Elementary Number Theory: Homework2

刘泓尊　2018011446　计 84

2020 年 4 月 2 日

Exercises 3.1

8. 证明整数 $Q_n = n! + 1$ 有一个大于 n 的素因子, $n \in \mathbb{Z}^+$(可以推出存在无穷多个素数)

证明. 因为 $Q_n > 1$，所以由 Lemma 3.1，Q_n 有一个素因子 p. 下面采用反证法，假设 $p \le n$, 则 $p \mid n!$, 则 $p \mid Q_n - n! = 1$，p 不是素数，矛盾! 所以 $Q_n = n! + 1$ 有一个大于 n 的素因子。
利用此结论可以证明素数的无穷性: 设 p_1 是 Q_1 的素因子，那么有 $p_1 > 1$，所以存在 p_2 是 Q_{p_1} 的素因子。故而存在 p_{i-1} 是 Q_{p_i} 的素因子。因此我们得到了无穷素数列 $p_1, p_2, \cdots, p_n, \cdots$, 所以素数有无穷多个。 □

9. 是否能够通过观察整数 $S_n = n! - 1$ 来证明无限多个素数?

证明. 当 $n \ge 3$ 时，$S_n > 1$, 有一个素因子 p。如果 $p \le n$ 则 $p \mid n! - S_n = 1$，即 $p = 1$，矛盾! 所以 $p > n$.
类似 3.1.8 的方法，可以得出有无限多个素数。 □

10. 用欧几里得对素数无限多的证明说明: 第 n 个素数 $p \le 2^{2^{n-1}}, n \in \mathbb{Z}^+$. 由此证明 $n \in \mathbb{Z}^+$ 时，小于 2^{n^n} 的素数至少有 $n+1$ 个

证明. 采用数学归纳法:
基础: $n = 1$ 时，$p_1 = 2 \le 2^{2^0} = 2$.
假设: $\forall k < n$，有 $p_k < 2^{2^k}$.
递推: 根据 Euclid 的证明，存在 $q \ne p_1, p_2, \cdots, p_n$，使得 $q \mid Q_n = p_1 p_2 \cdots p_n + 1$. 所以 $p_n < q \le Q_n = p_1 p_2 \cdots p_n + 1 < 2^{2^0} 2^{2^1} \cdots 2^{2^{n-1}} + 1 = 2^{2^0 + 2^1 + \cdots 2^{n-1}} + 1 = 2^{2^{n-1} - 1} + 1$.
即 $p_n \le 2^{2^{n-1} - 1} \le 2^{2^{n-1}}$.
接下来证明第二个命题:
假设: 小于 2^{n^n} 的素数只有少于 n 个. 那么对于第 $n+1$ 个素数 p_{n+1}，有 $p_{n+1} \le 2^{2^n}$。因为 p_{n+1} 必定为奇数，所以实际上 $p_{n+1} < 2^{2^n}$，矛盾。所以小于 2^{n^n} 的素数至少有 $n+1$ 个。 □

11. 令 $Q_n = p_1 p_2 \cdots p_n + 1$，其中 $p_1, p_2, \cdots, p_n$ 是前 n 个素数。对于 $n = 1, 2, 3, 4, 5, 6$ 给出 Q_n 的最小素因子。

证明. $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11, p_6 = 13$
$Q_1 = 3, Q_2 = 7, Q_3 = 31, Q_4 = 211, Q_5 = 2311, Q_6 = 30031$

设 Q_n 的最小素因子为 q_n，则:
$q_1 = 3, q_2 = 7, q_3 = 31, q_4 = 211, q_5 = 2311, q_6 = 59$ □

Exercises 3.3

14. 证明: 如果整数 a, b, c 使得 $(a, b) = 1$ 且 $c \mid (a + b)$, 那么 $(c, a) = (c, b) = 1$.

证明. 因为 $c \mid (a+b)$, 所以存在正整数 k 使得 $(a+b) = kc$。设 $p \mid a$ 且 $p \mid c$，则 $p|b = kc - a$，即 $p|(a, b) = 1$，所以 $p = 1$。即 $(a, c) = (b, c) = 1$ □

15. 证明: 如果非零整数 a, b, c 互素, 那么 $(a, bc) = (a, b)(a, c)$

证明. 设 $d = (a, b)$。则 $(a/d, b/d) = 1$. 下证 $(a/d, bc/d) = (a, c)$:
设 $e = (a/d, bc/d)$，则 $e \mid a/d$，所以 $(e, b/d) = 1$，所以 $e \mid c$。又因为 $e \mid a/d$, 所以 $e \mid a$，所以 $e \mid (a, c)$。设 $f = (a, c)$，则 $(f, b) = 1$, 进而 $(f, d) = 1$. 所以 $f \mid a/d$ 且 $f \mid bc/d$。所以 $f \mid e$。因为 $e \mid f = (a, c)$, 所以 $f = e$. 所以 $(a, b)(a, c) = de = d(a/d, bc/d) = (a, bc)$ □

16.

(a). 证明: 如果整数 $a, b, c, (a, b) = (a, c) = 1$，那么 $(a, bc) = 1$

证明. 存在整数 m, n, s, t 使得 $ma + nb = 1$, $sa + tc = 1$. 则 $1 = (ma + nb)(sa + tc) = (msa + nbs + mtc)a + (nt)bc$，所以 $(a, bc) = 1$ □

(b). 用数学归纳法证明，如果对整数 $a_1, a_2, \cdots, a_n$，有另一整数 b, 使得 $(a_1, b) = (a_2, b) = \cdots = (a_n, b) = 1$，那么 $(a_1 a_2 \cdots a_n, b) = 1$.

证明. 若 $(a_i, b) = 1, \forall i = 1, 2, \cdots, n$. 令 $A_i = \prod_{k=1}^{i} a_k$. 下面用数学归纳法证明 $(A_n, b) = 1$:
基础: $n = 2$ 时, 由 (a) 可知正确。
假设: $n = k$ 时 $(A_k, b) = 1$
递推: $n = k + 1$ 时, 因为 $(a_{k+1}, b) = 1$ 且 $(A_k, b) = 1$，
由 (a) 可知 $(A_{k+1}, b) = (A_k a_{k+1}, b) = 1$ □

Exercises 3.5

37.

(a). $[a, b] \mid c$ 当且仅当 $a \mid c$ 且 $b \mid c$

证明. 必要性: 因为 $[a, b] \mid c$, $a \mid [a, b]$, 所以 $a \mid c$。同理 $b \mid c$
充分性: 对 a, b, c 做最小素分解, $a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$,$b = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$,$c = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$. 若 $a \mid c$ 且 $b \mid c$，则 $r_i \leq c_i, s_i \leq c_i$，进而 $\max(r_i, s_i) \leq c_i$，
所以 $[a, b] = p_1^{\max(s_1, r_1)} p_2^{\max(s_2, r_2)} \cdots p_k^{\max(s_k, r_k)} \mid c$，即 $[a, b] \mid c$ □

(b). $[a_1, a_2, \cdots, a_n] \mid d$ **当且仅当** $a_i \mid d, i = 1, 2, \cdots, n$**.**

证明. 必要性: 因为 $[a_1, a_2, \cdots, a_n] \mid d$, $a_i \mid [a_1, a_2, \cdots, a_n]$, 所以 $a_i \mid d, i = 1, 2, \cdots, n$
充分性: 对 a_i, d 做最小素分解 $i = 1, 2, \cdots, n$.
$a_i = p_1^{r_{i_1}} p_2^{r_{i_2}} \cdots p_k^{r_{i_k}}$, $d = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$. 若 $a_i \mid d$, 则 $r_{i_k} \leq s_k$, 进而 $\max(r_{1_k}, r_{2_k}, \cdots, r_{n_k}) \leq s_k$,
所以 $[a_1, a_2, \cdots, a_n] = p_1^{\max(r_{1_1}, r_{2_1}, \cdots, r_{n_1})} p_2^{\max(r_{1_2}, r_{2_2}, \cdots, r_{n_2})} \cdots p_k^{\max(r_{1_k}, r_{2_k}, \cdots, r_{n_k})} \mid d$,
即 $[a_1, a_2, \cdots, a_n] \mid d$ □

38. 若 p **为素数,** $p \mid a^2$**, 则** $p \mid a$

证明. 由 Lemma 3.5，若 p 为素数，$p \mid a^2 = |a| \cdot |a|$，则有 $p \mid |a|$，进而 $p \mid a$. □

39. 证明: 若 $p \mid a^n$**, 则** $p \mid a$

证明. 由 Lemma 3.5，若 p 为素数，$p \mid a^n = \pm|a||a| \cdots |a|$，则有 $p \mid |a|$，进而 $p \mid a$. □

40. 证明: 若 $c \mid ab$**, 则** $c \mid (a, c)(b, c)$

证明. 采用反证法:
假设 $c \nmid (a, c)(b, c)$，则 $c \nmid (a, c)$ 且 $c \nmid (b, c)$。因为 $c \mid c$, 所以 $c \nmid a$, $c \nmid b$. 进而 $c \nmid ab$, 矛盾！
所以 $c \mid (a, c)(b, c)$. □

41.

(a). 若 $(a, b) = 1$**，则** $(a^n, b^n) = 1, \forall n$**.**

证明. 因为 $(a, b) = 1$, 设 $p \mid (a^n, b^n)$，下证 $p = 1$:
因为 $p \mid a^n, p \mid b^n$，所以由 3.5.39 题: $p \mid a, p \mid b$，进而 $p \mid (a, b) = 1$，所以 $p = 1$. □

(b). 若 $a^n \mid b^n$**，则** $a \mid b$**.**

证明. 采用反证法:
假设 $a \nmid b$，则存在素数幂 $p^k \mid a$, $p^k \nmid b$. 设 $a = p^k a'$, 则 $a^n = p^{nk} a'^n$，所以 $p_{kn} \mid a^n \mid b^n$. 所以 $b^n = b' p^{kn}$, 一定有 $b = \sqrt[n]{b'} p^k$. 矛盾!
所以 $a \mid b$. □

64. 若 $a_1, a_2, \cdots, a_n$ **两两互素, 则** $[a_1, a_2, \cdots, a_n] = a_1 a_2 \cdots a_n$

证明. 采用数学归纳法:
基础: $[a_1, a_2] = a_1 a_2 / (a_1, a_2) = a_1 a_2$
假设: 若 $a_1, a_2, \cdots, a_{n-1}$ 两两互素, 则 $[a_1, a_2, \cdots, a_{n-1}] = a_1 a_2 \cdots a_{n-1}$
递推: 对于 n，$[a_1, a_2, \cdots, a_n] = [[a_1, a_2, \cdots, a_{n-1}], a_n] = [a_1 a_2 \cdots a_{n-1}, a_n] = a_1 a_2 \cdots a_n$ □