

T1. 证明：若 $a \mid b$ 且 $c \mid d$, 则 $ac \mid bd$.

证明：由 $a \mid b$ 且 $c \mid d$, 存在 $q_1, q_2 \in \mathbb{Z}$, 使得 $b = aq_1, d = cq_2$.

则 $bd = aq_1 \cdot cq_2 = (ac)(q_1q_2)$, 即存在 $q = q_1q_2$ 使得 $bd = acq$,
所以 $ac \mid bd$.

T2. 设 $n \neq 1$, 证明: $(n-1)^2 \mid n^k - 1 \Leftrightarrow (n-1) \mid k$.

证明: 根据二项式定理, $n^k - 1 = [(n-1)+1]^k - 1 = (n-1)^k + C_k^1(n-1)^{k-1} + \dots + C_k^{k-2}(n-1)^2 + C_k^{k-1}(n-1) + 1 - 1 = (n-1)^2[(n-1)^{k-2} + C_k^1(n-1)^{k-3} + \dots + C_k^{k-2}] + C_k^{k-1}(n-1)$.

必要性 (\Rightarrow): 易知 $(n-1)^2 \mid (n-1)^2[(n-1)^{k-2} + C_k^1(n-1)^{k-3} + \dots + C_k^{k-2}]$, 又 $(n-1)^2 \mid n^k - 1$
故 $(n-1)^2 \mid C_k^{k-1}(n-1)$, 得 $(n-1) \mid C_k^{k-1} = k$.

充分性 (\Leftarrow): 由 $(n-1) \mid k$ 可得 $(n-1)^2 \mid k(n-1)$, 又已知 $(n-1)^2 \mid (n-1)^2[(n-1)^{k-2} + C_k^1(n-1)^{k-3} + \dots + C_k^{k-2}]$. 所以 $(n-1)^2 \mid n^k - 1$.

综上所述, $(n-1)^2 \mid n^k - 1 \Leftrightarrow (n-1) \mid k$.

T3. 设 $q \neq 0, \pm 1$. 若对任意的 a, b , 由 $q \mid ab$ 可推出 $q \mid a$ 或 $q \mid b$
至少有一个成立, 证明: q 一定是素数.

证明: (反证法) 假设 q 不是素数, 不妨令 $q = n_1 n_2$, 其中 $2 \leq n_1, n_2 < q$
 $n_1, n_2 \in \mathbb{Z}$
取 $a = n_1 q_1$, 其中 $n_1 + q_1$, $b = n_2 q_2$, 其中 $n_2 + q_2$. 则 $ab = n_1 n_2 q_1 q_2$
 $= q \cdot q_1 q_2$, 得 $q \mid ab$. 又 $n_1 + q_1$, 故 $q \nmid n_1 q_1$. 即 $q \nmid a$. 同理得
 $q \nmid b$. 与条件矛盾! 故假设不成立, q 一定是素数.

Date: _____

14. 证明: (1) $3k+1$ 形式的奇数一定是 $6h+1$ 形式。

证明: 不妨令该奇数为 m , 则 m 可表示为 $2n+1$, $n \in \mathbb{Z}$

由题意, $\begin{cases} m = 3k+1 \\ m = 2n+1 \end{cases} \Rightarrow \begin{cases} m-1 = 3k \\ m-1 = 2n \end{cases} \Rightarrow 3|m-1 \wedge 2|m-1$

所以 $6|m-1$, 即 $\exists h \in \mathbb{Z}$, 使得 $m-1=6h$, $m=6h+1$. 证毕

15. 证明: (1) 形如 $4k-1$ 的素数有无穷多个。

证明: (反证法) 假设形如 $4k-1$ 的素数只有有限个, 设为 p_1, p_2, \dots, p_m ,

由于 k 取 1, 2 时 3, 7 均为素数, 显然 $m > 1$. 由假设, 考虑 $N = 4p_1 p_2 \dots p_m - 1$,

由 $m > 1$ 得 $N > 1$, N 有素因子。又对任意 $k_1, k_2 \in \mathbb{Z}$, $(4k_1+1)(4k_2+1)$

$$= 16k_1 k_2 + 4k_1 + 4k_2 + 1 = 4(4k_1 k_2 + k_1 + k_2) + 1 \text{ 仍具有 } 4k+1 \text{ 形式,}$$

而素因子中除了 2 均可表示为 $4k+1$ 或 $4k-1$ 的形式, N 形式为 $4k-1$ 不可能为偶数, 且必有一个 $4k-1$ 形式的素因子 P , 则 $P \in \{p_1, p_2, \dots, p_m\}$

进而 $P | N - 4p_1 \dots p_m$, 即 $P | 1$, 矛盾! 假设不成立, 形如 $4k-1$ 的素数有无穷多个。

(第 12) 问同理)