上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

第一次作业

李子龙
123033910195

2023 年 9 月 21 日

1. 必答题

(a) 解：计算 gcd(227, 79) 如下：

$$\begin{aligned} 227 &= 79 * 2 + 69 \\ 79 &= 69 * 1 + 10 \\ 69 &= 10 * 6 + 9 \\ 10 &= 9 * 1 + 1 \\ 9 &= 1 * 9 + 0 \end{aligned}$$

所以 gcd(227, 79) = 1，即 227 和 79 互质。

(b) 答：没有。由于 7932 和 11958 都是偶数，至少有一个公因数 2，所以两个数不互质，不满足含有模逆的前提条件。

(c) 解：根据欧拉函数的定义，$\phi(21) = 21 \times \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{7}\right) = 12$，则

$$\begin{aligned} 227^{54996213} \bmod 21 &= 227^{54996213 \bmod \phi(21)} \bmod 21 \\ &= 227^{54996213 \bmod 12} \bmod 21 \\ &= 227^9 \bmod 21 \end{aligned}$$

由于 $227^9 = 227^8 \times 227^1$，所以使用平方相乘法：

$$227 \bmod 21 = 17 \qquad 227^2 \bmod 21 = 17^2 \bmod 21 = 15$$
$$227^4 \bmod 21 = 15^2 \bmod 21 = 15 \qquad 227^8 \bmod 21 = 15^2 \bmod 21 = 15$$

故

$$\begin{aligned} 227^{54996213} \bmod 21 = 227^9 \bmod 21 &= (227^8 \times 227^1) \bmod 21 \\ &= ((227^8 \bmod 21) \times (227 \bmod 21)) \bmod 21 \\ &= (15 \times 17) \bmod 21 \\ &= 3 \end{aligned}$$

(d) 解：由于质因数分解 $730 = 2 \times 5 \times 73$，根据欧拉函数的定义：

$$\begin{aligned}\phi(730) &= 730 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{73}\right) \\ &= 288\end{aligned}$$

2. 选答题

解：使用扩展欧拉算法

$$\begin{aligned}229 &= 2 \times 79 + 71 \\ 79 &= 1 \times 71 + 8 \\ 71 &= 8 \times 8 + 7 \\ 8 &= 1 \times 7 + 1\end{aligned}$$

反向，

$$\begin{aligned}1 &= 8 - 1 \times 7 \\ &= 8 - 1 \times (71 - 8 \times 8) = -1 \times 71 + 9 \times 8 \\ &= -1 \times 71 + 9 \times (79 - 1 \times 71) = 9 \times 79 - 10 \times 71 \\ &= 9 \times 79 - 10 \times (229 - 2 \times 79) = -10 \times 229 + 29 \times 79\end{aligned}$$

也就是

$$\gcd(79, 229) = 1 = -10 \times 229 + 29 \times 79$$

两侧同余于 229，

$$1 = 29 \times 79 \bmod 229$$

也就是 29 为 79 mod 229 的模逆。