组合数学作业

第 5 次

刘士祺 2017K8009929046

1. *(2 分)* 快速排序的期望时间复杂度有如下递推:

$$T(n) = \frac{1}{n}\sum_{k=0}^{n-1}(T(k) + T(n-k-1)) + O(n)$$

求证 $T(n) = O(n \cdot log(n))$。

解: 由

$$T(n) = \frac{1}{n}\sum_{k=0}^{n-1}(T(k) + T(n-k-1)) + O(n)$$

知

$$T(n) = \frac{2}{n}\sum_{k=0}^{n-1}T(k) + O(n)$$

故

$$nT(n) = 2\sum_{k=0}^{n-1}T(k) + O(n^2)$$

用 $T(n)$ 减去 $T(n-1)$ 得

$$\begin{aligned} nT(n) - (n-1)T(n-1) &= 2T(n-1) + O(n) \\ nT(n) - (n+1)T(n-1) &= O(n) \\ \frac{T(n)}{n+1} - \frac{T(n-1)}{n} &= O(\frac{1}{n}) \\ \frac{T(n)}{n+1} &= O(log(n)) \\ T(n) &= O(n \cdot log(n) \end{aligned}$$

□

2. *(2 分)* 证明:$\forall a, b \in \mathbb{N}, \exists p, q \in \mathbb{Z}, ap + bq = gcd(a, b)$。

解: 设 d 为集合 $\mathbb{S} = \{ax + by|x, y \in \mathbb{Z}, ax + by \geq 0\}$ 中的最小值 $ap+bq$。设 $a = dx+r, 0 \leq r < a$, 由 $r = a - xd = a - x(ap + bq) = a(1 - xp) - bxq$, 又 $r \in \mathbb{S}$, d 为 $\mathbb{S}$ 中最小正数，故 $r = 0$, 故 $d|a$, 同理, $d|b$。

对 $\forall i, i|a\&i|b$, 设 $a = mi, b = ni$, $d = ap + bq = i(mp + nq)$, 故 $i|k$, 故 $k = gcd(a, b)$。 □

3. *(2 分)* 证明 $\forall a > 1, m, n \in \mathbb{N}, gcd\,(a^m-1, a^n-1) = a^{gcd(m,n)}-1$。

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 $gcd(a^m - 1, a^n - 1) = gcd(0, a^{gcd(m,n)} - 1) = a^{gcd(m,n)}$。 □

4. *(2 分)* 已知 $\{F_n\}_{n=1}^{\infty}$ 是 Fibonacci 数列, 证明 $\forall m, n \in \mathbb{N}, gcd(F_m, F_n) = F_{gcd(m,n)}$。

解: 由于 $F_{m+n} = F_mF_{n+1} + F_{m+1}Fn$, 带入 $m = m - n, n = n$, 故 $F_m = F_{m-n}F_{n+1} +$

$Fm-n+1F_n$, 设 $gcd(F_m,F_n)=i$, $i|F_{m-n}$(由 $gcd(F_{n+1},F_n)=1$), 故 $i=gcd(F_{m-n},F_n)$(否则, 若 $ki=gcd(F_{m-n},F_n), k>1$, $ki|F_m$, 矛盾。
故 $gcd(F_m,F_n)=gcd(F_{m-n},F_n)$, 同理可证, $gcd(F_m,F_n)=F_{gcd(m,n)}$。 □

5. *(1 分)* 证明: 对于素数 $p>2$, $\binom{2p}{p}\equiv 2(mod\ p)$
解: 由卢卡斯定理
$$\binom{2p}{p}\equiv\binom{2}{1}+\binom{0}{0}\equiv 2(mod\ p)$$
□

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
$$h_p(n)=\sum_{i=1}^{\infty}\lfloor\frac{n}{ip}\rfloor$$
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. 计算下列式子, 其中 $(\frac{a}{p})$ 表示 Legendre 符号, 即如果 a 是 p 的二次剩余, 则 $(\frac{a}{p})=1$, 如果 a 是 p 的二次非剩余, 则 $(\frac{a}{p})=-1$

   a) *(1 分)* $(\frac{20}{67})$
   解: 67 是素数故 $(\frac{20}{67})\equiv 20^{\frac{67-1}{2}}\equiv -1(mod\ 67)$ □

   b) *(1 分)* $(\frac{14}{73})$
   解: 73 是素数故 $(\frac{14}{73})\equiv 14^{\frac{73-1}{2}}\equiv -1(mod\ 73)$ □

9. *(2 分)* $p=6k+5(k\in\mathbb{N})$ 是素数, 计算 $(\frac{-3}{p})$。
解

□

10. 将 $1 \sim 2n$ 填入 $2 \times n$ 的杨氏图表 (即要求图表中每行每列均单调递增), 有多少种不同的方案?

解: 设有 $s(n)$ 种方案, 左上角必为 1, 右下角必为 $2n$, 若 $2n$ 的上面为 $2n-1$, 则左面为 $2n-2$, 去掉最后两个, 方法数共为 $s(n-1)$, 若左面为 $2n-1$, 设上面为 $b(n \le b < 2n-1)$, 将 $b+1$ 换为 b, $b+2$ 换为 $b+1$ …, b 换为 $n-1$, 化为前一种情况。故 $s(n) = s(n-1) + (n-1)s(n-1) = ns(n-1)$ 又 $s(1) = 1$ 故 $s(n) = n!$。 $\square$