1 第十二题

使用类似辗转相除法的方法:

$$
\begin{aligned}
&r_0 = m \mod n\\
&r_1 = m - r_0 s_0 \quad s.t. \quad 0 \le r_1 < r_0\\
&\dots\\
&r_k = m - r_{k-1}s_{k-1}
\end{aligned}
$$

直到某一个r_{k+1}为零为止, 则类似辗转相除法正确性的证明, 可得$(m,\ n)$也是上述r_i的因数, 且因为$(m,n) \le r_k < r_{k-1} < \cdots < r_0$, 则必存在一个$k$, $s.t.\ r_k = (m,n)$(由良序性保证).
下证明$(2^m-1, 2^n+1) = (2^m-1, 2^{r_0}+1)$(不妨设$n > m$, $n \le m$时自然成立):

$$
\begin{aligned}
(2^m-1, 2^n+1) &= (2^m-1, 2^n+1-2^{n-m}(2^m-1))\\
&= (2^m-1, 2^{n-m}+1)\\
&= \dots\\
&= (2^m-1, 2^{n \mod m}+1)
\end{aligned}
$$

下证明$(2^m-1, 2^{r_i}+1) = (2^m-1, 2^{r_{i+1}}+1)$:

$$
\begin{aligned}
(2^m-1, 2^{r_i}+1) &= (2^m-1, 2^{m-r_i}(2^{r_i}+1)) \quad (because(2^m-1, 2^{m-r_i}) = 1)\\
&= (2^m-1, 2^{m-r_i}(2^{r_i}+1)-(2^m-1))\\
&= (2^m-1, 2^{m-r_i}+1)\\
&= \dots\\
&= (2^m-1, 2^{r_{i+1}}+1)
\end{aligned}
$$

则只需证明, $(2^{m_1 d}-1, 2^d+1) = 1$,其中$d = (m,n)$ $m = m_1 d$, 易得m_1, d都是奇数(因为m是奇数):
由分解式$2^{m_1 d}-1 = (2^d-1)(2^{(m_1-1)d}+...+2^d+1)$, 且:

$$
\begin{aligned}
(2^d+1, 2^{(m_1-1)d}+...+2^d+1) &= (2^d+1, 2^{(m_1-3)d}+...+2^d+1)\\
&= \dots\\
&= (2^d+1, 2^{2d}+2^d+1)\\
&= (2^d+1, 1)\\
&= 1
\end{aligned}
$$

, 并且$(2^d+1, 2^d-1) = (2^d+1, 2) = (1,2) = 1$, 所以有:

$$(2^d+1, (2^d-1)(2^{(m_1-1)d}+...+2^d+1)) = 1$$

证毕. $\square$