Problem 2.16

1 问题描述

对正整数 a, s, t, 证明

$$a^{\gcd(s,t)} - 1 = \gcd(a^s - 1, a^t - 1).$$

作为 bonus, 可以证明对任意正整数 $n > 1$, $n \nmid 2^n - 1$.

2 问题的证明

首先证明以下引理:

引理 1: 对任意正整数 a, m, n, 如果 $m \mid n$, 则有 $a^m - 1 \mid a^n - 1$.

引理 1 的证明: 存在整数 l 使得 $m \cdot l = n$, 因此可以得到如下等式:

$$a^n - 1 = (a^m - 1) \cdot \sum_{i=0}^{l-1} a^{i \cdot m}.$$

因此可以得到 $a^m - 1 \mid a^n - 1$.

首先由最大公约数性质, 可以设 $s = s_1 \cdot \gcd(s,t)$, $t = t_1 \cdot \gcd(s,t)$.

可以将原结论中的等式分解为下述两个命题的交:

$$P : a^{\gcd(s,t)} - 1 \mid \gcd(a^s - 1, a^t - 1)$$
$$Q : \gcd(a^s - 1, a^t - 1) \leq a^{\gcd(s,t)} - 1$$

对于命题 P, 可以由引理 1 得到 $a^{\gcd(s,t)} - 1 \mid a^s - 1$ 以及 $a^{\gcd(s,t)} - 1 \mid a^t - 1$, 即可推出 $a^{\gcd(s,t)} - 1 | \gcd(a^s - 1, a^t - 1)$, 即证命题 P.

对于命题 Q, 由裴蜀定理可以得到: 存在正整数 k, l 使得 $k \cdot s - l \cdot t = \gcd(s,t)$.

由引理 1 可以推出 $a^s - 1 \mid a^{k \cdot s} - 1$ 以及 $a^t - 1 \mid a^{l \cdot t} - 1$. 因此可得

$$\gcd(a^s - 1, a^t - 1) \mid \gcd(a^{k \cdot s} - 1, a^{l \cdot t} - 1)$$

由于

$$\begin{aligned}
\gcd(a^s - 1, a^t - 1) &\leq \gcd(a^{k \cdot s} - 1, a^{l \cdot t} - 1) \\
&= \gcd((a^{k \cdot s} - 1) - a^{\gcd(s,t)} \cdot (a^{l \cdot t} - 1), a^{l \cdot t} - 1) \\
&= \gcd(a^{\gcd(s,t)} - 1, a^{l \cdot t} - 1) \\
&\leq a^{\gcd(s,t)} - 1
\end{aligned}$$

即证命题 Q. 因此原命题得证.

3 Bonus 的证明

对于 n 为偶数的情形, 有 $2 \mid n$ 以及 $2 \nmid 2^n - 1$, 因此可以导出 $n \nmid 2^n - 1$.

对于 $n \geq 3$ 且 n 为奇数的情形, 存在最小素数 p 满足 $p \mid n$. 由 n 为奇数知 p 与 2 互素, 因此由费马小定理可以得到 $p \mid 2^{p-1} - 1$.

反设 $n \mid 2^n - 1$, 因此有 $p \mid 2^n - 1$. 代入上一题结论 $(a = 2, s = p - 1, t = n)$, 即有 $p \mid 2^{\gcd(p-1,n)} - 1$. 由于 p 是最小的满足 $p \mid n$ 的素数, 因此 $p - 1$ 与 n 互素, 即 $\gcd(p-1, n) = 1$, 从而 $p \mid 1$, 矛盾. 因此反设不成立, 原命题得证.