

组合数学作业

第 6 次

刘士祺 2017K8009929046

1. (2 分) 证明: 正整数 p 是素数当且仅当

$$(p-1)! \equiv -1 \pmod{p}$$

解: 必要性: 对于素数 p , 存在集合 $S = \{2, 3, 4, \dots, p-2\}$, 有 $\forall x \in S, \exists y \in S, xy \equiv 1 \pmod{p}$ 。
若 $\exists y_1, y_2, xy_1 \equiv xy_2 \equiv 1 \pmod{p}$, 则 $y_1 \equiv y_2 \pmod{p}$, 矛盾。故 $(p-1)! \equiv 1(p-1) \equiv -1 \pmod{p}$ 。
充分性: 设 $p = ab$, $a|(p-1)!$, 且 $b|(p-1)!$, 故若 $a \neq b$, $p|(p-1)!$, 矛盾。否则, $p = a^2$, $\gcd((p-1)!, p) \neq 1$, 矛盾, 故 p 为素数。 \square

2. (2 分) 证明: 若 a, b 是正整数, p 是素数, 则 $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

解: 由欧拉判别法, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$, 则有 $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}}b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod{p}$,
故 $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ \square

3. (2 分) $m(\geq n+1)$ 个球放在 n 个盒子 B_1, B_2, \dots, B_n 当中。现在把这 m 个球拿出来, 重新放入另外 $n+1$ 个新的盒子 $B_1^*, B_2^*, \dots, B_{n+1}^*$ 当中, 且每个新的盒子中至少有一个球。证明, 存在两个球, 每个都满足如下性质: 其所在的新盒子比其所在的旧盒子放入的球的个数更少。

解: 设 $m \geq n$, 有 $a^m - 1 = (a^{m-n} - 1)(a^n - 1) + (a^{m-n} - 1) + (a^n - 1)$, 设 $\gcd(a^m - 1, a^n - 1) = i$, $i|a^{m-n} - 1$, 设 $\gcd(a^n - 1, a^{m-n} - 1) = ki$, 故 $ki|a^m - 1$, 故 $\gcd(a^m - 1, a^n - 1) = ki$, 故 $k = 1$ 。
故 $\gcd(a^m - 1, a^n - 1) = \gcd(a^n - 1, a^{m-n} - 1)$, 该式可看作对 m, n 辗转相减, 故 $\gcd(a^m - 1, a^n - 1) = \gcd(0, a^{\gcd(m, n)} - 1) = a^{\gcd(m, n)}$ 。 \square

4. (2 分) p 是奇素数, 计算 $\left(\frac{-3}{p}\right)$ 。

解:

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

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & (3 | p-1) \\ -1 & (3 \nmid p-1) \end{cases}$$

\square

5. (1 分) 证明: 对于素数 $p > 2$, $\binom{2p}{p} \equiv 2 \pmod{p}$

解: 由卢卡斯定理

$$\binom{2p}{p} \equiv \binom{2}{1} + \binom{0}{0} \equiv 2 \pmod{p}$$

\square

6. (2 分) 对于素数 p 定义 $h_p(n)$ 为 $n!$ 中素数因子 p 的个数, 求证 $h_p(2n) \geq 2h_p(n)$ 。

解: 由

$$h_p(n) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{i^p} \right\rfloor$$

和

$$h_p(2n) = \sum_{i=1}^{\infty} \lfloor \frac{2n}{ip} \rfloor$$

又有设 $n = pk + r, 0 \leq r < k$, 有 $p = \lfloor \frac{n}{k} \rfloor$, 又 $2n = 2pk + 2r$, 故 $\lfloor \frac{2n}{k} \rfloor = 2p$ 或 $2p + 1 \geq 2p$ 。故

$$\sum_{i=1}^{\infty} \lfloor \frac{2n}{ip} \rfloor \geq 2 \sum_{i=1}^{\infty} \lfloor \frac{n}{ip} \rfloor$$

即 $h_p(2n) \geq 2h_p(n)$

□

7. (2 分) 证明: 任给 $m, n \in \mathbb{N}$, 都有 $m!n!(m+n)!|(2m)!(2n)!$ 。

解: 设 $S(m, n) = \frac{(2m)!(2n)!}{m!n!(m+n)!}$, 有

$$\begin{aligned} & S(m, n+1) + S(m+1, n) \\ &= S(m, n) \frac{2(2n+1)}{(m+n+1)} + S(m, n) \frac{2(2m+1)}{(m+n+1)} \\ &= 4S(m, n) \end{aligned}$$

故 $S(m, n+1) = 4S(m, n) - S(m+1, n)$, 又 $S(m, 0) = \frac{(2m)!}{m!} \in \mathbb{Z}$, 故 $\forall m, n, S(m, n) \in \mathbb{Z}$, 故 $m!n!(m+n)!|(2m)!(2n)!$ 。

□

8. 设集合 $A, B \in \mathbb{Z}$, 定义集合 $A+B = \{a+b | a \in A, b \in B\}$ 。证明: $|A+B| \geq |A| + |B| - 1$

解: 67 是素数故 $(\frac{20}{67}) \equiv 20^{\frac{67-1}{2}} \equiv -1 \pmod{67}$

□