余类群的单位群 $(\mathbb{Z}/m\mathbb{Z})^*$ 是循环群的充要条件证明

定理： $(\mathbb{Z}/m\mathbb{Z})^*$ 是循环群当且仅当 $m = 1, 2, 4, p^k, 2p^k$，其中 p 是奇素数，k 是正整数。

证明：

（一）必要性：如果 $(\mathbb{Z}/m\mathbb{Z})^*$ 是循环群，则 m 必须是 $1, 2, 4, p^k, 2p^k$ 之一。

我们将通过反证法证明。假设 m 不属于上述形式，我们将证明 $(\mathbb{Z}/m\mathbb{Z})^*$ 不是循环群。

1. **m 可以分解为两个互质的数：** 如果 m 可以分解为两个互质的数 $m = ab$，其中 $a > 2$ 且 $b > 2$，那么根据中国剩余定理，我们有：

   $(\mathbb{Z}/m\mathbb{Z})^* \cong (\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*$

   如果 $(\mathbb{Z}/a\mathbb{Z})^*$ 和 $(\mathbb{Z}/b\mathbb{Z})^*$ 都是循环群，那么它们的阶数分别是 $\phi(a)$ 和 $\phi(b)$，其中 ϕ 是欧拉函数。 由于 a > 2 和 b > 2，所以 $\phi(a)$ 和 $\phi(b)$ 都是偶数。 因此，$(\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*$ 中每个元素的阶都小于等于 $\operatorname{lcm}(\phi(a), \phi(b)) < \phi(a)\phi(b) = \phi(m)$。 这意味着 $(\mathbb{Z}/m\mathbb{Z})^*$ 不可能是循环群。

2. **m 的形式：** 因此，如果 $(\mathbb{Z}/m\mathbb{Z})^*$ 是循环群，那么 m 必须是 $p_1^{k_1}$ 的形式，或者 $2p_1^{k_1}的形式，其中p_1$ 是素数。

3. **排除 $m = 2^k$ 且 $k \geq 3$ 的情况：** 如果 $m = 2^k$ 且 $k \geq 3$，那么 $(\mathbb{Z}/2^k\mathbb{Z})^*$ 同构于 $\mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$。 这个群不是循环群，因为存在两个阶为 2 的元素，并且没有阶为 $\phi(2^k) = 2^{k-1}$ 的元素。

4. **排除 $m = p^k$ 且 p = 2, k >=3 的情况：** 已经排除

5. **排除 $m = 2p^k$ 且 p = 2, k >=3 的情况：** 已经排除

因此，如果 $(\mathbb{Z}/m\mathbb{Z})^*$ 是循环群，那么 m 必须是 $1, 2, 4, p^k, 2p^k$ 之一，其中 p 是奇素数，k 是正整数。

（二）充分性：如果 m 是 $1, 2, 4, p^k, 2p^k之一，则(\mathbb{Z}/m\mathbb{Z})^*$ 是循环群。

1. **m = 1, 2, 4：** $(\mathbb{Z}/1\mathbb{Z})^* = \{1\}$，$(\mathbb{Z}/2\mathbb{Z})^* = \{1\}$，$(\mathbb{Z}/4\mathbb{Z})^* = \{1, 3\}$。 这些群显然都是循环群。

2. **m = p^k，其中 p 是奇素数，k 是正整数：** 这是数论中的一个经典结果。 证明比较复杂，需要用到本原根的概念。 简要思路如下：

   - 证明存在模 p 的本原根 g，即 g 的阶为 p-1。
   - 证明存在模 p^2 的本原根 g'，且 g' 模 p 等于 g。
   - 通过归纳法，证明存在模 p^k 的本原根 g''，且 g'' 模 p^{k-1} 等于 g'。
   - 因此，$(\mathbb{Z}/p^k\mathbb{Z})^*$ 是循环群，生成元为 g''。

3. **m = $2p^k，其中p是奇素数，k是正整数：**如果g是模p^k的本原根，那么g也是模$2p^k$ 的本原根，或者 g + p^k 是模 $2p^k$ 的本原根。 具体来说：

- 如果 g 是奇数，那么 g 就是模 $2p^k$ 的本原根。
- 如果 g 是偶数，那么 g + p^k 是奇数，且 g + p^k 是模 $2p^k$ 的本原根。

因此，$(\mathbb{Z}/2p^k\mathbb{Z})^*$ 是循环群。

总结：

我们证明了 $(\mathbb{Z}/m\mathbb{Z})^*$ 是循环群当且仅当 $m = 1, 2, 4, p^k, 2p^k$，其中 p 是奇素数，k 是正整数。 证明过程结合了中国剩余定理、欧拉函数、本原根等数论知识。

注意： 本原根的存在性证明本身比较复杂，需要一定的数论基础。