组合数学作业 6

1. 证明:$\lceil \frac{n}{m} \rceil = \lfloor \frac{n+m-1}{m} \rfloor$, 其中, m,n 为整数

证明 这个结论在二者不要求为整数时是不正确的, 比如 $m = 10, n = 0.5$, 带入后得到 $LHS = 1, RHS = 0$/par 在 m, n 为整数时, 对于 $\frac{n}{m}$ 进行讨论

a.$\frac{n}{m} \in \mathbb{Z}$ 时:

设 $\frac{n}{m} = N$, 则

$$\begin{aligned} LHS &= \frac{n}{m} \\ RHS &= \lfloor \frac{n+m-1}{m} \rfloor = \frac{n}{m} + \lfloor \frac{m-1}{m} \rfloor = \frac{n}{m} \end{aligned}$$

b.$\frac{n}{m}$ 不为整数时不妨设 $n = qm + r$, 其中 $r \in \{1, 2, \ldots, m-1\}$

$$\begin{aligned} LHS &= q + 1 \\ RHS &= \lfloor \frac{qm + r + m - 1}{m} \rfloor \\ &= q + \lfloor \frac{r + m - 1}{m} \rfloor \\ &= q + 1 \end{aligned}$$

□

2. 对奇素数 p 和正整数 b 满足 $p \nmid b$, 证明:

$$(\frac{b}{p}) + (\frac{2b}{p}) + \cdots + (\frac{(p-1)b}{p}) = 0$$

证明 根据 Legendre 符号的性质, 有 $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ 于是, 原式等于

$$((\frac{1}{p}) + (\frac{2}{p}) + \cdots + (\frac{p-1}{p}))(\frac{b}{p}) = 0$$

而因为 $p \nmid b$, 所以, 只需证:

$$(\frac{1}{p}) + (\frac{2}{p}) + \cdots + (\frac{p-1}{p}) = 0$$

根据课上所讲的 Lemma

$$a^{\frac{p-1}{2}} \equiv 1 \, (mod \, p)$$

这个同余方程的解至多有 $\frac{p-1}{2}$ 个, 而 p 的二次剩余正好有 $\frac{p-1}{2}$ 个, 于是在 $1 \sim p-1$ 中, 恰有一半是上述同余方程的解, 另一半是 $a^{\frac{p-1}{2}} \equiv -1 \, (mod \, p)$ 的解, 于是我们证明了

$$(\frac{1}{p}) + (\frac{2}{p}) + \cdots + (\frac{p-1}{p}) = 0$$

显然, 我们可以进一步得到

$$((\frac{1}{p}) + (\frac{2}{p}) + \cdots + (\frac{p-1}{p}))(\frac{b}{p}) = 0$$

□

3. 利用二次互反律计算下列式子

a.$(\frac{60}{107})$

b.$(\frac{105}{139})$

解 对于 a, 对 60 进行质因数分解, 再根据 *Legendre* 符号的性质, 可以得到

$$(\frac{60}{107}) = (\frac{4}{107})(\frac{3}{107})(\frac{5}{107})$$

显然, $(\frac{4}{107}) = 1$, 根据二次互反律

$$(\frac{3}{107})(\frac{107}{3}) \equiv (-1)^{53} = -1$$

$$(\frac{107}{3}) = (\frac{2}{3}) = -1$$

$$(\frac{3}{107}) = 1$$

再次利用二次互反律

$$(\frac{5}{107})(\frac{107}{5}) = 1$$

$$(\frac{107}{5}) = (\frac{2}{5}) = -1$$

$$(\frac{5}{107}) = -1$$

综合以上结果, 我们可以得到

$$(\frac{60}{107}) = -1$$

对于 b, 采用同样的思路

$$(\frac{105}{139}) = (\frac{3}{139})(\frac{7}{139})(\frac{5}{139})$$

下面利用二次互反律分别计算三个子式

$$(\frac{3}{139})(\frac{139}{3}) = -1$$

$$(\frac{139}{3}) = (\frac{1}{3}) = 1$$

于是得到 $(\frac{3}{139}) = -1$

$$(\frac{5}{139})(\frac{139}{5}) = 1$$

$$(\frac{139}{5}) = (\frac{4}{5}) = 1$$

于是得到 $(\frac{5}{139})=1$

$$(\frac{7}{139})(\frac{139}{7})=-1$$

$$(\frac{139}{7})=(\frac{-1}{7})$$

又 Euler 判别准则

$$(\frac{-1}{7})\equiv(-1)^{\frac{7-1}{2}}=-1$$

于是得到 $(\frac{7}{139})=1$ 综合上述三个结果, 最终可以得到

$$(\frac{105}{139})=1$$

4. 利用 $(\frac{-2}{p})$ 证明:

$a.8k-3$ 型的素数有无穷多个

$b.8k+3$ 型的素数有无穷多个

证明 首先对 $(\frac{-2}{p})$ 进行讨论 (p 为奇素数), 由 Legendre 符号的性质, $(\frac{-2}{p})=(\frac{-1}{p})(\frac{2}{p})$, 根据课上的推导, 我们有以下结论

$$(\frac{-1}{p})=\begin{cases}1 & p=4k+1\\ -1 & p=4k+3\end{cases}\qquad(\frac{2}{p})=\begin{cases}1 & p=8k\pm1\\ -1 & p=8k\pm3\end{cases}$$

综合这两个结论, 我们可以得到

$$(\frac{-2}{p})=\begin{cases}1 & p=8k+1,8k+3\\ -1 & p=8k+5,8k+7\end{cases}$$

对于 a, 假设 $8k-3$ 型的素数只有 $p_1<p_2<\cdots<p_m$ 有限个, 考虑如下构造

$$p=2p_1^2p_2^2\cdots p_m^2+2$$

这时候考虑任意一个奇素因子 q, 设 $k=p_1p_2\cdots p_m$, 有

$$q|2k^2+2$$
$$q|4k^2+4$$

由此可以推出 $(\frac{-4}{q})=(\frac{-2}{q})(\frac{2}{q})=1$ 满足这样的奇素数 $p=8k+1,8k-3$, 但是根据构造, p 与任意 $8k-3$ 的素数互素, 于是推得 $p\equiv2\,(mod\,8)$, 但根据构造 $p\equiv4\,(mod\,8)$, 矛盾, 于是 $8k-3$ 型的素数有无穷多个

更正 这个证明有错误, 因为 p 中 2 的指数不一定是 1, 应该考虑如下构造

$$p=p_1^2p_2^2\cdots p_m^2+4$$

如此则有

$$q|k^2+4$$

由此可以推出 $(\frac{-4}{q})=(\frac{-2}{q})(\frac{2}{q})=1$ 满足这样的奇素数 $p=8k+1,8k-3$，但是根据构造，p 与任意 $8k-3$ 的素数互素，于是 $p\equiv 1\,(mod\,8)$，但是根据构造 $p\equiv 5\,(mod\,8)$，矛盾

对于 b，同样利用类似的思路，沿用 a 问的记号，假设 $8k+3$ 型的素数只有 $p_1<p_2<\cdots<p_m$ 有限个，考虑如下构造

$$p=2p_1^2p_2^2\cdots p_m^2+1$$

则 p 与 $p_1,p_2,\ldots,p_m$ 互素，设 q 是 p 的一个素因子，有

$$q|2k^2+1$$
$$q|4k^2+2$$

也即 $(\frac{-2}{p})=1$，根据 p 与 $p_1,p_2,\ldots,p_m$ 互素，则 q 只能是 $8k+1$ 型的素数，进而可以推得 $p\equiv 1\,(mod\,8)$ 但根据 p 的构造，$p\equiv 3\,(mod\,8)$，矛盾，于是 $8k+3$ 型的素数有无穷多个

□

5. *a. 对奇素数 p，计算 $(\frac{-3}{p})$*

b. 证明：$3k+1$ 型的素数有无穷多个

解 首先计算 $(\frac{-3}{p})$，根据 Legendre 符号，$(\frac{-3}{p})=(\frac{-1}{p})(\frac{3}{p})$

对于 $(\frac{-1}{p})$，根据 Euler 判别，$(\frac{-1}{p})=(-1)^{\frac{p-1}{2}}$，所以有

$$(\frac{-1}{p})=\begin{cases}1 & p=4k+1\\ -1 & p=4k-1\end{cases}$$

对于 $(\frac{3}{p})$，由二次互反律

$$(\frac{3}{p})(\frac{p}{3})=(-1)^{\frac{(p-1)(3-1)}{4}}=(-1)^{\frac{p-1}{2}}$$

所以我们推得

$$(\frac{3}{p})(\frac{p}{3})=\begin{cases}1 & p=4k+1\\ -1 & p=4k-1\end{cases}$$

对于 $(\frac{p}{3})$，对 $p\,(p\neq 3)$ 进行讨论，我们可以得到

$$(\frac{p}{3})=\begin{cases}1 & p=3k+1\\ -1 & p=3k-1\end{cases}$$

综合上述结论, 我们得到

$$(\frac{3}{p}) = \begin{cases} 1 & p = 12k+1, 12k-1 \\ -1 & otherwise \end{cases}$$

进而可以得到

$$(\frac{-3}{p}) = \begin{cases} 1 & p = 12k+1, 12k+7 \\ -1 & otherwise \end{cases}$$

下面证明 $3k+1$ 型的素数有无穷多个, 思路类似, 假设 $3k+1$ 型的素数只有 $p_1 < p_2 < \cdots < p_m$ 有限个, 沿用上一题的记号, 考虑如下构造

$$p = 3p_1^2 p_2^2 \cdots p_m^2 + 1$$

则对于 p 的任意一个奇素数 q, 满足

$$q | 3k^2 + 1$$
$$q | 9k^2 + 3$$

于是我们可以得到 $(\frac{-3}{q}) = 1$, 则 q 是 $12k+1, 12k+7$ 型的素数, 进一步我们可以得到 $p \equiv 2 (mod 12)$, 接下来考虑 $p_1 \sim p_m$, 因为它们都是 $3k+1$ 型的素数, 于是我们可以得到 $p \equiv 1, 7 \, (mod \, 12)$, 进而有 $p^2 \equiv 1 \, (mod \, 12)$, 根据 p 的构造我们有 $p \equiv 4 \, (mod \, 12)$, 矛盾, 所以 $3k+1$ 型的素数有无穷多个 更正 这个的证明和之前的更正有同样的错误, 应该考虑如下构造

$$p = 3p_1^2 p_2^2 \cdots p_m^2 + 4$$

于是我们可以得到

$$q | 3k^2 + 4$$
$$q | 9k^2 + 12$$

于是 $(\frac{-12}{q}) = (\frac{-3}{q})$, 所以 q 是 $3k+1$ 型的素数, 但是根据构造, p 与任意 $3k+1$ 型的任意素数互素, 矛盾

6. 设素数 $p \equiv 1 \, (mod \, 4)$, 证明 $\{1, 2, \ldots, p-1\}$ 中 p 的二次剩余之和为 $\frac{p(p-1)}{4}$

证明 根据题意, p 是 $4k+1$ 型的素数, 于是我们有 $(\frac{-1}{p}) = 1$, 我们有如下重要结论

$$(\frac{i}{p}) = (\frac{-i}{p}) = (\frac{p-i}{p})$$

此结论说明, i 和 $p-i$ 二者一定同时取, 再这个范围内的二次剩余一共有 $\frac{p-1}{2}$ 个, 于是所有的二次剩余和

$$S = \frac{1}{2} \times \frac{p-1}{2} \times p = \frac{p(p-1)}{4}$$

□

7. 证明: 在单位圆内任取 6 个点, 必有两个点的距离小于等于 1

证明 考虑将这个圆等分为 6 个扇形, 并且保证有一个点 P 在某个分界线上, 此时其他的点如果在以 P 所在半径为边的两个扇形内, 则存在两个点的距离不超过 1, 反之如果没有点在 P 相邻的两个扇形中, 则根据抽屉原理, 剩下四个扇形中一定至少有一个有两个点, 则这两个点的距离小于等于 1 □

8. 证明: 在边长为 1 的正方形内任取 9 个点, 至少有 3 个点组成的三角形面积小于等于 $\frac{1}{8}$

证明 考虑将这 9 个点中的其中 8 个连成一个 8 边形 (剩下的那个点在这个八边形中, 无所谓凹凸), 则这个 8 边形的端点和内部的点依次连接, 构成了 8 个不重叠的三角形, 如果对于任意三个点, 组成三角形的面积都大于 $\frac{1}{8}$, 则这个八边形的面积大于 1, 超出了这个单位正方形, 于是至少有 3 个点组成的三角形面积小于等于 $\frac{1}{8}$ □

证明 这个证明可能会在面临一些共线的情况时出现问题, 导致出现的图形不是八边形, 于是给出另一种证明

考虑将这个单位矩形等分为四个等面积的, 面积为 $\frac{1}{4}$ 的矩形, 由抽屉原理, 一定有三个点处于同一矩形内, 则这三个点所构成的三角形的面积不可能超过这个矩形的一半, 也即 $\frac{1}{8}$ □

9. 一个房间里有 10 个人, 他们当中没有人超过 60 岁 (年龄以整数给出, 至少 1 岁), 证明其中总存在两组人, 满足这两组人中不包含相同的人, 并且这两组人的年龄和相同

解 在这 10 个人之中, 一共有 1023 种分组, 而一组的年龄和一共有 $60 \times 10 = 600$ 种, 由抽屉原理, 一定有两种不同的分组, 他们的年龄和时相同的, 此时如果两组没有相同的人, 则得证, 如果有, 则两组同时将这个人删去, 仍然满足年龄和相同的条件

10. 一名学生有 37 天准备考试, 他需要准备的总时间不超过 60 小时, 并且她每天至少准备 1 小时, 假定她每天要准备的时间都是整数小时, 证明总存在连续的若干天, 期间她恰好学习了 13 小时

证明 设每天学习的时间为 $h_i, h_i \in \mathbb{N}^+$ 考虑前缀和 $S_k = \sum_{i=1}^{k} h_i$, 则依据题意, 我们有

$$1 \leq S_1 < S_2 < \cdots < S_{37} \leq 60$$

我们考虑 $S_1 + 13 < S_2 + 13 < \cdots < S_{37} + 13$, 一共有 $37 \times 2 = 74$ 个" 苹果", 但最多只有 $60 + 13 = 73$ 个抽屉, 于是必然有两个和大小相同, 根据前缀和的严格单调上升, 一定存在 $i < j, S_i + 13 = S_j$ □

11. 设有奇素数 p, q 和正整数 a, 满足 $p \nmid a$ 并且 $p \equiv \pm q \pmod{4a}$, 则 $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$